I riferimenti normativi del processo civile telematico.[1]

Questo documento informatico contiene in ordine cronologico e per estratto i riferimenti normativi più importanti per lo studio del Processo Civile Telematico[2].

Sono stati realizzati qui di seguito due indici con collegamenti ipertestuali.

Il primo indice è meramente cronologico, il secondo è per argomenti.

Nell'indice cronologico il collegamento tra il riferimento normativo ed il relativo testo avviene cliccando sul numero della corrispondente pagina; nell'indice per argomenti occorre cliccare sul relativo link.

Terminata la consultazione del riferimento normativo, è possibile, utilizzando il collegamento in calce al testo, ritornare agli indici.

AVVERTENZE

(I)

Tra i riferimenti normativi è riportato anche il testo del DPR 123/2001 sebbene il successivo art. 37 del DM 44/2011 abbia precisato che al momento della sua entrata in vigore cessavano di avere efficacia "nel processo civile" le disposizioni di cui al detto DPR e del decreto del Ministro della giustizia 17 luglio 2008. Tuttavia, si è ritenuto opportuno riportarne comunque il testo poiché in dottrina si ritiene che lo stesso sia ancora vigente per il processo civile atteso che l'art. 4 del d.l. 193/2009, in virtù del quale è stato emesso il DM 44/2011, si limitava a prevedere che le regole tecniche del processo civile telematico all'epoca vigenti (quelle del D.M. 17 luglio 2008) si dovevano continuare ad applicare fino alla data di entrata in vigore dei decreti previsti dai commi 1 e 2 del medesimo articolo, decreti che sarebbero stati emanati dal Ministro della giustizia ai sensi del comma 3 dell'art. 17 della legge n. 400 del 1988.

Pertanto, secondo questa dottrina, l'emanazione del D.M. 44/2001, prevista dal citato art. 4, avrebbe dovuto comportare esclusivamente la cessazione di efficacia nel processo civile delle regole tecniche di cui al D.M. 17 luglio 2008 e non anche delle disposizioni del Regolamento di cui al DPR 123/2001 considerato, peraltro, che, ai sensi del terzo comma dell'art. 17 della legge n. 400 del 1988, i regolamenti ministeriali, come per l'appunto il DM 44/2011, non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo.

(II)

Per motivi di esegesi normativa è stato riportato anche il testo dell'art. 51 del d.l. 112/2008, convertito con modificazioni, dalla legge 6 agosto 2008, n. 133, e modificato dal decreto-legge 29 dicembre 2009, n. 193, convertito con modificazioni, dalla legge 22 febbraio 2010, n. 24, sulle comunicazioni di cancelleria a mezzo PEC sebbene i

[1] a cura di Pietro Lupi, magistrato ordinario.
[2] Aggiornato al 23 aprile 2019.

primi tre commi, che riguardano detta materia, siano stati abrogati dall'art. 16 del d.l. 179/2012 convertito con modificazioni, nella legge 221/2012.

Vai all'indice cronologico

Vai all'indice dei riferimenti normativi per argomenti

A - Indice cronologico delle fonti normative del PCT

B - Indice dei riferimenti normativi degli argomenti principali.

Attestazioni di conformità

Art. 518 c.p.c. (Forma del pignoramento)

Art. 521-bis c.p.c. (Pignoramento e custodia di autoveicoli, motoveicoli e rimorchi)

Art. 543 c.p.c. (Forma del pignoramento)

Art. 557 c.p.c. (Deposito dell'atto di pignoramento)

Art. 3-bis L. 53/1994

Art. 9 L. 53/1994

Art. 16-bis, commi 2, ult. periodo, e 9-bis d.l. 179/2012

Art. 16-decies d.l. 179/12 (Potere di certificazione di conformità delle copie degli atti e dei provvedimenti)

Art. 16-undecies d.l. 179/12 (Modalità dell'attestazione di conformità)

Art. 19-ter Provv. Resp. SIA 16 aprile 2014 (Modalità dell'attestazione di conformità apposta su un documento informatico separato)

Compenso professionale

Art. 4, comma 1-bis, D.M. 55/2014 (Parametri generali per la determinazione dei compensi in sede giudiziale)

Deposito telematico degli atti del Giudice.

Art. 15 DM 44/2011 (Regole tecniche per il deposito dell'atto del processo da parte dei soggetti abilitati interni)

Art. 16 Provv. DGSIA 16.4.2014 (Specifiche tecniche per il deposito dell'atto del processo da parte dei soggetti abilitati interni)

Deposito telematico degli atti degli abilitati esterni (avvocati e ausiliari del giudice).

Art. 13 DM 44/2011 (Regole tecniche per la trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati)

Art. 14 DM 44/2011 (Regole tecniche per i documenti probatori e allegati non informatici)

Art. 12 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per il formato dell'atto del processo in forma di documento informatico)

Art. 13 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per il formato dei documenti informatici allegati)

Art. 14 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per la trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati)

Art. 15 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per i documenti probatori e allegati non informatici)

Documento informatico.

Art. 15 Legge 15 marzo 1997, n. 59

Art. 20 CAD (Documento informatico)

Art. 22 CAD (Copie informatiche di documenti analogici)

Art. 23 CAD (Copie analogiche di documenti informatici)

Art. 23bis CAD (Duplicati e copie informatiche di documenti informatici)

Art. 71 CAD (Linee Guida)

D.P.C.M. 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione)

D.P.C.M. 13 novembre 2014 (Regole tecniche sul documento informatico)

Art. 16-decies d.l. 179/12 (Potere di certificazione di conformità delle copie degli atti e dei provvedimenti)

Art. 16-undecies d.l. 179/12 (Modalità dell'attestazione di conformità)

Art. 19-ter Provv. Resp. SIA 16 aprile 2014 (Modalità dell'attestazione di conformità apposta su un documento informatico separato)

Domicilio digitale e Identità digitale.

Art. 1, lett n-ter, CAD (Definizioni)

Art. 3bis CAD (Identità digitale e domicilio digitale del cittadino)

Art. 6 CAD (Utilizzo del domicilio digitale)

Art. 6-bis CAD (Registro INI-PEC)

Art. 6-ter (Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi)

Art. 6-quater (Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro)

Art. 62 CAD (Anagrafe nazionale della popolazione residente – ANPR)

Domicilio digitale della parte nel processo civile.

Art. 16-sexies d.l. 179/12 (Domicilio digitale)

Esecuzioni

Art. 16-bis, co. 2, d.l. 179/12 (Obbligatorietà del deposito telematico degli atti processuali)

Art. 490 c.p.c. (Pubblicità degli avvisi)

Art. 492-bis c.p.c. (Ricerca con modalità telematiche dei beni da pignorare)

Art. 518 c.p.c. (Forma del pignoramento)

Art. 521-bis c.p.c. (Pignoramento e custodia di autoveicoli, motoveicoli e rimorchi)

Art. 543 c.p.c. (Forma del pignoramento)

Art. 557 c.p.c. (Deposito dell'atto di pignoramento)

Art. 155-quater disp. att. c.p.c. (Modalità di accesso alle banche dati)

Art. 159-ter disp. att. c.p.c. (Iscrizione a ruolo del processo esecutivo per espropriazione a cura di soggetto diverso dal creditore)

Art. 161-ter disp. att. c.p.c. (Vendite con modalità telematiche)

Art. 164-ter disp. att. c.p.c. (Inefficacia del pignoramento per mancato deposito della nota di iscrizione a ruolo)

Facoltatività del deposito telematico degli atti introduttivi e della costituzione in giudizio.

Art. 16-bis d.l. 179/12 (comma 1bis)

Fascicolo informatico.

Art. 41 CAD (Procedimento e fascicolo informatico)

Art. 9 DM 44/2011 (Sistema informatico di gestione del fascicolo informatico)

Art. 11 Provv. Resp. SIA 16.4.2014 (Fascicolo informatico)

Artt. 12 e 13 DPR 123/2001

Art. 13 DPCM 13 novembre 2014

Firma digitale.

Art. 1 CAD, lett. s (Definizione della firma digitale)

Art. 21 CAD (Documento informatico sottoscritto con firma elettronica)

Art. 24 CAD (Firma digitale)

Art. 25 CAD (Firma autenticata)

Art. 32 CAD (Obblighi del titolare e del prestatore di servizi)

Art. 35 CAD (Dispositivi sicuri e procedure per la generazione della firma)

D.P.C.M. 22 febbraio 2013 (Regole tecniche firma elettronica)

Normativa comunitaria

Regolamento UE Eidas 910/2014

Notificazioni e comunicazioni telematiche effettuate dalla Cancelleria.

Art. 136 c.p.c. (Comunicazioni)

Art. 137 c.p.c. (Notificazioni)

Art. 4 d.l. 193/2009 (Misure urgenti per la digitalizzazione della giustizia)

Art. 16 d.l. 179/2012 (Biglietti di cancelleria, comunicazioni e notificazioni per via telematica)

Art. 16 DM 44/2011 (Regole tecniche per le comunicazioni per via telematica)

Art. 17 DM 44/2011 (Regole tecniche per le notificazioni per via telematica)

Art. 17 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per le comunicazioni e notificazioni per via telematica)

Art. 18 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per la comunicazione dati sensibili)

Art. 6 DPR 123/2001

Art. 51 d.l. 112/2008

Notifiche via PEC effettuate dagli Avvocati.

Legge 21 gennaio 1994, n. 53

Art. 16-septies d.l. 179/12 (orario delle notificazioni via PEC)

Art. 18 DM 44/20011 (Notificazioni per via telematica eseguite dagli avvocati)

Art. 19-bis Provv. Resp. SIA 16.4.2014 (Notificazioni per via telematica eseguite dagli avvocati)

Art. 16-ter D.L. 179/2012 (Pubblici registri PEC)

Art. 9 DPR 68/2005 (Firma elettronica delle ricevute e della busta di trasporto)

Art. 6-bis CAD (Registro INI-PEC)

Notifiche telematiche tramite UNEP

Art. 137 c.p.c. (Notificazioni)

Art. 149-bis c.p.c. (Notificazione a mezzo posta elettronica)

Art. 17 DM 44/2011 (Regole tecniche per le notificazioni per via telematica)

Art. 19 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche per le notificazioni per via telematica a cura degli uffici NEP)

Obbligatorietà del PCT

Art. 44 d.l. 90/2014 (Obbligatorietà del deposito telematico degli atti processuali)

Art. 16-bis d.l. 179/2012

Pagamenti telematici

Art. 5 CAD (Effettuazione di pagamenti con modalità informatiche)

Art. 4 d.l. 193/2009 (Misure urgenti per la digitalizzazione della giustizia)

Artt. 30 e segg. DM 44/2011 (Regole tecniche)

Art. 26 Provv Resp. SIA 16.4.2014 (Specifiche tecniche)

PEC

D.P.R. 11 febbraio 2005, n. 68

Art. 6 DPR 68/2005 (Ricevuta di accettazione e di avvenuta consegna)

Art. 8 DPR 68/2005 (Avviso di mancata consegna)

Art. 9 DPR 68/2005 (Firma elettronica delle ricevute e della busta di trasporto)

Art. 48 CAD (Posta elettronica certificata)

DPCM 2 novembre 2005 (Regole tecniche)

Decreto Legge 25 giugno 2008, n. 185 (Obbligo delle imprese, dei professionisti e della Pubbliche Amministrazioni di comunicazione del proprio indirizzo PEC)

D.P.C.M. 27 settembre 2012

Art. 16-ter D.L. 179/2012 (Pubblici registri degli indirizzi PEC)

Art. 21 Provv. Resp. SIA 16.4.2014 (Requisiti della casella di PEC del soggetto abilitato esterno)

Portale dei servizi telematici

Art. 6 D.M. 44/2011 (Regole tecniche)

Art. 5 Provv. Resp. SIA 16.4.2014 (Specifiche tecniche)

Portale Vendite Pubbliche (PVP)

Art. 490 c.p.c. (Pubblicità degli avvisi)

Art. 631-bis c.p.c. (Omessa pubblicità sul portale delle vendite pubbliche)

Art. 161-quater disp. att. c.p.c.

Art. 4 D.L. 59/2016

D.M. 5/12/2017

Procura alle liti

art. 83 c.p.c. (Procura alle liti)

art. 18, comma 5, D.M. 44/2011

Protezione dati personali nell'attività giudiziaria

Decreto legislativo 30 giugno 2003, n. 196

REGINDE

Art. 7 D.M. 44/2011 (Regole tecniche)

Art. 7, 8, 9 e 9-bis Provv. Resp. SIA 16.4.2014 (Specifiche tecniche)

Vendite telematiche

Art. 161-ter disp. att. c.p.c. (Vendite con modalità telematiche)

D.M. 32/2015 (regole tecniche)

Art. 7 D.M. 31/10/2006

Art. 23 D.L. 83/2015

Regio Decreto 28 ottobre 1940, n. 1443 - Codice di procedura civile (ESTRATTO).

(ritorna all'indice cronologico)

(*ritorna all'indice per argomenti*)

LIBRO PRIMO
DISPOSIZIONI GENERALI
TITOLO III
DELLE PARTI E DEI DIFENSORI
CAPO II
Dei difensori

Art. 83
(Procura alle liti)

Quando la parte sta in giudizio col ministero di un difensore, questi deve essere munito di procura. La procura alle liti può essere generale o speciale, e deve essere conferita con atto pubblico o scrittura privata autenticata.

La procura speciale può essere anche apposta in calce o a margine della citazione, del ricorso, del controricorso, della comparsa di risposta o d'intervento, del precetto o della domanda d'intervento nell'esecuzione, ovvero della memoria di nomina del nuovo difensore, in aggiunta o in sostituzione del difensore originariamente designato. In tali casi l'autografia della sottoscrizione della parte deve essere certificata dal difensore. La procura si considera apposta in calce anche se rilasciata su foglio separato che sia però congiunto materialmente all'atto cui si riferisce, o su documento informatico separato sottoscritto con firma digitale e congiunto all'atto cui si riferisce mediante strumenti informatici, individuati con apposito decreto del Ministero della giustizia. Se la procura alle liti è stata conferita su supporto cartaceo, il difensore che si costituisce attraverso strumenti telematici ne trasmette la copia informatica autenticata con firma digitale, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e trasmessi in via telematica.

La procura speciale si presume conferita soltanto per un determinato grado del processo, quando nell'atto non è espressa volontà diversa.

TITOLO VI
DEGLI ATTI PROCESSUALI
CAPO I
Delle forme degli atti e dei provvedimenti
Sezione IV
Delle comunicazioni e delle notificazioni

Art. 136
(Comunicazioni)

Il cancelliere, con biglietto di cancelleria, fa le comunicazioni che sono prescritte dalla legge o dal giudice al pubblico ministero, alle parti, al consulente, agli altri ausiliari del giudice e ai testimoni, e dà notizia di quei provvedimenti per i quali è disposta dalla legge tale forma abbreviata di comunicazione.

Il biglietto è consegnato dal cancelliere al destinatario, che ne rilascia ricevuta, ovvero trasmesso a mezzo posta elettronica certificata, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.

Salvo che la legge disponga diversamente, se non è possibile procedere ai sensi del comma che precede, il biglietto viene trasmesso a mezzo telefax, o è rimesso all'ufficiale giudiziario per la notifica.

Art. 137
(Notificazioni)

Le notificazioni, quando non è disposto altrimenti, sono eseguite dall'ufficiale giudiziario, su istanza di parte o su richiesta del pubblico ministero o del cancelliere.

L'ufficiale giudiziario esegue la notificazione mediante consegna al destinatario di copia conforme all'originale dell'atto da notificarsi. Se l'atto da notificare o comunicare è costituito da un documento informatico e il destinatario non possiede indirizzo di posta elettronica certificata, l'ufficiale giudiziario esegue la notificazione mediante consegna di una copia dell'atto su supporto cartaceo, da lui dichiarata conforme all'originale, e conserva il documento informatico per i due anni successivi.

Se richiesto, l'ufficiale giudiziario invia l'atto notificato anche attraverso strumenti telematici all'indirizzo di posta elettronica dichiarato dal destinatario della notifica o dal suo procuratore, ovvero consegna ai medesimi, previa esazione dei relativi diritti, copia dell'atto notificato, su supporto informatico non riscrivibile.

Se la notificazione non può essere eseguita in mani proprie del destinatario, tranne che nel caso previsto dal secondo comma dell'articolo 143, l'ufficiale giudiziario consegna o deposita la copia dell'atto da notificare in busta che provvede a sigillare e su cui trascrive il numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso. Sulla busta non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto.

Le disposizioni di cui al terzo comma si applicano anche alle comunicazioni effettuate con biglietto di cancelleria ai sensi degli articoli 133 e 136.

149-bis
(Notificazione a mezzo posta elettronica)

Se non è fatto espresso divieto dalla legge, la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento cartaceo.

Se procede ai sensi del primo comma, l'ufficiale giudiziario trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante da pubblici elenchi.

La notifica si intende perfezionata nel momento in cui il gestore rende disponibile il documento informatico nella casella di posta elettronica certificata del destinatario.

L'ufficiale giudiziario redige la relazione di cui all'articolo 148, primo comma, su documento informatico separato, sottoscritto con firma digitale e congiunto all'atto cui si riferisce mediante strumenti informatici, individuati con apposito decreto del Ministero della giustizia. La relazione contiene le informazioni di cui all'articolo 148, secondo comma, sostituito il luogo della consegna con l'indirizzo di posta elettronica presso il quale l'atto è stato inviato.

Al documento informatico originale o alla copia informatica del documento cartaceo sono allegate, con le modalità previste dal quarto comma, le ricevute di invio e di consegna previste dalla normativa, anche regolamentare, concernente la trasmissione e la ricezione dei documenti informatici trasmessi in via telematica.

Eseguita la notificazione, l'ufficiale giudiziario restituisce all'istante o al richiedente, anche per via telematica, l'atto notificato, unitamente alla relazione di notificazione e agli allegati previsti dal quinto comma.

(ritorna all'indice cronologico)

(ritorna all'indice per argomenti)

TITOLO III
DELLE IMPUGNAZIONI
CAPO III
Del ricorso per cassazione
Sezione II
Del procedimento e dei provvedimenti

Art. 388.
(Trasmissione di copia del dispositivo al giudice di merito)

Copia della sentenza è trasmessa dal cancelliere della Corte a quello del giudice che ha pronunciato la sentenza impugnata, affinché ne sia presa nota in margine all'originale di quest'ultima. La trasmissione può avvenire anche in via telematica.

LIBRO TERZO
DEL PROCESSO DI ESECUZIONE
TITOLO II
DELL'ESPROPRIAZIONE FORZATA
CAPO I
Dell'espropriazione forzata in generale

Sezione I
Dei modi e delle forme dell'espropriazione forzata in generale

Art. 490
(Pubblicità degli avvisi)

Quando la legge dispone che di un atto esecutivo sia data pubblica notizia, un avviso contenente tutti i dati, che possono interessare il pubblico, deve essere inserito sul portale del Ministero della giustizia in un'area pubblica denominata "portale delle vendite pubbliche".

In caso di espropriazione di beni mobili registrati, per un valore superiore a 25.000 euro, e di beni immobili, lo stesso avviso, unitamente a copia dell'ordinanza del giudice e della relazione di stima redatta ai sensi dell'articolo 173-bis delle disposizioni di attuazione del presente codice, è altresì inserito in appositi siti internet almeno quarantacinque giorni prima del termine per la presentazione delle offerte o della data dell'incanto.

Anche su istanza del creditore procedente o dei creditori intervenuti muniti di titolo esecutivo il giudice può disporre inoltre che l'avviso sia inserito almeno quarantacinque giorni prima del termine per la presentazione delle offerte una o più volte sui quotidiani di informazione locali aventi maggiore diffusione nella zona interessata o, quando opportuno, sui quotidiani di informazione nazionali o che sia divulgato con le forme della pubblicità commerciale. Sono equiparati ai quotidiani, i giornali di informazione locale, multisettimanali o settimanali editi da soggetti iscritti al Registro operatori della comunicazione (ROC) e aventi caratteristiche editoriali analoghe a quelle dei quotidiani che garantiscono la maggior diffusione nella zona interessata. Nell'avviso è omessa l'indicazione del debitore.

Sezione II
Del pignoramento

Art. 492-bis
(Ricerca con modalità telematiche dei beni da pignorare)

Su istanza del creditore, il presidente del tribunale del luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede, verificato il diritto della parte istante a procedere ad esecuzione forzata, autorizza la ricerca con modalità telematiche dei beni da pignorare. L'istanza deve contenere l'indicazione dell'indirizzo di posta elettronica ordinaria ed il numero di fax del difensore nonché, ai fini dell'articolo 547, dell'indirizzo di posta elettronica certificata. L'istanza non può essere proposta prima che sia decorso il termine di cui all'articolo 482. Se vi è pericolo nel ritardo, il presidente del tribunale autorizza la ricerca telematica dei beni da pignorare prima della notificazione del precetto.

Fermo quanto previsto dalle disposizioni in materia di accesso ai dati e alle informazioni degli archivi automatizzati del Centro elaborazione dati istituito presso il Ministero dell'interno ai sensi dell'articolo 8 della legge 1° aprile 1981, n. 121, con l'autorizzazione di cui al primo comma il presidente del tribunale o un giudice da lui delegato dispone che l'ufficiale giudiziario acceda mediante collegamento telematico diretto ai dati contenuti nelle banche dati delle pubbliche amministrazioni e, in particolare, nell'anagrafe tributaria, compreso l'archivio dei rapporti finanziari, e in quelle degli enti previdenziali, per l'acquisizione di tutte le informazioni rilevanti per l'individuazione di cose e crediti da sottoporre ad esecuzione, comprese quelle relative ai rapporti intrattenuti dal debitore con istituti di credito e datori di lavoro o committenti. Terminate le operazioni l'ufficiale giudiziario redige un unico processo verbale nel quale indica tutte le banche dati interrogate e le relative risultanze. L'ufficiale giudiziario procede a pignoramento munito del titolo esecutivo e del precetto, anche acquisendone copia dal fascicolo informatico. Nel caso di cui al primo comma, quarto periodo, il precetto è consegnato o trasmesso all'ufficiale giudiziario prima che si proceda al pignoramento.

Se l'accesso ha consentito di individuare cose che si trovano in luoghi appartenenti al debitore compresi nel territorio di competenza dell'ufficiale giudiziario, quest'ultimo accede agli stessi per provvedere d'ufficio agli adempimenti di cui agli articoli 517, 518 e 520. Se i luoghi non sono compresi nel territorio di competenza di cui al periodo precedente, copia autentica del verbale è rilasciata al creditore che, entro quindici giorni dal rilascio a pena d'inefficacia della richiesta, la presenta, unitamente all'istanza per gli adempimenti di cui agli articoli 517, 518 e 520, all'ufficiale giudiziario territorialmente competente. L'ufficiale giudiziario, quando non rinviene una cosa individuata mediante l'accesso nelle banche dati di cui al secondo comma, intima al debitore di indicare entro quindici giorni il luogo in cui si trova, avvertendolo che l'omessa o la falsa comunicazione è punita a norma dell'articolo 388, sesto comma, del codice penale.

Se l'accesso ha consentito di individuare crediti del debitore o cose di quest'ultimo che sono nella disponibilita' di terzi, l'ufficiale giudiziario notifica d'ufficio, ove possibile a norma dell'articolo 149-bis o a mezzo telefax, al debitore e al terzo il verbale, che dovra' anche contenere l'indicazione del credito per cui si procede, del titolo esecutivo e del precetto, dell'indirizzo di posta elettronica certificata di cui al primo comma, del luogo in cui il creditore ha eletto domicilio o ha dichiarato di essere residente, dell'ingiunzione, dell'invito e dell'avvertimento al debitore di cui all'articolo 492, primo, secondo e terzo comma, nonché l'intimazione al terzo di non disporre delle cose o delle somme dovute, nei limiti di cui all'articolo 546. Il verbale di cui al presente comma è notificato al terzo per estratto, contenente esclusivamente i dati a quest'ultimo riferibili.

Quando l'accesso ha consentito di individuare piu' crediti del debitore o piu' cose di quest'ultimo che sono nella disponibilita' di terzi l'ufficiale giudiziario sottopone ad esecuzione i beni scelti dal creditore.

Quando l'accesso ha consentito di individuare sia cose di cui al terzo comma che crediti o cose di cui al quinto comma, l'ufficiale giudiziario sottopone ad esecuzione i beni scelti dal creditore.

CAPO II
Dell'espropriazione mobiliare presso il debitore
Sezione I
Del pignoramento

Art. 518
(Forma del pignoramento)

L'ufficiale giudiziario redige delle sue operazioni processo verbale nel quale dà atto dell'ingiunzione di cui all'articolo 492 e descrive le cose pignorate, nonché il loro stato, mediante rappresentazione fotografica ovvero altro mezzo di ripresa audiovisiva, determinandone approssimativamente il presumibile valore di realizzo con l'assistenza, se ritenuta utile o richiesta dal creditore, di un esperto stimatore da lui scelto. Se il pignoramento cade su frutti non ancora raccolti o separati dal suolo, l'ufficiale giudiziario ne descrive la natura, la qualità e l'ubicazione.

Quando ritiene opportuno differire le operazioni di stima l'ufficiale giudiziario redige un primo verbale di pignoramento, procedendo senza indugio e comunque entro il termine perentorio di trenta giorni alla definitiva individuazione dei beni da assoggettare al pignoramento sulla base dei valori indicati dall'esperto, al quale è consentito in ogni caso accedere al luogo in cui i beni si trovano. Il giudice dell'esecuzione liquida le spese ed il compenso spettanti all'esperto, tenuto conto dei valori di effettiva vendita o assegnazione dei beni o, in qualunque altro caso, sulla base dei valori stimati.

Nel processo verbale l'ufficiale giudiziario fa relazione delle disposizioni date per conservare le cose pignorate.

Se il debitore non è presente, l'ufficiale giudiziario rivolge l'ingiunzione alle persone indicate nell'articolo 139, secondo comma, e consegna loro un avviso dell'ingiunzione stessa per il debitore. In mancanza di dette persone affigge l'avviso alla porta dell'immobile in cui ha eseguito il pignoramento.

Compiute le operazioni, l'ufficiale giudiziario consegna senza ritardo al creditore il processo verbale, il titolo esecutivo e il precetto. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi degli atti di cui al periodo precedente, entro quindici giorni dalla consegna. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il cancelliere al momento del deposito forma il fascicolo dell'esecuzione. Sino alla scadenza del termine di cui all'articolo 497 copia del processo verbale è conservata dall'ufficiale giudiziario a disposizione del debitore. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie degli atti di cui al primo periodo del presente comma sono depositate oltre il termine di quindici giorni dalla consegna al creditore.

Su istanza del creditore, da depositare non oltre il termine per il deposito dell'istanza di vendita, il giudice, nominato uno stimatore quando appare opportuno, ordina l'integrazione del pignoramento se ritiene che il presumibile valore di realizzo dei beni pignorati sia inferiore a quello indicato nel primo comma. In tale caso l'ufficiale giudiziario riprende senza indugio le operazioni di ricerca dei beni.

Art. 521-bis
Pignoramento e custodia di autoveicoli, motoveicoli e rimorchi

Oltre che con le forme previste dall'articolo 518, il pignoramento di autoveicoli, motoveicoli e rimorchi può essere eseguito anche mediante notificazione al debitore e successiva trascrizione di un atto nel quale si indicano esattamente, con gli estremi richiesti dalla legge speciale per la loro iscrizione nei

pubblici registri, i beni e i diritti che si intendono sottoporre ad esecuzione, e gli si fa l'ingiunzione prevista nell'articolo 492. Il pignoramento contiene altresì l'intimazione a consegnare entro dieci giorni i beni pignorati, nonché i titoli e i documenti relativi alla proprietà e all'uso dei medesimi, all'istituto vendite giudiziarie autorizzato ad operare nel territorio del circondario nel quale è compreso il luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede ((o, in mancanza, a quello più vicino.

Col pignoramento il debitore è costituito custode dei beni pignorati e di tutti gli accessori comprese le pertinenze e i frutti, senza diritto a compenso.

Al momento della consegna l'istituto vendite giudiziarie assume la custodia del bene pignorato e ne dà immediata comunicazione al creditore pignorante, a mezzo posta elettronica certificata ove possibile. Decorso il termine di cui al primo comma, gli organi di polizia che accertano la circolazione dei beni pignorati o comunque li rinvengono procedono al ritiro della carta di circolazione nonché, ove possibile, dei titoli e dei documenti relativi alla proprietà e all'uso dei beni pignorati e consegnano il bene pignorato all'istituto vendite giudiziarie più vicino al luogo in cui il bene pignorato è stato rinvenuto. Si applica il terzo comma.

Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'atto di pignoramento perché proceda alla trascrizione nei pubblici registri. Entro trenta giorni dalla comunicazione di cui al terzo comma, il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi del titolo esecutivo, del precetto, dell'atto di pignoramento e della nota di trascrizione. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo.

Il cancelliere forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie dell'atto di pignoramento, del titolo esecutivo e del precetto sono depositate oltre il termine di cui al quinto comma.

In deroga a quanto previsto dall'articolo 497, l'istanza di assegnazione o l'istanza di vendita deve essere depositata entro quarantacinque giorni dal deposito da parte del creditore della nota di iscrizione a norma del presente articolo ovvero dal deposito da parte di quest'ultimo delle copie conformi degli atti, a norma dell'articolo 159-ter delle disposizioni per l'attuazione del presente codice.

Si applicano in quanto compatibili le disposizioni del presente capo.

(ritorna all'indice cronologico)

(*ritorna all'indice per argomenti*)

CAPO III
Dell'espropriazione presso terzi
Sezione I
Del pignoramento e dell'intervento

Art. 543
(Forma del pignoramento)

Il pignoramento di crediti del debitore verso terzi o di cose del debitore che sono in possesso di terzi, si esegue mediante atto notificato al terzo e al debitore a norma degli articoli 137 e seguenti.

L'atto deve contenere, oltre all'ingiunzione al debitore di cui all'articolo 492:

1) l'indicazione del credito per il quale si procede, del titolo esecutivo e del precetto;

2) l'indicazione, almeno generica, delle cose o delle somme dovute e l'intimazione al terzo di non disporne senza ordine di giudice;

3) la dichiarazione di residenza o l'elezione di domicilio nel comune in cui ha sede il tribunale competente nonché l'indicazione dell'indirizzo di posta elettronica certificata del creditore procedente;

4) la citazione del debitore a comparire davanti al giudice competente, con l'invito al terzo a comunicare la dichiarazione di cui all'articolo 547 al creditore procedente entro dieci giorni a mezzo raccomandata ovvero a mezzo di posta elettronica certificata; con l'avvertimento al terzo che in caso di mancata comunicazione della dichiarazione, la stessa dovrà essere resa dal terzo comparendo in un'apposita udienza e che quando il terzo non compare o, sebbene comparso, non rende la dichiarazione, il credito pignorato o il possesso di cose di appartenenza del debitore, nell'ammontare o nei termini indicati dal creditore, si considereranno non contestati ai fini del procedimento in corso e dell'esecuzione fondata sul provvedimento di assegnazione)).

Nell'indicare l'udienza di comparizione si deve rispettare il termine previsto nell'articolo 501.

Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'originale dell'atto di citazione. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi dell'atto di citazione, del titolo esecutivo e del precetto, entro trenta giorni dalla consegna. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il cancelliere al momento del deposito forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie degli atti di cui al secondo periodo sono depositate oltre il termine di trenta giorni dalla consegna al creditore.

Quando procede a norma dell'articolo 492-bis, l'ufficiale giudiziario consegna senza ritardo al creditore il verbale, il titolo esecutivo ed il precetto, e si applicano le disposizioni di cui al quarto comma. Decorso il termine di cui all'articolo 501, il creditore pignorante e ognuno dei creditori intervenuti muniti di titolo esecutivo possono chiedere l'assegnazione o la vendita delle cose mobili o l'assegnazione dei crediti. Sull'istanza di cui al periodo precedente il giudice fissa l'udienza per l'audizione del creditore e del debitore e provvede a norma degli articoli 552 o 553. Il decreto con cui viene fissata l'udienza di cui al periodo precedente è notificato a cura del creditore procedente e deve contenere l'invito e l'avvertimento al terzo di cui al numero 4) del secondo comma.

Art. 557
(Deposito dell'atto di pignoramento)

Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'atto di pignoramento e la nota di trascrizione restituitagli dal conservatore dei registri immobiliari. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi del titolo esecutivo, del precetto, dell'atto di pignoramento e della nota di trascrizione entro quindici giorni dalla consegna dell'atto di pignoramento. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Nell'ipotesi di cui all'articolo 555, ultimo comma, il creditore deve depositare la nota di trascrizione appena restituitagli dal conservatore dei registri immobiliari.

Il cancelliere forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie dell'atto di pignoramento, del titolo esecutivo e del precetto sono depositate oltre il termine di quindici giorni dalla consegna al creditore.

TITOLO VI
DELLA SOSPENSIONE E DELL'ESTINZIONE DEL PROCESSO
CAPO II
Dell'estinzione del processo

Art. 631-bis
(Omessa pubblicità sul portale delle vendite pubbliche)

Se la pubblicazione sul portale delle vendite pubbliche non è effettuata nel termine stabilito dal giudice per causa imputabile al creditore pignorante o al creditore intervenuto munito di titolo esecutivo, il giudice dichiara con ordinanza l'estinzione del processo esecutivo e si applicano le disposizioni di cui all'articolo 630, secondo e terzo comma. La disposizione di cui al presente articolo non si applica quando la pubblicità sul portale non è stata effettuata perché i sistemi informatici del dominio giustizia non sono funzionanti, a condizione che tale circostanza sia attestata a norma dell'articolo 161-quater delle disposizioni per l'attuazione del presente codice.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Regio Decreto 18 dicembre 1941, n. 1368 - Disposizioni per l'attuazione del Codice di procedura civile e disposizioni transitorie (ESTRATTO).

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

TITOLO II.
DEGLI ESPERTI E DEGLI AUSILIARI DEL GIUDICE
CAPO III.
Dei registri di cancelleria e degli atti del cancelliere.

Art. 45
(Forma delle comunicazioni del cancelliere)

Quando viene redatto su supporto cartaceo il biglietto, col quale il cancelliere esegue le comunicazioni a norma dell'articolo 136 del codice, si compone di due parti uguali, una delle quali deve essere consegnata al destinatario e l'altra deve essere conservata nel fascicolo d'ufficio.

Il biglietto contiene in ogni caso l'indicazione dell'ufficio giudiziario, della sezione alla quale la causa è assegnata, dell'istruttore se è nominato, del numero del ruolo generale sotto il quale l'affare è iscritto e del ruolo dell'istruttore il nome delle parti ed il testo integrale del provvedimento comunicato.

Nella parte che viene inserita nel fascicolo di ufficio deve essere stesa la relazione di notificazione dell'ufficiale giudiziario ò scritta la ricevuta del destinatario. Se l'ufficiale giudiziario si avvale del servizio postale, il cancelliere conserva nel fascicolo d'ufficio anche la ricevuta della raccomandata.

Quando viene trasmesso a mezzo posta elettronica certificata il biglietto di cancelleria è costituito dal messaggio di posta elettronica certificata, formato ed inviato nel rispetto della normativa, anche regolamentare, concernente la trasmissione e la ricezione dei documenti informatici.

TITOLO IV.
DEL PROCESSO DI ESECUZIONE
Capo I.
Del titolo esecutivo e dell'espropriazione forzata in generale.

Art. 155-quater
(Modalità di accesso alle banche dati)

Le pubbliche amministrazioni che gestiscono banche dati contenenti informazioni utili ai fini della ricerca di cui all'articolo 492-bis del codice mettono a disposizione degli ufficiali giudiziari gli accessi, con le modalità di cui all'articolo 58 del codice di cui al decreto legislativo 7 marzo 2005, n. 82[3], e successive modificazioni, su richiesta del Ministero della giustizia. Sino a quando non sono definiti dall'Agenzia per l'Italia digitale gli standard di comunicazione e le regole tecniche di cui al comma 2 del predetto articolo 58 e, in ogni caso, quando l'amministrazione che gestisce la banca dati o il Ministero della giustizia non dispongono dei sistemi informatici per la cooperazione applicativa di cui all'articolo 72, comma 1, lettera e), del medesimo codice di cui al decreto legislativo n. 82 del 2005, l'accesso è consentito previa stipulazione, senza nuovi o maggiori oneri per la finanza pubblica, di una convenzione finalizzata alla fruibilità informatica dei dati, sentito il Garante per la protezione dei dati personali. Il Ministero della giustizia pubblica sul portale dei servizi telematici l'elenco delle banche dati per le quali è operativo l'accesso da parte dell'ufficiale giudiziario per le finalità di cui all'articolo 492-bis del codice.

Il Ministro della giustizia può procedere al trattamento dei dati acquisiti senza provvedere all'informativa di cui all'articolo 13 del decreto legislativo 30 giugno 2003, n. 196.

E' istituito, presso ogni ufficio notifiche, esecuzioni e protesti, il registro cronologico denominato "Modello ricerca beni", conforme al modello adottato con il decreto del Ministro della giustizia di cui al primo comma.

[3] L'art. 58 del CAD è stato abrogato dal D.Lgs 26 agosto 2016, n. 179.

L'accesso da parte dell'ufficiale giudiziario alle banche dati di cui all'articolo 492-bis del codice e a quelle individuate con il decreto di cui al primo comma è gratuito. La disposizione di cui al periodo precedente si applica anche all'accesso effettuato a norma dell'articolo 155-quinquies di queste disposizioni.

Art. 159-ter
(Iscrizione a ruolo del processo esecutivo per espropriazione a cura di soggetto diverso dal creditore).

Colui che, prima che il creditore abbia depositato la nota di iscrizione a ruolo prevista dagli articoli 518, 521-bis, 543 e 557 del codice, deposita per primo un atto o un'istanza deve depositare la nota di iscrizione a ruolo e una copia dell'atto di pignoramento. Quando al deposito della nota di iscrizione a ruolo procede uno dei soggetti di cui all'articolo 16-bis, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, diverso dal creditore, il deposito può aver luogo con modalità non telematiche e la copia dell'atto di pignoramento può essere priva dell'attestazione di conformità. Quando l'istanza proviene dall'ufficiale giudiziario, anche nel caso di cui all'articolo 520, primo comma, del codice, all'iscrizione a ruolo provvede d'ufficio il cancelliere. Quando l'iscrizione a ruolo ha luogo a norma del presente articolo, il creditore, nei termini di cui agli articoli 518, 521-bis, 543 e 557 del codice, provvede, a pena di inefficacia del pignoramento, al deposito delle copie conformi degli atti previsti dalle predette disposizioni e si applica l'articolo 164-ter delle presenti disposizioni.

Art. 161-ter
(Vendite con modalità telematiche).

Il Ministro della giustizia stabilisce con proprio decreto le regole tecnico-operative per lo svolgimento della vendita di beni mobili e immobili mediante gara telematica nei casi previsti dal codice, nel rispetto dei principi di competitività, trasparenza, semplificazione, efficacia, sicurezza, esattezza e regolarità delle procedure telematiche. Con successivi decreti le regole tecnico-operative di cui al primo comma sono adeguate all'evoluzione scientifica e tecnologica. Se occorre, le medesime regole tecnico-operative sono integrate al fine di assicurare un agevole collegamento tra il portale delle vendite pubbliche e i portali dei gestori delle vendite telematiche.

Art. 161-quater.
(Modalità di pubblicazione sul portale delle vendite pubbliche)

La pubblicazione sul portale delle vendite pubbliche è effettuata a cura del professionista delegato per le operazioni di vendita o del commissionario o, in mancanza, del creditore pignorante o del creditore intervenuto munito di titolo esecutivo ed in conformità alle specifiche tecniche, che possono determinare anche i dati e i documenti da inserire. Le specifiche tecniche sono stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia entro sei mesi dalla data di entrata in vigore della presente disposizione e sono rese disponibili mediante pubblicazione nel portale delle vendite pubbliche. Quando la pubblicità riguarda beni immobili o beni mobili registrati, la pubblicazione non può essere effettuata in mancanza della prova dell'avvenuto pagamento del contributo per la pubblicazione, previsto dall'articolo 18-bis del decreto del Presidente della Repubblica 30 maggio 2002, n. 115.

Il portale delle vendite pubbliche deve inviare all'indirizzo di posta elettronica ordinaria o certificata, ad ogni interessato che ne ha fatto richiesta e si è registrato mediante un'apposita procedura disciplinata dalle specifiche tecniche di cui al primo comma, un avviso contenente le informazioni relative alle vendite di cui è stata effettuata la pubblicità.

Il portale delle vendite pubbliche provvede all'archiviazione e alla gestione dei dati relativi alle vendite in esso pubblicate.

Il mancato funzionamento dei sistemi informatici è attestato dal responsabile dei sistemi informativi automatizzati del Ministero della giustizia.

Art. 164-ter
(Inefficacia del pignoramento per mancato deposito della nota di iscrizione a ruolo)

Quando il pignoramento è divenuto inefficace per mancato deposito della nota di iscrizione a ruolo nel termine stabilito, il creditore entro cinque giorni dalla scadenza del termine ne fa dichiarazione al debitore e all'eventuale terzo, mediante atto notificato. In ogni caso ogni obbligo del debitore e del terzo cessa quando la nota di iscrizione a ruolo non è stata depositata nei termini di legge.

La cancellazione della trascrizione del pignoramento si esegue quando è ordinata giudizialmente ovvero quando il creditore pignorante dichiara, nelle forme richieste dalla legge, che il pignoramento è divenuto inefficace per mancato deposito della nota di iscrizione a ruolo nel termine stabilito.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Legge 21 gennaio 1994, n. 53 - Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali (ESTRATTO)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art.1.

1. L'avvocato o il procuratore legale, munito di procura alle liti a norma dell'art. 83 del codice di procedura civile e della autorizzazione del consiglio dell'ordine nel cui albo è iscritto a norma dell'art. 7 della presente legge, può eseguire la notificazione di atti in materia civile, amministrativa e stragiudiziale a mezzo del servizio postale, secondo le modalità previste dalla legge 20 novembre 1982, n. 890, salvo che l'autorità giudiziaria disponga che la notifica sia eseguita personalmente. Quando ricorrono i requisiti di cui al periodo precedente, fatta eccezione per l'autorizzazione del consiglio dell'ordine, la notificazione degli atti in materia civile, amministrativa e stragiudiziale può essere eseguita a mezzo di posta elettronica certificata.

Art. 2

(omissis)

Art. 3-bis.

1. La notificazione con modalità telematica si esegue a mezzo di posta elettronica certificata all'indirizzo risultante da pubblici elenchi, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. La notificazione può essere eseguita esclusivamente utilizzando un indirizzo di posta elettronica certificata del notificante risultante da pubblici elenchi.
2. Quando l'atto da notificarsi non consiste in un documento informatico, l'avvocato provvede ad estrarre copia informatica dell'atto formato su supporto analogico, attestandone la conformità con le modalità previste dall'articolo 16-undecies del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. La notifica si esegue mediante allegazione dell'atto da notificarsi al messaggio di posta elettronica certificata.[4]
3. La notifica si perfeziona, per il soggetto notificante, nel momento in cui viene generata la ricevuta di accettazione prevista dall'articolo 6, comma 1, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna prevista dall'articolo 6, comma 2, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
4. Il messaggio deve indicare nell'oggetto la dizione: «notificazione ai sensi della legge n. 53 del 1994».
5. L'avvocato redige la relazione di notificazione su documento informatico separato, sottoscritto con firma digitale ed allegato al messaggio di posta elettronica certificata. La relazione deve contenere:
a) il nome, cognome ed il codice fiscale dell'avvocato notificante;
b) (SOPPRESSO);
c) il nome e cognome o la denominazione e ragione sociale ed il codice fiscale della parte che ha conferito la procura alle liti;
d) il nome e cognome o la denominazione e ragione sociale del destinatario;
e) l'indirizzo di posta elettronica certificata a cui l'atto viene notificato;
f) l'indicazione dell'elenco da cui il predetto indirizzo è stato estratto;
g) l'attestazione di conformità di cui al comma 2.
6. Per le notificazioni effettuate in corso di procedimento deve, inoltre, essere indicato l'ufficio giudiziario, la sezione, il numero e l'anno di ruolo.

Art. 4

(*omissis*)

Art. 6.

1. L'avvocato o il procuratore legale, che compila la relazione o le attestazioni di cui agli articoli 3, 3-bis e 9 o le annotazioni di cui all'articolo 5, è considerato pubblico ufficiale ad ogni effetto.

[4] Le parole "attestandone la conformità con le modalità previste dall'articolo 16-undecies del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221" sono state inserite, in sede di conversione del d.l. 83/2015, dalla legge 132/2015.

2. Il compimento di irregolarità o abusi nell'esercizio delle facoltà previste dalla presente legge costituisce grave illecito disciplinare, indipendentemente dalla responsabilità prevista da altre norme.

Art. 7.

1. L'avvocato o il procuratore legale, che intende avvalersi delle facoltà previste dalla presente legge, deve essere previamente autorizzato dal consiglio dell'ordine nel cui albo è iscritto; tale autorizzazione potrà essere concessa esclusivamente agli avvocati o procuratori legali che non abbiano procedimenti disciplinari pendenti e che non abbiano riportato la sanzione disciplinare della sospensione dall'esercizio professionale o altra più grave sanzione e dovrà essere prontamente revocata in caso di irrogazione delle dette sanzioni ovvero, anche indipendentemente dall'applicazione di sanzioni disciplinari, in tutti i casi in cui il consiglio dell'ordine, anche in via cautelare, ritenga motivatamente inopportuna la prosecuzione dell'esercizio delle facoltà previste dalla presente legge.
2. Il provvedimento di rigetto o di revoca, emesso in camera di consiglio dopo aver sentito il professionista, è impugnabile davanti al Consiglio nazionale forense nel termine di dieci giorni solo per motivi di legittimità ed è immediatamente esecutivo, indipendentemente dalla sua eventuale impugnazione.
3. In caso di revoca dell'autorizzazione, l'avvocato o il procuratore legale consegna al consiglio dell'ordine il registro di cui all'art. 8, sul quale vengono annotati il provvedimento di revoca e l'eventuale annullamento del medesimo.
4. I provvedimenti del consiglio dell'ordine adottati ai sensi della presente legge sono resi pubblici nei modi più ampi.
4-bis. *Le* **disposizioni del presente articolo non si applicano alle notifiche effettuate a mezzo posta elettronica certificata.**

Art. 8

(*omissis*).

Art. 9

1. Nei casi in cui il cancelliere deve prendere nota sull'originale del provvedimento dell'avvenuta notificazione di un atto di opposizione o di impugnazione, ai sensi dell'art. 645 del codice di procedura civile[5] e dell'art. 123 delle disposizioni per l'attuazione, transitorie e di coordinamento del codice di procedura civile[6], il notificante provvede, contestualmente alla notifica, a depositare copia dell'atto notificato presso il cancelliere del giudice che ha pronunciato il provvedimento.
1-bis. Qualora non si possa procedere al deposito con modalità telematiche dell'atto notificato a norma dell'articolo 3-bis, l'avvocato estrae copia su supporto analogico del messaggio di posta elettronica certificata, dei suoi allegati e della ricevuta di accettazione e di avvenuta consegna e ne attesta la conformità ai documenti informatici da cui sono tratte ai sensi dell'articolo 23, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
1-ter. In tutti i casi in cui l'avvocato debba fornire prova della notificazione e non sia possibile fornirla con modalità telematiche, procede ai sensi del comma 1-bis.[7]

Art. 10.

1. Agli atti notificati ai sensi della presente legge è apposta, al momento dell'esibizione o del deposito nella relativa procedura, apposita marca, il cui modello e importo sono stabiliti con decreto del Ministro di grazia e giustizia. Quando l'atto è notificato a norma dell'art. 3–bis il pagamento dell'importo di cui al periodo precedente non è dovuto.
2. (omissis).

---

[5] Art. 645 c.p.c. Opposizione (*a decreto ingiuntivo*). 1. L'opposizione si propone davanti all'ufficio giudiziario al quale appartiene il giudice che ha emesso il decreto, con atto di citazione notificato al ricorrente nei luoghi di cui all'art. 638. **Contemporaneamente l'ufficiale giudiziario deve notificare avviso dell'opposizione al cancelliere affinché ne prenda nota sull'originale del decreto**. 2. In seguito all'opposizione il giudizio si svolge secondo le norme del procedimento ordinario davanti a giudice adito. L'anticipazione di cui all'articolo 163-bis, terzo comma, deve essere disposta fissando l'udienza per la comparizione delle parti non oltre trenta giorni dalla scadenza del termine minimo a comparire.

[6] Art. 123 disp. att. c.p.c. Avviso d'impugnazione alla cancelleria. 1. **L'ufficiale giudiziario che ha notificato un atto d'impugnazione deve darne immediatamente avviso scritto al cancelliere del giudice che ha pronunciato la sentenza impugnata**. 2. Il cancelliere deve fare annotazione dell'impugnazione sull'originale della sentenza.

[7] Comma inserito dalla legge n. 114/2014 in sede di conversione del d.l. 90/2014.

Articolo 11

1. Le notificazioni di cui alla presente legge sono nulle e la nullità è rilevabile d'ufficio, se mancano i requisiti soggettivi ed oggettivi ivi previsti, se non sono osservate le disposizioni di cui agli articoli precedenti e, comunque, se vi è incertezza sulla persona cui è stata consegnata la copia dell'atto o sulla data della notifica.

(ritorna all'indice cronologico) (*torna all'indice per argomenti*)

Legge 15 marzo 1997, n. 59 (in Suppl. ordinario n. 56, alla Gazz. Uff. 17 marzo, n. 63). Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (cd. Legge Bassanini 1) (ESTRATTO).

(ritorna all'indice cronologico)

(omissis)
CAPO II
(omissis)

Art. 15

1. (abrogato).
2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

D.P.R. 13 febbraio 2001, n. 123 - Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti (G.U. 17 aprile, n. 89)

(ritorna all'indice cronologico)
(torna all'Avvertenza)

Art. 1
Definizioni

1. Agli effetti del presente regolamento si intende per:
a) "documento informatico": la rappresentazione informatica del contenuto di atti, fatti o dati giuridicamente rilevanti ai sensi del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;
b) "duplicato del documento informatico": la riproduzione del documento informatico effettuata su un qualsiasi tipo di supporto elettronico facilmente trasportabile;
c) "documento probatorio": l'atto avente efficacia probatoria ai sensi del codice civile e del codice di procedura civile;
d) "firma digitale": il risultato della procedura informatica disciplinata dal decreto del Presidente della Repubblica 10 novembre 1997, n. 513;
e) "dominio giustizia": l'insieme delle risorse hardware e software, mediante il quale l'amministrazione della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura;
f) "sistema informatico civile": è il sottoinsieme delle risorse del dominio giustizia mediante il quale l'amministrazione della giustizia tratta il processo civile;
g) "gestore del sistema di trasporto delle informazioni": il gestore indicato dall'articolo 13, comma 2, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;
h) "indirizzo elettronico": l'indirizzo di posta elettronica come definito dall'articolo 1, comma 1, lettera l), del decreto del Presidente della Repubblica 10 novembre 1997, n. 513;
i) "ricevuta di consegna": il messaggio generato ed inviato automaticamente al mittente dal gestore del sistema di trasporto delle informazioni del destinatario nel momento in cui il messaggio inviato è reso disponibile al destinatario medesimo nella sua casella di posta elettronica;
j) "certificatore della firma digitale": il soggetto previsto dagli articoli 8, 9 e 17 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Art. 2
Campo di applicazione

1. É ammessa la formazione, la comunicazione e la notificazione di atti del processo civile mediante documenti informatici nei modi previsti dal presente regolamento.
2. L'attività di trasmissione, comunicazione o notificazione, dei documenti informatici è effettuata per via telematica attraverso il sistema informatico civile, fatto salvo quanto stabilito dall'articolo 6.
3. Si applicano le disposizioni del decreto del Presidente della Repubblica 10 novembre 1997, n. 513, ove non diversamente stabilito dal presente regolamento.

Art. 3
Sistema informatico civile

1. Il sistema informatico civile è strutturato con modalità che assicurano:
a) l'individuazione dell'ufficio giudiziario e del procedimento;
b) l'individuazione del soggetto che inserisce, modifica o comunica l'atto;
c) l'avvenuta ricezione della comunicazione dell'atto;
d) l'automatica abilitazione del difensore e dell'ufficiale giudiziario.
2. Al sistema informatico civile possono accedere attivamente soltanto i difensori delle parti e gli ufficiali giudiziari per le attività rispettivamente consentite dal presente regolamento.
3. Con decreto del Ministro della giustizia, sentita l'Autorità per l'informatica nella pubblica amministrazione, sono stabilite le regole tecnico-operative per il funzionamento e la gestione del sistema informatico civile, nonché per l'accesso dei difensori delle parti e degli ufficiali giudiziari. Con il medesimo decreto sono stabilite le regole tecnico-operative relative alla conservazione e all'archiviazione dei documenti informatici, conformemente alle prescrizioni di cui all'articolo 2, comma 15, della legge 24

dicembre 1993, n. 537, e all'articolo 18 del decreto del Presidente della Repubblica 10 novembre 1997, n. 513.

Art. 4
Atti e provvedimenti

1. Tutti gli atti e i provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale come espressamente previsto dal presente regolamento.
2. Se non è possibile procedere alla sottoscrizione nella forma di cui al comma 1, gli atti e i provvedimenti vengono redatti o stampati su supporto cartaceo, sottoscritti nei modi ordinari e allegati al fascicolo cartaceo. La copia informatica degli stessi è inserita nel fascicolo informatico con le modalità di cui agli articoli 12 e 13.
3. Ove dal presente regolamento non è espressamente prevista la sottoscrizione del documento informatico con la firma digitale, questa è sostituita dall'indicazione del nominativo del soggetto procedente prodotta sul documento dal sistema automatizzato, a norma dell'articolo 3, comma 2, del decreto legislativo 12 febbraio 1993, n. 39.

Art. 5
Processo verbale

1. Il processo verbale, redatto come documento informatico, è sottoscritto con firma digitale da chi presiede l'udienza e dal cancelliere. Nei casi in cui è richiesto, le parti e i testimoni procedono alla sottoscrizione delle dichiarazioni o del verbale apponendo la propria firma digitale.
2. Se non è possibile procedere alla sottoscrizione nella forma di cui al comma 1, il processo verbale viene redatto o stampato su supporto cartaceo, sottoscritto nei modi ordinari e allegato al fascicolo cartaceo. La copia informatica del processo verbale è allegata al fascicolo informatico con le modalità di cui agli articoli 12 e 13.

Art. 6
Comunicazioni e notificazione

1. Le comunicazioni con biglietto di cancelleria, nonché la notificazione degli atti, effettuata quest'ultima come documento informatico sottoscritto con firma digitale, possono essere eseguite per via telematica, oltre che attraverso il sistema informatico civile, anche all'indirizzo elettronico dichiarato ai sensi dell'articolo 7.
2. La parte che richiede la notificazione di un atto trasmette per via telematica l'atto medesimo all'ufficiale giudiziario, che procede alla notifica con le medesime modalità.
3. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, trae dall'atto ricevuto come documento informatico la copia su supporto cartaceo, ne attesta la conformità all'originale e provvede a notificare la copia stessa unitamente al duplicato del documento informatico, nei modi di cui agli articoli 138 e seguenti del codice di procedura civile.
4. Eseguita la notificazione, l'ufficiale giudiziario restituisce per via telematica l'atto notificato, munito della relazione della notificazione attestata dalla sua firma digitale.

(*torna all'indice per argomenti*)

(*leggi l'Avvertenza*)

Art. 7
Indirizzo elettronico

1. Ai fini delle comunicazioni e delle notificazioni ai sensi dell'articolo 6, l'indirizzo elettronico del difensore è unicamente quello comunicato dal medesimo al Consiglio dell'ordine e da questi reso disponibile ai sensi del comma 3 del presente articolo. Per gli esperti e gli ausiliari del giudice l'indirizzo elettronico è quello comunicato dai medesimi ai propri ordini professionali o all'albo dei consulenti presso il tribunale.
2. Per tutti i soggetti diversi da quelli indicati nel comma 1, l'indirizzo elettronico è quello dichiarato al certificatore della firma digitale al momento della richiesta di attivazione della procedura informatica di certificazione della firma digitale medesima, ove reso disponibile nel certificato.
3. Gli indirizzi elettronici di cui al comma 1, comunicati tempestivamente dagli ordini professionali al Ministero della giustizia, nonché quelli degli uffici giudiziari e degli uffici notifiche (UNEP), sono consultabili anche in via telematica secondo le modalità operative stabilite dal decreto di cui all'articolo 3, comma 3.

Art. 8
Attestazione temporale

1. La comunicazione e la notificazione si ha per eseguita alla data apposta dal notificatore alla ricevuta di consegna mediante la procedura di validazione temporale a norma del decreto del Presidente della Repubblica 10 novembre 1997, n. 513. Per la comunicazione e la notificazione eseguite dalla cancelleria e dall'ufficiale giudiziario la data riportata nella ricevuta di consegna tiene luogo della suddetta procedura di validazione temporale.
2. I dati relativi a quanto previsto dal comma 1, sono conservati dal notificatore per un periodo non inferiore a cinque anni secondo le modalità tecnico-operative stabilite dal decreto di cui all' articolo 3, comma 3.

Art. 9
Costituzione in giudizio e deposito

1. La parte che procede all'iscrizione a ruolo o alla costituzione in giudizio per via telematica trasmette con il medesimo mezzo i documenti probatori come documenti informatici o le copie informatiche dei documenti probatori su supporto cartaceo.

Art. 10
Procura alle liti

1. Se la procura alle liti è stata conferita su supporto cartaceo, il difensore, che si costituisce per via telematica, trasmette la copia informatica della procura medesima, asseverata come conforme all'originale mediante sottoscrizione con firma digitale.

Art. 11
Iscrizione a ruolo

1. La nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale.
2. La nota di iscrizione a ruolo trasmessa per via telematica è redatta in modo conforme al modello definito con il decreto di cui all'articolo 3, comma 3.

Art. 12
Fascicolo informatico

1. La cancelleria procede alla formazione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.
2. Nel fascicolo informatico sono inseriti, secondo le modalità di cui al comma 1, anche i documenti probatori offerti in comunicazione o prodotti dalle parti o comunque acquisiti al processo. Per i documenti probatori prodotti o comunque acquisiti su supporto cartaceo l'inserimento nel fascicolo informatico delle relative copie informatiche è effettuato dalla cancelleria, sempre che l'operazione non sia eccessivamente onerosa.
3. La formazione del fascicolo informatico non elimina l'obbligo di formazione del fascicolo d'ufficio su supporto cartaceo.

(*torna all'indice per argomenti*)

(leggi l'Avvertenza)

Art. 13
Formazione del fascicolo informatico

1. Ogni fascicolo informatico riceve la stessa numerazione del fascicolo cartaceo ed è formato secondo quanto stabilito dall'articolo 36 delle norme di attuazione del codice di procedura civile.
2. L'indice degli atti contiene anche l'indicazione dei documenti conservati solo nel fascicolo cartaceo ed è redatto in modo da consentire la diretta consultazione degli atti e dei documenti informatici.
3. Gli atti e i documenti probatori depositati dalle parti, contestualmente alla costituzione in giudizio o successivamente, sono inseriti in apposite sezioni del fascicolo informatico contenenti ciascuna l'indicazione del giudizio e della parte cui si riferiscono.
4. Ai sensi dell'articolo 12, comma 2, è eccessivamente onerosa l'estrazione della copia informatica di documenti probatori prodotti o acquisiti su supporto cartaceo, ai fini dell'inserimento nel fascicolo

informatico da parte della cancelleria, quando il formato del documento da copiare è diverso da quelli indicati con il decreto di cui all'articolo 3, comma 3, ovvero se il numero delle pagine da copiare è superiore a venti. Con il medesimo decreto il numero delle pagine è periodicamente aggiornato.
5. In deroga al comma 4 la cancelleria procede comunque all'estrazione della copia informatica di documenti probatori prodotti o acquisiti su supporto cartaceo quando la parte allega ad essi la copia su supporto informatico.
6. Il fascicolo informatico è consultabile dalla parte, oltre che in via telematica, anche nei locali della cancelleria attraverso un videoterminale.
7. Dopo la precisazione delle conclusioni il responsabile della cancelleria appone al fascicolo informatico la firma digitale.

(*torna all'indice per argomenti*)

(*leggi l'Avvertenza*)

Art. 14

Produzione degli atti e dei documenti probatori su supporto informatico

1. Gli atti e i documenti probatori offerti in comunicazione dalle parti dopo la costituzione in giudizio possono essere prodotti, oltre che per via telematica, anche mediante deposito in cancelleria del supporto informatico che li contiene. Il supporto informatico deve essere compatibile con i tipi e i modelli stabiliti al riguardo dal decreto di cui all'articolo 3, comma 3, e deve contenere anche il relativo indice, la cui integrità è attestata dal difensore con la firma digitale.
2. Il responsabile della cancelleria procede a duplicare nel fascicolo informatico gli atti, i documenti probatori e l'indice indicati nel comma 1.
3. Il supporto informatico è restituito alla parte dopo la duplicazione di cui al comma 2.

Art. 15

Deposito della relazione del C.T.U.

1. La relazione prevista dall'articolo 195 del codice di procedura civile può essere depositata per via telematica come documento informatico sottoscritto con firma digitale.
2. Con lo stesso mezzo devono essere allegati i documenti e le osservazioni delle parti o la copia informatica di questi ove gli originali sono stati prodotti su supporto cartaceo. In tal caso gli originali sono depositati dal consulente tecnico d'ufficio senza ritardo, in ogni caso prima dell'udienza successiva alla scadenza del termine per il deposito della relazione.
3. Il giudice, tenuto conto di un eventuale successivo utilizzo dei dati contenuti nella consulenza tecnica d'ufficio, può disporre che la relazione o parte di essa sia redatta in modo conforme a modelli definiti con il decreto di cui all'articolo 3, comma 3.

(*torna all'indice per argomenti*)

(*leggi l'Avvertenza*)

Art. 16

Trasmissione dei fascicoli

1. Qualora non sia necessario acquisire il fascicolo d'ufficio su supporto cartaceo, la trasmissione del fascicolo d'ufficio può avvenire, in ogni stato e grado, anche per via telematica con particolari modalità, stabilite con il decreto di cui all'articolo 3, comma 3, e dirette ad assicurarne l'integrità, l'autenticità e la riservatezza.
2. Prima dell'inoltro, il responsabile della cancelleria è tenuto a controllare che il contenuto del fascicolo d'ufficio su supporto cartaceo sia presente nel fascicolo informatico.

Art. 17

Trasmissione della sentenza

1. La trasmissione per via telematica della minuta della sentenza o della sentenza stessa, redatte come documenti informatici sottoscritti con firma digitale, è effettuata, ai sensi dell'articolo 119 delle norme di attuazione del codice di procedura civile, con particolari modalità stabilite con il decreto di cui all'articolo 3, comma 3, e dirette ad assicurarne l'integrità, l'autenticità e la riservatezza.
2. Il cancelliere, ai fini del deposito della sentenza ai sensi dell'articolo 133 del codice di procedura civile, sottoscrive la sentenza stessa con la propria firma digitale.

Art. 18

Informatizzazione del processo amministrativo e contabile[8]

1. Le disposizioni del presente regolamento si applicano, in quanto compatibili, anche al processo amministrativo e ai processi innanzi alle sezioni giurisdizionali della Corte dei conti.
2. Con decreti del Presidente del Consiglio dei Ministri, sentita l'Autorità per l'informatica nella pubblica amministrazione, sono stabilite le regole tecnico-operative per il funzionamento e la gestione del sistema informatico della giustizia amministrativa e contabile. I decreti sono adottati entro il termine di cui all'articolo 19, comma 2.

Art. 19
Disposizioni finali

1. Le disposizioni del presente regolamento si applicano ai giudizi iscritti a ruolo dopo il 1° gennaio 2002.
2. Il decreto ministeriale previsto dall'articolo 3, comma 3, è adottato entro il 30 ottobre 2001.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. é fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)

[8] Ai sensi dell'articolo 20-bis, comma 4, del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni, dalla L. 17 dicembre 2012, n. 221, le disposizioni di quest'articolo cessano di avere efficacia dalla data di cui al comma 3 del medesimo articolo 20-bis del D.L. 179/2012.

Decreto legislativo 30 giugno 2003, n. 196, Codice in Materia di Protezione dei Dati Personali (ESTRATTO)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Capo III - Informatica giuridica

Art. 51.
Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.
2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52
Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.
2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.
3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: "In caso di diffusione omettere le generalità e gli altri dati identificativi di....".
4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.
5. Fermo restando quanto previsto dall'articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.
6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 209 del Codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50, provvede in modo analogo in caso di richiesta di una parte.
7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

(ritorna all'indice cronologico)

D.P.R. 11 febbraio 2005 n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

ART. 1
Oggetto e definizioni

1. Il presente regolamento stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.
2. Ai fini del presente regolamento si intende per:
a) busta di trasporto, il documento informatico che contiene il messaggio di posta elettronica certificata;
b) Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: «CNIPA», l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
c) dati di certificazione, i dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata;
d) dominio di posta elettronica certificata, l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete;
e) log dei messaggi, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore;
f) messaggio di posta elettronica certificata, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
g) posta elettronica certificata, ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;
h) posta elettronica, un sistema elettronico di trasmissione di documenti informatici;
i) riferimento temporale, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
l) utente di posta elettronica certificata, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonché eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;
m) virus informatico, un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

ART.2
Soggetti del servizio di posta elettronica certificata

1. Sono soggetti del servizio di posta elettronica certificata:
a) il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
b) il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
c) il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

ART. 3
Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:
«1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.».

ART. 4
Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge.

2. [Abrogato]
3. [Abrogato]
4. [Abrogato]
5. Le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione della disponibilità, nonché le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17.
6. La validità della trasmissione e ricezione del messaggio di posta elettronica certificata è attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6.
7. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono di uno dei gestori di cui agli articoli 14 e 15.

ART. 5
Modalità della trasmissione e interoperabilità

1. Il messaggio di posta elettronica certificata inviato dal mittente al proprio gestore di posta elettronica certificata viene da quest'ultimo trasmesso al destinatario direttamente o trasferito al gestore di posta elettronica certificata di cui si avvale il destinatario stesso; quest'ultimo gestore provvede alla consegna nella casella di posta elettronica certificata del destinatario.
2. Nel caso in cui la trasmissione del messaggio di posta elettronica certificata avviene tra diversi gestori, essi assicurano l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

ART. 6
Ricevuta di accettazione e di avvenuta consegna

1. Il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata.
2. Il gestore di posta elettronica certificata utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna.
3. La ricevuta di avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.
4. La ricevuta di avvenuta consegna può contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.
5. La ricevuta di avvenuta consegna è rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.
6. La ricevuta di avvenuta consegna è emessa esclusivamente a fronte della ricezione di una busta di trasporto valida secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
7. Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

ART. 7
Ricevuta di presa in carico

1. Quando la trasmissione del messaggio di posta elettronica certificata avviene tramite più gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio.

ART. 8
Avviso di mancata consegna

1. Quando il messaggio di posta elettronica certificata non risulta consegnabile il gestore comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna tramite un avviso secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

ART. 9

Firma elettronica delle ricevute e della busta di trasporto

1. Le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute stesse secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
2. La busta di trasporto è sottoscritta con una firma elettronica di cui al comma 1 che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

(*torna all'indice per argomenti*)

ART. 10

Riferimento temporale

1. Il riferimento temporale e la marca temporale sono formati in conformità a quanto previsto dalle regole tecniche di cui all'articolo 17.
2. I gestori di posta elettronica certificata appongono un riferimento temporale su ciascun messaggio e quotidianamente una marca temporale sui log dei messaggi.

ART. 11

Sicurezza della trasmissione

1. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella busta di trasporto.
2. Durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi.
3. Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.
4. I gestori di posta elettronica certificata prevedono, comunque, l'esistenza di servizi di emergenza che in ogni caso assicurano il completamento della trasmissione ed il rilascio delle ricevute.

ART. 12

Virus informatici

1. Qualora il gestore del mittente riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.
2. Qualora il gestore del destinatario riceva messaggi con virus informatici è tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente, affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

ART. 13

Livelli minimi di servizio

1. I gestori di posta elettronica certificata sono tenuti ad assicurare il livello minimo di servizio previsto dalle regole tecniche di cui all'articolo 17.

ART. 14

Elenco dei gestori di posta elettronica certificata

1. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.
2. Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.

3. I richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro.
4. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione devono, inoltre, possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.
5. Non possono rivestire la carica di rappresentante legale, di componente del consiglio di amministrazione, di componente del collegio sindacale, o di soggetto comunque preposto all'amministrazione del gestore privato coloro i quali sono stati sottoposti a misure di prevenzione, disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, e della legge 31 maggio 1965, n. 575, e successive modificazioni, ovvero sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione, alla reclusione non inferiore ad un anno per delitti contro la pubblica amministrazione, in danno di sistemi informatici o telematici, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, ovvero per un delitto in materia tributaria.
6. Il richiedente deve inoltre:
a) dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;
b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;
c) rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 17;
d) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
e) utilizzare per la firma elettronica, di cui all'articolo 9, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;
f) adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;
g) prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;
h) fornire, entro i dodici mesi successivi all'iscrizione nell'elenco dei gestori di posta elettronica certificata, dichiarazione di conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti, relativa al processo di erogazione di posta elettronica certificata;
i) fornire copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.
7. Trascorsi novanta giorni dalla presentazione, la domanda si considera accolta qualora il CNIPA non abbia comunicato all'interessato il provvedimento di diniego.
8. Il termine di cui al comma 7 può essere interrotto una sola volta esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
9. Il procedimento di iscrizione nell'elenco dei gestori di posta elettronica certificata di cui al presente articolo può essere sospeso nei confronti dei soggetti per i quali risultano pendenti procedimenti penali per delitti in danno di sistemi informatici o telematici.
10. I soggetti di cui al comma 1 forniscono i dati, previsti dalle regole tecniche di cui all'articolo 17, necessari per l'iscrizione nell'elenco dei gestori.
11. Ogni variazione organizzativa o tecnica concernente il gestore ed il servizio di posta elettronica certificata è comunicata al CNIPA entro il quindicesimo giorno.
12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo è causa di cancellazione dall'elenco.
13. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1.

ART. 15
Gestori di posta elettronica certificata stabiliti nei Paesi dell'Unione europea

1. Può esercitare il servizio di posta elettronica certificata il gestore del servizio stabilito in altri Stati membri dell'Unione europea che soddisfi, conformemente alla legislazione dello Stato membro di stabilimento, formalità e requisiti equivalenti ai contenuti del presente decreto e operi nel rispetto delle regole tecniche di cui all'articolo 17. È fatta salva in particolare, la possibilità di avvalersi di gestori

stabiliti in altri Stati membri dell'Unione europea che rivestono una forma giuridica equipollente a quella prevista dall'articolo 14, comma 3.
2. Per i gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea il CNIPA verifica l'equivalenza ai requisiti ed alle formalità di cui al presente decreto e alle regole tecniche di cui all'articolo 17.

ART. 16
Disposizioni per le pubbliche amministrazioni

1. Le pubbliche amministrazioni possono svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata, oppure avvalersi dei servizi offerti da altri gestori pubblici o privati, rispettando le regole tecniche e di sicurezza previste dal presente regolamento.
2. L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata.
3. Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.
4. Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative.[9]

ART. 17
Regole tecniche

1. Il Ministro per l'innovazione e le tecnologie definisce, ai sensi dell'articolo 8, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sentito il Ministro per la funzione pubblica, le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi è acquisito il concerto del Ministro delle comunicazioni[10].

ART. 18
Disposizioni finali

1. (omissis)

(ritorna all'indice cronologico)

[9] Ma vedi il successivo art. 4 del d.l. 193/2009 che ha stabilito che nel processo civile e nel processo penale, tutte le comunicazioni e notificazioni per via telematica si effettuano [, nei casi consentiti], mediante posta elettronica certificata, ai sensi del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e delle regole tecniche stabilite con i decreti previsti dal comma 1.
[10] Per le regole tecniche c.f.r. Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie 2 novembre 2005)

Decreto legislativo 7 marzo 2005, n. 82. Codice dell'Amministrazione Digitale (CAD) (ESTRATTO)[11]

(ritorna all'indice cronologico)

CAPO I
PRINCIPI GENERALI
SEZIONE I
Sezione I
Definizioni, finalità e ambito di applicazione

Art.1
Definizioni

1. Ai fini del presente codice si intende per:
0a) AgID: l'Agenzia per l'Italia digitale di cui all'articolo 19 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134;
a) b) *(soppresse)*
c) carta d'identità elettronica: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;
d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;
e) f) g) h) i) *(soppresse)*
i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;
i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;
i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;
i-quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;
i-sexies) dati territoriali: i dati che attengono, direttamente o indirettamente, a una località o a un'area geografica specifica;
l) *(soppresso)*
l-bis) formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;
l-ter) dati di tipo aperto: i dati che presentano le seguenti caratteristiche:
1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;
3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36;
m), n) *(soppresse)*

[11] L'art. 61, co. 2, del D.lvo 26 agosto 2016, n. 179, in vigore dal 14 settembre 2016, ha previsto che "Al decreto legislativo n. 82 del 2005 sono apportate le seguenti modificazioni: a) le parole: «presente decreto», ovunque ricorrano, sono sostituite dalle seguenti: «presente Codice»; b) la parola: «DigitPA», ovunque ricorra, è sostituita dalla seguente: «AgID»; c) la rubrica del Capo VIII è sostituita dalla seguente: «Sistema pubblico di connettività» e la ripartizione in sezioni dello stesso Capo è abrogata; d) la parola «cittadino», ovunque ricorra, si intende come «persona fisica» e le espressioni «chiunque» e «cittadini e imprese», ovunque ricorrano, si intendono come «soggetti giuridici»".

n-bis) riutilizzo: uso del dato di cui all'articolo 2, comma 1, lettera e), del decreto legislativo 24 gennaio 2006, n. 36;
n-ter) domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Regolamento eIDAS", valido ai fini delle comunicazioni elettroniche aventi valore legale;
n-quater) servizio in rete o on-line: qualsiasi servizio di una amministrazione pubblica fruibile a distanza per via elettronica;
o) *(soppressa)*
p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;
q), q-bis), r) *(soppressi)*
s) firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
t), u) *(soppressi)*
u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;
u-ter) *(soppressi)*
u-quater) identità digitale: la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64;
v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
z) *(soppressa)*
aa) titolare di firma elettronica: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione nonché alle applicazioni per la sua apposizione della sua firma elettronica;
bb) *(soppressa)*
cc) titolare del dato: uno dei soggetti di cui all'articolo 2, comma 2, che ha originariamente formato per uso proprio o commissionato ad altro soggetto il documento che rappresenta il dato, o che ne ha la disponibilità;
dd) interoperabilità: caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;
ee) cooperazione applicativa: la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informatici dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi;
ff) Linee guida: le regole tecniche e di indirizzo adottate secondo il procedimento di cui all'articolo 71.
1-bis. Ai fini del presente Codice, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS;
1-ter. Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.

(*torna all'indice per argomenti*)

Art. 2
Finalità e ambito di applicazione

1. Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.
2. Le disposizioni del presente Codice si applicano:

a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165[12], nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;
b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b).
2-bis. *(abrogato)*
3. Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto.
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici e la fruibilità delle informazioni digitali si applicano anche agli organismi di diritto pubblico.
5. Le disposizioni del presente Codice si applicano nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196.
6. Le disposizioni del presente Codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile. Le disposizioni del presente Codice si applicano al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico.
6-bis. Ferma restando l'applicabilità delle disposizioni del presente decreto agli atti di liquidazione, rettifica, accertamento e di irrogazione delle sanzioni di natura tributaria, con decreto del Presidente del Consiglio dei ministri o del Ministro delegato, adottato su proposta del Ministro dell'economia e delle finanze, sono stabiliti le modalità e i termini di applicazione delle disposizioni del presente Codice alle attività e funzioni ispettive e di controllo fiscale.

SEZIONE II
Diritti dei cittadini e delle imprese

Art. 3
Carta della cittadinanza digitale

1. Chiunque ha il diritto di usare le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2, anche ai fini della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute.
1-bis. *(abrogato)*
1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.
1-quater. - 1-quinquies. - 1-sexies. *(abrogati)*

Art. 3bis
Identità digitale e Domicilio digitale

[12] L'articolo 1, comma 2, del d.lvo 30 marzo 2001, n. 165, così recita: "Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI".

01. Chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, lettere a) e b), tramite la propria identità digitale[13].
1. I soggetti di cui all'articolo 2, comma 2, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese hanno l'obbligo di dotarsi di un domicilio digitale iscritto nell'elenco di cui agli articoli 6-bis o 6-ter.
1-bis. Fermo restando quanto previsto al comma 1, chiunque ha facoltà di eleggere il proprio domicilio digitale da iscrivere nell'elenco di cui all'articolo 6-quater. Fatto salvo quanto previsto al comma 3-bis, chiunque ha la facoltà di richiedere la cancellazione del proprio domicilio digitale dall'elenco di cui all'articolo 6-quater.
1-ter. I domicili digitali di cui ai commi 1 e 1-bis sono eletti secondo le modalità stabilite con le Linee guida. Le persone fisiche possono altresì eleggere il domicilio digitale avvalendosi del servizio di cui all'articolo 64-bis.
1-quater. I soggetti di cui ai commi 1 e 1-bis hanno l'obbligo di fare un uso diligente del proprio domicilio digitale e di comunicare ogni modifica o variazione del medesimo secondo le modalità fissate nelle Linee guida.
2. (abrogato)
3. (abrogato)
3-bis. Con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per la semplificazione e la pubblica amministrazione, sentiti l'AgID e il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, è stabilita la data a decorrere dalla quale le comunicazioni tra i soggetti di cui all'articolo 2, comma 2, e coloro che non hanno provveduto a eleggere un domicilio digitale ai sensi del comma 1-bis, avvengono esclusivamente in forma elettronica. Con lo stesso decreto sono determinate le modalità con le quali ai predetti soggetti è messo a disposizione un domicilio digitale e sono individuate altre modalità con le quali, per superare il divario digitale, i documenti possono essere consegnati a coloro che non sono in grado di accedere direttamente a un domicilio digitale.
4. A decorrere dal 1° gennaio 2013, salvo i casi in cui è prevista dalla normativa vigente una diversa modalità di comunicazione o di pubblicazione in via telematica, le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con la persona fisica esclusivamente tramite il domicilio digitale dalla stessa dichiarato, anche ai sensi dell'articolo 21-bis della legge 7 agosto 1990, n. 241, senza oneri di spedizione a suo carico. Ogni altra forma di comunicazione non può produrre effetti pregiudizievoli per il destinatario. L'utilizzo di differenti modalità di comunicazione rientra tra i parametri di valutazione della performance dirigenziale ai sensi dell'articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.
4-bis. In assenza del domicilio digitale e fino alla data fissata nel decreto di cui al comma 3-bis, i soggetti di cui all'articolo 2, comma 2, possono predisporre le comunicazioni ai soggetti che non hanno eletto un domicilio digitale ai sensi del comma 1-bis come documenti informatici sottoscritti con firma digitale o firma elettronica qualificata o avanzata, da conservare nei propri archivi, ed inviare agli stessi, per posta ordinaria o raccomandata A.R., copia analogica di tali documenti sottoscritti con firma autografa, sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.
4-ter. Le disposizioni di cui al precedente comma soddisfano a tutti gli effetti di legge gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente laddove la copia analogica inviata al persona fisica contenga una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto ed è disponibile presso l'amministrazione in conformità alle Linee guida.
4-quater. Le modalità di predisposizione della copia analogica di cui al comma 4-bis e 4-ter soddisfano le condizioni di cui all'articolo 23, comma 2-bis, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.
4-quinquies. Il domicilio speciale di cui all'articolo 47 del Codice civile può essere eletto anche presso un domicilio digitale diverso da quello di cui al comma 1-ter. In tal caso, ferma restando la validità ai fini delle comunicazioni elettroniche aventi valore legale, colui che lo ha eletto non può opporre eccezioni relative alla forma e alla data della spedizione e del ricevimento delle comunicazioni o notificazioni ivi indirizzate.
5. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

(*torna all'indice per argomenti*)

[13] Comma inserito dal D.lvo 217/2017. L'art. 65 di questo decreto prevede che "Il diritto di cui all'articolo 3-bis, comma 01, è riconosciuto a decorrere dal 1° gennaio 2018".

Art.4

Partecipazione al procedimento amministrativo informatico

(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 5[14]

Effettuazione di pagamenti con modalità informatiche

1. I soggetti di cui all'articolo 2, comma 2, sono obbligati ad accettare, tramite la piattaforma di cui al comma 2, i pagamenti spettanti a qualsiasi titolo attraverso sistemi di pagamento elettronico, ivi inclusi, per i micro-pagamenti, quelli basati sull'uso del credito telefonico. Tramite la piattaforma elettronica di cui al comma 2, resta ferma la possibilità di accettare anche altre forme di pagamento elettronico, senza discriminazione in relazione allo schema di pagamento abilitato per ciascuna tipologia di strumento di pagamento elettronico come definita ai sensi dell'articolo 2, punti 33), 34) e 35) del regolamento UE 2015/751 del Parlamento europeo e del Consiglio del 29 aprile 2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

2. Al fine di dare attuazione al comma 1, l'AgID mette a disposizione, attraverso il Sistema pubblico di connettività, una piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, al fine di assicurare, attraverso gli strumenti di cui all'articolo 64, l'autenticazione dei soggetti interessati all'operazione in tutta la gestione del processo di pagamento[15].

2-bis. Ai sensi dell'articolo 71, e sentita la Banca d'Italia, sono determinate le modalità di attuazione del comma 1, inclusi gli obblighi di pubblicazione di dati e le informazioni strumentali all'utilizzo degli strumenti di pagamento di cui al medesimo comma.

2-ter. I soggetti di cui all'articolo 2, comma 2, consentono di effettuare pagamenti elettronici tramite la piattaforma di cui al comma 2 anche per il pagamento spontaneo di tributi di cui all'articolo 2-bis del decreto-legge 22 ottobre 2016, n. 193, convertito, con modificazioni dalla legge 1° dicembre 2016, n. 225.

2-quater. I prestatori di servizi di pagamento abilitati eseguono pagamenti a favore delle pubbliche amministrazioni attraverso l'utilizzo della piattaforma di cui al comma 2. Resta fermo il sistema dei versamenti unitari di cui all'articolo 17 e seguenti del decreto legislativo 9 luglio 1997, n. 241, Capo III, fino all'adozione di un decreto del Presidente del Consiglio dei ministri o del Ministro delegato, su proposta del Ministro dell'economia e delle finanze, di concerto con il Ministro del lavoro e delle politiche sociali, sentite l'Agenzia delle entrate e l'AgID, che fissa, anche in maniera progressiva, le modalità tecniche per l'effettuazione dei pagamenti tributari e contributivi tramite la piattaforma di cui al comma 2.[16]

2-quinquies. Tramite la piattaforma di cui al comma 2, le informazioni sui pagamenti sono messe a disposizione anche del Ministero dell'economia e delle finanze - Dipartimento Ragioneria generale dello Stato.

3. 3-bis. 3-ter. *(abrogati)*

4. L'Agenzia per l'Italia digitale, sentita la Banca d'Italia, definisce linee guida per la specifica dei codici identificativi del pagamento di cui al comma 1 e le modalità attraverso le quali il prestatore dei servizi di pagamento mette a disposizione dell' ente le informazioni relative al pagamento medesimo.

5. Le attività previste dal presente articolo si svolgono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

---

[14] Il D.L. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, ha disposto (con l'art. 8, comma 1) che "Ai fini dell'attuazione degli obiettivi di cui all'Agenda digitale italiana anche in coerenza con gli obiettivi dell'Agenda digitale europea, la gestione della piattaforma di cui all'articolo 5, comma 2, del decreto legislativo 7 marzo 2005, n. 82, nonché i compiti, relativi a tale piattaforma, svolti dall'Agenzia per l'Italia digitale, sono trasferiti alla Presidenza del Consiglio dei ministri che a tal fine si avvale, se nominato, del Commissario straordinario di cui all'articolo 63, comma 1, del decreto legislativo 26 agosto 2016, n. 179".

[15] Il D.Lgs. 13 dicembre 2017, n. 217, come modificato dal D.L. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, ha disposto (con l'art. 65, comma 2) che "L'obbligo per i prestatori di servizi di pagamento abilitati di utilizzare esclusivamente la piattaforma di cui all'articolo 5, comma 2, del decreto legislativo n. 82 del 2005 per i pagamenti verso le pubbliche amministrazioni decorre dal 31 dicembre 2019".

[16] Ai sensi dell'art. 65, co. 3, del D.lvo 217/2017 "il decreto del Presidente del Consiglio dei ministri di cui all'articolo 5, comma 2-quater, del decreto legislativo n. 82 del 2005, come introdotto dal presente decreto, è adottato entro centottanta giorni dalla data di entrata in vigore del presente decreto".

(*torna all'indice per argomenti*)

Art. 5-bis
Comunicazioni tra imprese e amministrazioni pubbliche

(*omissis*)

Art. 6
Utilizzo del domicilio digitale

1. Le comunicazioni tramite i domicili digitali sono effettuate agli indirizzi inseriti negli elenchi di cui agli articoli 6-bis, 6-ter e 6-quater, o a quello eletto come domicilio speciale per determinati atti o affari ai sensi dell'articolo 3-bis, comma 4-quinquies. Le comunicazioni elettroniche trasmesse ad uno dei domicili digitali di cui all'articolo 3-bis producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente. Le suddette comunicazioni si intendono spedite dal mittente se inviate al proprio gestore e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo. La data e l'ora di trasmissione e ricezione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.
1-bis. *(abrogato)*
1-ter. L'elenco dei domicili digitali delle imprese e dei professionisti è l'Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti di cui all'articolo 6-bis. L'elenco dei domicili digitali dei soggetti di cui all'articolo 2, comma 2, lettere a) e b), è l'Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi, di cui all'articolo 6-ter. L'elenco dei domicili digitali delle persone fisiche e degli altri enti di diritto privato diversi da quelli di cui al primo e al secondo periodo è l'Indice degli indirizzi delle persone fisiche e degli altri enti di diritto privato di cui all'articolo 6-quater.
1-quater. I soggetti di cui all'articolo 2, comma 2, notificano direttamente presso i domicili digitali di cui all'articolo 3-bis i propri atti, compresi i verbali relativi alle sanzioni amministrative, gli atti impositivi di accertamento e di riscossione e le ingiunzioni di cui all'articolo 2 del regio decreto 14 aprile 1910, n. 639, fatte salve le specifiche disposizioni in ambito tributario. La conformità della copia informatica del documento notificato all'originale è attestata dal responsabile del procedimento in conformità a quanto disposto agli articoli 22 e 23-bis.
2. *(abrogato)*
2-bis. *(abrogato)*

(*torna all'indice per argomenti*)

Art. 6-bis
Indice nazionale dei domicili digitali delle imprese e dei professionisti

1. Al fine di favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra i soggetti di cui all'articolo 2, comma 2 e le imprese e i professionisti in modalità telematica, è istituito, il pubblico elenco denominato Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.
2. L'Indice nazionale di cui al comma 1 è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, in attuazione di quanto previsto dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2. I domicili digitali inseriti in tale Indice costituiscono mezzo esclusivo di comunicazione e notifica con i soggetti di cui all'articolo 2, comma 2.
2-bis. L'INI-PEC acquisisce dagli ordini e dai collegi professionali gli attributi qualificati dell'identità digitale ai fini di quanto previsto dal decreto di cui all'articolo 64, comma 2-sexies.
3. *(abrogato)*
4. Il Ministero per lo sviluppo economico, al fine del contenimento dei costi e dell'utilizzo razionale delle risorse, sentita l'Agenzia per l'Italia Digitale, si avvale per la realizzazione e gestione operativa dell'Indice nazionale di cui al comma 1 delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce con proprio regolamento, da emanare entro 60 giorni dalla data di entrata in vigore del presente Codice, le modalità di accesso e di aggiornamento.
5. Nel regolamento di cui al comma 4 sono anche definite le modalità e le forme con cui gli ordini e i collegi professionali comunicano all'Indice nazionale di cui al comma 1 tutti gli indirizzi PEC relativi ai professionisti di propria competenza e sono previsti gli strumenti telematici resi disponibili dalle Camere

di commercio per il tramite delle proprie strutture informatiche al fine di ottimizzare la raccolta e aggiornamento dei medesimi indirizzi.
6. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

(*torna all'indice per argomenti*)
(***torna all'art. 16ter d.l. 179 del 2012***)

Art. 6-ter[17]

Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi

1. Al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è istituito il pubblico elenco di fiducia denominato "Indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi", nel quale sono indicati i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.
2. La realizzazione e la gestione dell'Indice sono affidate all'AgID, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.
3. Le amministrazioni di cui al comma 1 e i gestori di pubblici servizi aggiornano gli indirizzi e i contenuti dell'Indice tempestivamente e comunque con cadenza almeno semestrale, secondo le indicazioni dell'AgID. La mancata comunicazione degli elementi necessari al completamento dell'Indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

(*torna all'indice per argomenti*)

Art. 6-quater.

Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese

1. è istituito il pubblico elenco dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese, nel quale sono indicati i domicili eletti ai sensi dell'articolo 3-bis, comma 1-bis. La realizzazione e la gestione dell'Indice sono affidate all'AgID, che vi provvede avvalendosi delle strutture informatiche delle Camere di commercio già deputate alla gestione dell'elenco di cui all'articolo 6-bis.
2. Per i professionisti iscritti in albi ed elenchi il domicilio digitale è l'indirizzo inserito nell'elenco di cui all'articolo 6-bis, fermo restando il diritto di eleggerne uno diverso ai sensi dell'articolo 3-bis, comma 1-bis. Ai fini dell'inserimento dei domicili dei professionisti nel predetto elenco il Ministero dello sviluppo economico rende disponibili all'AgID, tramite servizi informatici individuati nelle Linee guida, i relativi indirizzi già contenuti nell'elenco di cui all'articolo 6-bis.[18]
3. Al completamento dell'ANPR di cui all'articolo 62, AgID provvede al trasferimento dei domicili digitali contenuti nell'elenco di cui al presente articolo nell'ANPR.

(*torna all'indice per argomenti*)
(***torna all'art. 16ter d.l. 179 del 2012***)

[17] L'art. 66, co. 6, del D.lvo 217/2017 ha stabilito che "Con decreto del Presidente del Consiglio dei ministri o del Ministro delegato, di concerto con il Ministro della giustizia, sono stabiliti le modalità e i tempi per la confluenza dell'elenco di cui all'articolo 16, comma 12, del decreto-legge n. 179 del 2012 in una sezione speciale dell'elenco di cui all'articolo 6-ter del decreto legislativo n. 82 del 2005, consultabile esclusivamente dagli uffici giudiziari, dagli uffici notificazioni, esecuzioni e protesti e dagli avvocati. Con il medesimo decreto sono altresì stabilite le modalità con le quali le pubbliche amministrazioni che non risultino già iscritte nell'elenco di cui all'articolo 16, comma 12, del decreto-legge n. 179 del 2012, comunicano l'indirizzo di posta elettronica certificata da inserire nella sezione speciale di cui al presente comma. A decorrere dalla data fissata nel suddetto decreto, ai fini di cui all'articolo 16-ter del decreto-legge n. 179 del 2012, si intende per pubblico elenco anche la predetta sezione dell'elenco di cui all'articolo 6-ter del decreto legislativo n. 82 del 2005".

[18] L'art. 65 del D.lvo 217/2017 stabilisce al riguardo che "(omissis) 4. La realizzazione dell'indice di cui all'articolo 6-quater del decreto legislativo n. 82 del 2005, è effettuata dall'AgID entro dodici mesi dall'entrata in vigore del presente decreto. AgID cessa la gestione del predetto elenco al completamento dell'ANPR, ai sensi dell'articolo 6-quater, comma 3, del decreto legislativo n. 82 del 2005, come modificato dal presente decreto. 5. In sede di prima applicazione dell'articolo 6-quater, comma 2, del decreto legislativo n. 82 del 2005, AgID comunica alle imprese e ai professionisti che, alla data di entrata in vigore del presente decreto, risultano iscritti in albi ed elenchi, tramite l'indirizzo di cui all'articolo 6-bis del suddetto decreto, l'inserimento dello stesso indirizzo nell'elenco di cui all'articolo 6-quater del medesimo decreto. Entro trenta giorni l'interessato può comunicare il proprio dissenso ovvero indicare un indirizzo diverso".

Art. 6-quinquies.
Consultazione e accesso

1. La consultazione on-line degli elenchi di cui agli articoli 6-bis, 6-ter e 6-quater è consentita a chiunque senza necessità di autenticazione. Gli elenchi sono realizzati in formato aperto.
2. L'estrazione dei domicili digitali dagli elenchi, di cui agli articoli 6-bis, 6-ter e 6-quater, è effettuata secondo le modalità fissate da AgID nelle Linee guida.
3. In assenza di preventiva autorizzazione del titolare dell'indirizzo, è vietato l'utilizzo dei domicili digitali di cui al presente articolo per finalità diverse dall'invio di comunicazioni aventi valore legale o comunque connesse al conseguimento di finalità istituzionali dei soggetti di cui all'articolo 2, comma 2.
4. Gli elenchi di cui agli articoli 6-bis, 6-ter e 6-quater contengono le informazioni relative alla elezione, modifica o cessazione del domicilio digitale.

Art. 7
Qualità dei servizi resi e soddisfazione dell'utenza

(omissis)

Art. 8
Alfabetizzazione informatica dei cittadini

1. Lo Stato e i soggetti di cui all'articolo 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo.

Art. 8-bis
Connettività alla rete Internet negli uffici e luoghi pubblici

1. I soggetti di cui all'articolo 2, comma 2, favoriscono, in linea con gli obiettivi dell'Agenda digitale europea, la disponibilità di connettività alla rete Internet presso gli uffici pubblici e altri luoghi pubblici, in particolare nei settori scolastico, sanitario e di interesse turistico, anche prevedendo che la porzione di banda non utilizzata dagli stessi uffici sia messa a disposizione degli utenti nel rispetto degli standard di sicurezza fissati dall'Agid.
2. I soggetti di cui all'articolo 2, comma 2, mettono a disposizione degli utenti connettività a banda larga per l'accesso alla rete Internet nei limiti della banda disponibile e con le modalità determinate dall'AgID.[19]

Art. 9
Partecipazione democratica elettronica

(omissis)

Art. 10
Sportello unico per le attività produttive
(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)

Art. 11
Registro informatico degli adempimenti amministrativi per le imprese
(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)

SEZIONE III
Organizzazione delle pubbliche amministrazioni Rapporti fra Stato, Regioni e autonomie locali

[19] Ai sensi dell'art. 62, co. 3, del D.Lvo 26 agosto 2016, n. 179, "l'AgID definisce i limiti e le modalità di applicazione dell'articolo 8-bis, comma 2, del decreto legislativo n. 82 del 2005, introdotto dall'articolo 9 del presente decreto entro centottanta giorni dall'entrata in vigore del presente decreto".

Art. 12
Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa

1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese di cui al presente Codice in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui all'articolo 14-bis, comma 2, lettera b).
1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150, dettano disposizioni per l'attuazione delle disposizioni del presente Codice.
1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente Codice ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente Codice è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.
2. Le pubbliche amministrazioni utilizzano, nei rapporti interni, in quelli con altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche di cui all'articolo 71.
3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici , ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.
3-bis. I soggetti di cui all'articolo 2, comma 2, favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.
4. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
5. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
5-bis. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 13
Formazione informatica dei dipendenti pubblici

1. Le pubbliche amministrazioni, nell'ambito delle risorse finanziarie disponibili, attuano politiche di reclutamento e formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistive, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4.
1-bis. Le politiche di formazione di cui al comma 1 sono altresì volte allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali dei dirigenti, per la transizione alla modalità operativa digitale.

Art. 14
Rapporti tra Stato, Regioni e autonomie locali

(omissis)

Art. 14-bis
Agenzia per l'Italia digitale

1. L'Agenzia per l'Italia Digitale (AgID) è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato, e con l'Agenda digitale europea. AgID, in particolare, promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione e nel rapporto tra questa, i cittadini e le imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia. Essa presta la propria collaborazione alle istituzioni

dell'Unione europea e svolge i compiti necessari per l'adempimento degli obblighi internazionali assunti dallo Stato nelle materie di competenza.
2. AgID svolge le funzioni di:
a) emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea;
b) programmazione e coordinamento delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante la redazione e la successiva verifica dell'attuazione del Piano triennale per l'informatica nella pubblica amministrazione contenente la fissazione degli obiettivi e l'individuazione dei principali interventi di sviluppo e gestione dei sistemi informativi delle amministrazioni pubbliche. Il predetto Piano è elaborato dall'AgID, anche sulla base dei dati e delle informazioni acquisiti dai soggetti di cui all'articolo 2, comma 2, ed è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato entro il 30 settembre di ogni anno;
c) monitoraggio delle attività svolte dalle amministrazioni, ivi inclusi gli investimenti effettuati ai sensi dell'articolo 1, comma 492, lettera a-bis), della legge 11 dicembre 2016, n. 232, in relazione alla loro coerenza con il Piano triennale di cui alla lettera b) e verifica dei risultati conseguiti dalle singole amministrazioni con particolare riferimento ai costi e benefici dei sistemi informatici secondo le modalità fissate dalla stessa Agenzia;
d) predisposizione, realizzazione e gestione di interventi e progetti di innovazione, anche realizzando e gestendo direttamente o avvalendosi di soggetti terzi, specifici progetti in tema di innovazione ad essa assegnati nonché svolgendo attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale, anche a carattere intersettoriale;
e) promozione della cultura digitale e della ricerca anche tramite comunità digitali regionali;
f) rilascio di pareri tecnici, obbligatori e non vincolanti, sugli schemi di contratti e accordi quadro da parte delle pubbliche amministrazioni centrali concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati per quanto riguarda la congruità tecnico-economica, qualora il valore lordo di detti contratti sia superiore a euro 1.000.000,00 nel caso di procedura negoziata e a euro 2.000.000,00 nel caso di procedura ristretta o di procedura aperta. Il parere è reso tenendo conto dei principi di efficacia, economicità, ottimizzazione della spesa delle pubbliche amministrazioni e favorendo l'adozione di infrastrutture condivise e standard che riducano i costi sostenuti dalle singole amministrazioni e il miglioramento dei servizi erogati, nonché in coerenza con i principi, i criteri e le indicazioni contenuti nei piani triennali approvati. Il parere è reso entro il termine di quarantacinque giorni dal ricevimento della relativa richiesta. Si applicano gli articoli 16 e 17-bis della legge 7 agosto 1990, n. 241, e successive modificazioni. Copia dei pareri tecnici attinenti a questioni di competenza dell'Autorità nazionale anticorruzione è trasmessa dall'AgID a detta Autorità;
g) rilascio di pareri tecnici, obbligatori e vincolanti, sugli elementi essenziali delle procedure di gara bandite, ai sensi dell'articolo 1, comma 512 della legge 28 dicembre 2015, n. 208, da Consip e dai soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66, concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e definiti di carattere strategico nel piano triennale. Il parere è reso entro il termine di quarantacinque giorni dal ricevimento della relativa richiesta e si applica l'articolo 17-bis della legge 7 agosto 1990, n. 241, e successive modificazioni. Ai fini della presente lettera per elementi essenziali si intendono l'oggetto della fornitura o del servizio, il valore economico del contratto, la tipologia di procedura che si intende adottare, il criterio di aggiudicazione e relativa ponderazione, le principali clausole che caratterizzano le prestazioni contrattuali. Si applica quanto previsto nei periodi da 2 a 5 della lettera f);
h) definizione di criteri e modalità per il monitoraggio sull'esecuzione dei contratti da parte dell'amministrazione interessata ovvero, su sua richiesta, da parte della stessa AgID;
i) vigilanza sui servizi fiduciari ai sensi dell'articolo 17 del regolamento UE 910/2014 in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui conservatori di documenti informatici accreditati, nonché sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza;
l) ogni altra funzione attribuitale da specifiche disposizioni di legge e dallo Statuto.

3. Fermo restando quanto previsto al comma 2, AgID svolge ogni altra funzione prevista da leggi e regolamenti già attribuita a AgID, all'Agenzia per la diffusione delle tecnologie per l'innovazione nonché al Dipartimento per l'innovazione tecnologica della Presidenza del Consiglio dei ministri.

Art. 15
Digitalizzazione e riorganizzazione

(omissis)

Art. 16
Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie

(omissis)

Art. 17
Responsabile per la transizione digitale e difensore civico digitale

(omissis).

Art. 18
Piattaforma nazionale per la governance della trasformazione digitale

(omissis)

Art. 19
Banca dati per la legislazione in materia di pubblico impiego

(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)

CAPO II
DOCUMENTO INFORMATICO, FIRME ELETTRONICHE, SERVIZI FIDUCIARI E TRASFERIMENTI DI FONDI

SEZIONE I
Documento informatico

Art. 20
Validità ed efficacia probatoria dei documenti informatici

1. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.

1-ter. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.

1-quater. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico.

2. COMMA ABROGATO DAL D.LGS. 30 DICEMBRE 2010, N. 235.

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica , sono stabilite con le Linee guida.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle Linee guida.

(*torna all'indice per argomenti*)

Art. 21
Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale.

1. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
2. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
2-bis. Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, primo comma, n. 13, del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo. [20]
2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110[21], ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.
3. - 4. (COMMI ABROGATI DAL D.LGS 26 AGOSTO 2016, N. 179).
5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

(*torna all'indice per argomenti*)

Art. 22
Copie informatiche di documenti analogici

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se sono formati ai sensi dell'articolo 20, comma 1-bis, primo periodo. La loro esibizione e produzione sostituisce quella dell'originale.
1-bis. La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.
2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le Linee guida.

---

[20] Art. 1350 c.c. (Atti che devono farsi per iscritto): "Devono farsi per atto pubblico o per scrittura privata, sotto pena di nullità: 1) i contratti che trasferiscono la proprietà di beni immobili; 2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta; 3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti; 4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione; 5) gli atti di rinunzia ai diritti indicati dai numeri precedenti; 6) i contratti di affrancazione del fondo enfiteutico; 7) i contratti di anticresi; 8) i contratti di locazione di beni immobili per una durata superiore a nove anni; 9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato; 10) gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato; 11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari; 12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti; 13) gli altri atti specialmente indicati dalla legge".

[21] Il D.lvo n. 110/2010 reca "disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'articolo 65 della legge 18 giugno 2009, n. 69".

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle Linee guida hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.
4. Le copie formate ai sensi dei commi 1, 1-bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.
5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.
6. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

(*torna all'indice per argomenti*)

Art. 23
Copie analogiche di documenti informatici

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.
2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.
2-bis. Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le Linee guida, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I soggetti che procedono all'apposizione del contrassegno rendono disponibili gratuitamente sul proprio sito Internet istituzionale idonee soluzioni per la verifica del contrassegno medesimo.

(*torna all'indice per argomenti*)

Art. 23bis
Duplicati e copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle Linee guida.
2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti Linee guida, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

(*torna all'indice per argomenti*)

Art. 23ter
Documenti amministrativi informatici

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
1-bis. La copia su supporto informatico di documenti formati dalle pubbliche amministrazioni in origine su supporto analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto identico a quello del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.
2. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò

delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle Linee guida; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.
4. In materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, le Linee guida sono definite anche sentito il Ministero dei beni e delle attività culturali e del turismo.
5. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
5-bis. I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4.
6. Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22 , 23 e 23-bis .

Art. 23quater
Riproduzioni informatiche

1. All'articolo 2712 del codice civile dopo le parole: "riproduzioni fotografiche" è inserita la seguente: ", informatiche".[22]

SEZIONE II
Firme elettroniche, certificati e prestatori di servizi fiduciari

Art. 24
Firma digitale

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le Linee guida, la validità del certificato stesso, nonché gli elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso. Le linee guida definiscono altresì le modalità, anche temporali, di apposizione della firma.
4-bis. L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione, salvo che lo stato di sospensione sia stato annullato. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4-ter. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
a) il certificatore possiede i requisiti previsti dal regolamento eIDAS ed è qualificato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui al medesimo regolamento;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

(*torna all'indice per argomenti*)

Art. 25
Firma autenticata

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato[23].

[22] Art. 2712 c.c. (Riproduzioni meccaniche): "Le riproduzioni fotografiche, *informatiche* o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime".
[23] Art. 2703 c.c. (Sottoscrizione autenticata): "Si ha per riconosciuta la sottoscrizione autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. L'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la

2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.
3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

(*torna all'indice per argomenti*)

Art. 26
Certificatori

(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 27
Certificatori qualificati

(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 28
Certificati di firma elettronica qualificata[24]

1. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
2. In aggiunta alle informazioni previste nel Regolamento eIDAS nel certificato di firma elettronica qualificata può essere inserito il codice fiscale. Per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si può indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo univoco.
3. Il certificato di firma elettronica qualificata può contenere, ove richiesto dal titolare di firma elettronica o dal terzo interessato, le seguenti informazioni, se pertinenti e non eccedenti rispetto allo scopo per il quale il certificato è richiesto:
a) le qualifiche specifiche del titolare di firma elettronica, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3;
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili;
c-bis) uno pseudonimo, qualificato come tale.
3-bis. Le informazioni di cui al comma 3 sono riconoscibili da parte dei terzi e chiaramente evidenziati nel certificato. Le informazioni di cui al comma 3 possono anche essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con le Linee guida sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali.
4. Il titolare di firma elettronica, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.
4-bis. Il certificatore ha l'obbligo di conservare le informazioni di cui ai commi 3 e 4 per almeno venti anni decorrenti dalla scadenza del certificato di firma.

---

sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive".

[24] Ai sensi dell'art. 62, co. 4, del D.lvo 26 agosto 2016, n. 179, "i certificati qualificati rilasciati prima dell'entrata in vigore del presente decreto a norma della direttiva 1999/93/CE, sono considerati certificati qualificati di firma elettronica a norma del regolamento eIDAS e dell'articolo 28 del decreto legislativo n. 82 del 2005, come modificato dall'articolo 24 del presente decreto, fino alla loro scadenza".

Art. 29[25]

Qualificazione e accreditamento

1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale di cui all'articolo 64 presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida. I soggetti che intendono svolgere l'attività di conservatore di documenti informatici presentano all'AgID domanda di accreditamento, secondo le modalità fissate dalle Linee guida.
2. Il richiedente deve trovarsi nelle condizioni previste dall'articolo 24 del Regolamento eIDAS, deve avere natura giuridica di società di capitali e deve disporre dei requisiti di onorabilità, tecnologici e organizzativi, nonché delle garanzie assicurative e di eventuali certificazioni, adeguate rispetto al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. I predetti requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei ministri, sentita l'AgID. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche.[26]
3. *(abrogato)*
4. La domanda di qualificazione o di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità dell'AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
6. A seguito dell'accoglimento della domanda, il AgID dispone l'iscrizione del richiedente in un apposito elenco pubblico di fiducia, tenuto dal AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
7. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
8. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse dell'AgID, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 30

Responsabilità dei prestatori di servizi fiduciari qualificati, dei gestori di posta elettronica certificata, dei gestori dell'identità digitale e di conservatori

1. I prestatori di servizi fiduciari qualificati, i gestori di posta elettronica 1. I prestatori di servizi fiduciari qualificati, i gestori di posta elettronica certificata, i gestori dell'identità digitale e i conservatori di documenti informatici, iscritti nell'elenco di cui all'articolo 29, comma 6, che cagionano danno ad altri nello svolgimento della loro attività, sono tenuti al risarcimento, se non provano di avere adottato tutte le misure idonee a evitare il danno.
2. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

---

[25] Ai sensi dell'art. 65, co. 7, del D.lvo 217/2017, come modificato dal d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, è stato previsto che "Con decreto del Presidente del Consiglio dei ministri, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali, sono adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certificata di cui agli articoli 29 e 48 del decreto legislativo del 7 marzo 2005, n. 82, al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. A far data dall'entrata in vigore del decreto di cui al primo periodo, l'articolo 48 del decreto legislativo n. 82 del 2005 è abrogato".

[26] L'art. 65 del D.lvo 217/2017 prevede al comma 8 che "il decreto del Presidente del Consiglio dei ministri di cui all'articolo 29, comma 2, del decreto legislativo n. 82 del 2005, come modificato dal presente decreto, è adottato entro centottanta giorni dalla data di entrata in vigore del presente decreto. Fino all'adozione del predetto decreto, restano efficaci le disposizioni dell'articolo 29, comma 3, dello stesso decreto nella formulazione previgente all'entrata in vigore del decreto legislativo 26 agosto 2016, n. 179 e dell'articolo 44-bis, commi 2 e 3, del decreto legislativo n. 82 del 2005 nella formulazione previgente all'entrata in vigore del presente decreto".

3. Il prestatore di servizi di firma digitale o di altra firma elettronica qualificata non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti eventualmente ai sensi dell'articolo 28, comma 3, a condizione che limiti d'uso e di valore siano chiaramente riconoscibili secondo quanto previsto dall'articolo 28, comma 3-bis posti dallo stesso o derivanti dal superamento del valore limite.

Art. 31

Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata.

(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 32

Obblighi del titolare e del prestatore di servizi di firma elettronica qualificata

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il prestatore di servizi di firma elettronica qualificata è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il prestatore di servizi di firma elettronica qualificata che rilascia certificati qualificati deve comunque:

a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;

b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle Linee guida, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle Linee guida;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

f) *(abrogato)*

g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare di firma elettronica qualificata o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare di firma elettronica qualificata, di sospetti abusi o falsificazioni, secondo quanto previsto dalle Linee guida;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.
4. Il prestatore di servizi di firma elettronica qualificata è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il prestatore di servizi di firma elettronica qualificata raccoglie i dati personali direttamente dalla persona cui si riferiscono o, previo suo esplicito consenso, tramite il terzo, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

(*torna all'indice per argomenti*)

Art. 32bis
Sanzioni per i prestatori di servizi fiduciari qualificati, per i gestori di posta elettronica certificata, per i gestori dell'identità digitale e per i conservatori

1. L'AgID può irrogare ai prestatori di servizi fiduciari qualificati, ai gestori di posta elettronica certificata, ai gestori dell'identità digitale e ai conservatori accreditati, che abbiano violato gli obblighi del Regolamento eIDAS o del presente Codice «relative alla prestazione dei predetti servizi, sanzioni amministrative in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza, per importi da un minimo di euro 40.000,00 a un massimo di euro 400.000,00, fermo restando il diritto al risarcimento del maggior danno. Le violazioni del presente Codice idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio si considerano gravi. AgID, laddove accerti tali gravi violazioni, dispone altresì la cancellazione del fornitore del servizio dall'elenco dei soggetti qualificati e il divieto di accreditamento o qualificazione per un periodo fino ad un massimo di due anni. Le sanzioni vengono irrogate dal direttore generale dell'AgID, sentito il Comitato di indirizzo. Si applica, in quanto compatibile, la disciplina della legge 24 novembre 1981, n. 689.
1-bis. L'AgID irroga la sanzione amministrativa di cui al comma 1 e diffida i soggetti a conformare la propria condotta agli obblighi previsti dalla disciplina vigente.
2. Fatti salvi i casi di forza maggiore o di caso fortuito, qualora si verifichi un malfunzionamento nei servizi forniti dai soggetti di cui al comma 1 che determini l'interruzione del servizio, ovvero in caso di mancata o intempestiva comunicazione dello stesso disservizio a AgID o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), AgID, ferma restando l'irrogazione delle sanzioni amministrative, diffida altresì i soggetti di cui al comma 1 a ripristinare la regolarità del servizio o ad effettuare le comunicazioni previste. Se l'interruzione del servizio ovvero la mancata o intempestiva comunicazione sono reiterati nel corso di un biennio, successivamente alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico.
3. Nei casi di cui ai commi 1, 1-bis; e 2 può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione secondo la legislazione vigente in materia di pubblicità legale.
4. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 33
Uso di pseudonimi

(ARTICOLO ABROGATO DALL'ART. 64 DEL D.LVO 217/2017)

Art. 34
Norme particolari per le pubbliche amministrazioni

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di qualificarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati;
b) possono rivolgersi a prestatori di servizi di firma digitale o di altra firma elettronica qualificata, secondo la vigente normativa in materia di contratti pubblici.
1-bis. Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:

a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati accreditati come conservatori presso l'AgID.
2. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
3. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
4. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
5. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

Art. 35
Dispositivi sicuri e procedure per la generazione della firma

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
1-bis) Fermo restando quanto previsto dal comma 1, i dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico soddisfano i requisiti di cui all'Allegato II del Regolamento eIDAS.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare di firma elettronica, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.
4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5.
5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico prescritti dall'Allegato II del regolamento eIDAS è accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato. La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'Agenzia per l'Italia digitale in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica.
Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.
6. La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 30, comma 2, del Regolamento eIDAS. Ove previsto dall'organismo di cui al periodo precedente, la valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'AgID in conformita' alle linee guida di cui al comma 5.

(*torna all'indice per argomenti*)

Art. 36
Revoca e sospensione dei certificati qualificati

1. Il certificato qualificato deve essere a cura del certificatore:
a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;
b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;
c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.
2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle Linee guida, per violazione delle regole tecniche ivi contenute.

3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4. Le modalità di revoca o sospensione sono previste nelle Linee guida.

Art. 37
Cessazione dell'attività

1. Il prestatore di servizi fiduciari qualificato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al AgID e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
2. Il prestatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro prestatore o l'annullamento della stessa. L'indicazione di un prestatore di servizi fiduciari qualificato sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il prestatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.
4. L'AgID rende nota la data di cessazione dell'attività del prestatore di cui al comma 1 tramite l'elenco di cui all'articolo 29, comma 6.
4-bis. Qualora il prestatore di cui al comma 1 cessi la propria attività senza indicare, ai sensi del comma 2, un prestatore di servizi fiduciari qualificato sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso AgID che ne garantisce la conservazione e la disponibilità.
4-ter. Nel caso in cui il prestatore di cui al comma 1 non ottemperi agli obblighi previsti dal presente articolo, AgID intima al prestatore di ottemperarvi entro un termine non superiore a trenta giorni. In caso di mancata ottemperanza entro il suddetto termine, si applicano le sanzioni di cui all'articolo 32-bis; le sanzioni pecuniarie previste dal predetto articolo sono aumentate fino al doppio.

(omissis)

CAPO III

GESTIONE, CONSERVAZIONE E ACCESSIBILITA' DEI DOCUMENTI E FASCICOLI INFORMATICI

Sezione I.
Documenti della pubblica amministrazione

Art. 40.
Formazione di documenti informatici.

1. Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri,con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida.
2. (abrogato)
3. (abrogato)
4. (abrogato)

Art. 40-bis
Protocollo informatico.

1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del d.P.R. 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida.

Art. 40-ter
Sistema pubblico di ricerca documentale

1. La Presidenza del Consiglio dei ministri promuove lo sviluppo e la sperimentazione di un sistema volto a facilitare la ricerca dei documenti soggetti a obblighi di pubblicità legale, trasparenza o a registrazione di protocollo ai sensi dell'articolo 53 del d.P.R. 28 dicembre 2000, n. 445, e di cui all'articolo 40-bis e dei fascicoli dei procedimenti di cui all'articolo 41, nonché a consentirne l'accesso on-line ai soggetti che ne abbiano diritto ai sensi della disciplina vigente.

Sezione II.
Gestione e conservazione dei documenti

Art. 41
Procedimento e fascicolo informatico

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione. Per ciascun procedimento amministrativo di loro competenza, esse forniscono gli opportuni servizi di interoperabilità o integrazione, ai sensi di quanto previsto dagli articoli 12 e 64-bis.
1-bis. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).
2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da soggetti giuridici formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.
2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento e dagli interessati, nei limiti ed alle condizioni previste dalla disciplina vigente, attraverso i servizi di cui agli articoli 40-ter e 64-bis. Le Linee guida per la costituzione, l'identificazione, l'accessibilità attraverso i suddetti servizi e l'utilizzo del fascicolo sono dettate dall'AgID ai sensi dell'articolo 71 e sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa dell'integrazione.
2-ter. Il fascicolo informatico reca l'indicazione:
a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;
d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
e-bis) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida.
2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990«e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. AgID detta, ai sensi dell'articolo 71, Linee guida idonee a garantire l'interoperabilità tra i sistemi di gestione dei fascicoli dei procedimenti e i servizi di cui agli articoli 40-ter e 64-bis.
3. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179).

(*torna all'indice per argomenti*)

(omissis)

Art. 43.

Conservazione ed esibizione dei documenti

1. Gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida.

1-bis. Se il documento informatico è conservato per legge da uno dei soggetti di cui all'articolo 2, comma 2, cessa l'obbligo di conservazione a carico dei cittadini e delle imprese che possono in ogni momento richiedere accesso al documento stesso ai medesimi soggetti di cui all'articolo 2, comma 2. Le amministrazioni rendono disponibili a cittadini ed imprese i predetti documenti attraverso servizi on-line accessibili previa identificazione con l'identità' digitale di cui all'articolo 64 ed integrati con i servizi di cui agli articoli 40-ter e 64-bis.

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali ai sensi della disciplina vigente al momento dell'invio dei singoli documenti nel sistema di conservazione.

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle Linee guida.

4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

Art. 44.

Requisiti per la gestione e conservazione dei documenti informatici

1. Il sistema di gestione informatica dei documenti delle pubbliche amministrazioni, di cui all'articolo 52 del d.P.R. 28 dicembre 2000, n. 445, è organizzato e gestito, anche in modo da assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida.

1-bis. Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi.

1-ter. Il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida.

1-quater. Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis.

Art. 44-bis

Conservatori accreditati

(ARTICOLO ABROGATO DALL'ART. 64 DEL D.LVO 217/2017)

CAPO IV
TRASMISSIONE INFORMATICA DEI DOCUMENTI

Art. 45

Valore giuridico della trasmissione

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Art. 46
Dati particolari contenuti nei documenti trasmessi

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via digitale possono contenere soltanto i dati sensibili e giudiziari consentiti da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

Art. 47
Trasmissione dei documenti tra le pubbliche amministrazioni

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il documento può essere, altresì, reso disponibile previa comunicazione delle modalità di accesso telematico allo stesso.
1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del d.P.R. 28 dicembre 2000, n. 445;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle Linee guida. È in ogni caso esclusa la trasmissione di documenti a mezzo fax;
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al d.P.R. 11 febbraio 2005, n. 68.
3. I soggetti di cui all'articolo 2, comma 2, lettere a) e b), provvedono ad istituire e pubblicare nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi almeno una casella di posta elettronica certificata per ciascun registro di protocollo. Le pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

(*torna all'indice per argomenti*)

Art. 48
Posta elettronica certificata[27]

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con le regole tecniche adottate ai sensi dell'articolo 71.
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi alle regole tecniche adottate ai sensi dell'articolo 71.

(*torna all'indice per argomenti*)

[27] Ai sensi dell'art. 65, co. 7, del D.lvo 217/2017, come modificato dal d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12, è stato previsto che "Con decreto del Presidente del Consiglio dei ministri, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali, sono adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certificata di cui agli articoli 29 e 48 del decreto legislativo del 7 marzo 2005, n. 82, al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. A far data dall'entrata in vigore del decreto di cui al primo periodo, l'articolo 48 del decreto legislativo n. 82 del 2005 è abrogato".

Art. 49
Segretezza della corrispondenza trasmessa per via telematica.

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

CAPO V
Dati delle pubbliche amministrazioni e identità digitali, istanze e servizi on-line

SEZIONE I
Dati delle pubbliche amministrazioni

Art. 50
Disponibilità dei dati delle pubbliche amministrazioni

1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.
2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del d.P.R. 28 dicembre 2000, n. 445.
2-bis. Le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti di cui all'articolo 2, comma 2, fermi restando i limiti di cui al comma 1. La predetta attività si svolge secondo le modalità individuate dall'AgID con le Linee guida.
3. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
3-bis. Il trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del dato.

(omissis)

Art. 52
Accesso telematico e riutilizzo dei dati.

1. *(abrogato)*
2. I dati e i documenti che i soggetti di cui all'articolo 2, comma 2, pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza di cui all'articolo 2, comma 1, lettera h), del decreto legislativo 24 gennaio 2006, n. 36, si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 1, comma 1, lettere l-bis) e l-ter, del presente Codice, ad eccezione dei casi in cui la pubblicazione riguardi dati personali del presente Codice.
3. Nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la formazione, la raccolta e la gestione di dati, i soggetti di cui all'articolo 2, comma 2, prevedono clausole idonee a consentirne l'utilizzazione in conformità a quanto previsto dall'articolo 50.
4. Le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni rientrano tra i parametri di valutazione della performance dirigenziale.
5. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).

6. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
7. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
8. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
9. L'Agenzia svolge le attività indicate dal presente articolo con le risorse umane, strumentali, e finanziarie previste a legislazione vigente.

Art. 53
Siti Internet delle pubbliche amministrazioni

1. Le pubbliche amministrazioni realizzano siti istituzionali su reti telematiche che rispettano i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di' consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54.
1-bis. Le pubbliche amministrazioni pubblicano, ai sensi dell'articolo 9 del decreto legislativo 14 marzo 2013, n. 33, anche il catalogo dei dati e dei metadati, nonché delle relative banche dati in loro possesso e i regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo di tali dati e metadati, fatti salvi i dati presenti in Anagrafe tributaria.
1-ter. Con le Linee guida di cui all'articolo 71 sono definite le modalità per la realizzazione e la modifica dei siti delle amministrazioni.
2. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.
3. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.

Art. 54
Contenuto dei siti delle pubbliche amministrazioni.

1. I siti delle pubbliche amministrazioni contengono i dati di cui al decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, nonché quelli previsti dalla legislazione vigente.

(omissis)

Art. 56
Dati identificativi delle questioni pendenti dinanzi autorità giudiziaria di ogni ordine e grado.

1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti.
2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.
2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003.

Art. 57
Moduli e formulari
(ARTICOLO ABROGATO DAL D.LGS 14 MARZO 2013, N. 33)

Art. 57 *bis*
Indice degli indirizzi delle pubbliche amministrazioni
(ARTICOLO ABROGATO DAL D.LGS 26 AGOSTO 2016, N. 179)

(*torna all'indice per argomenti*)

SEZIONE II
Fruibilità dei dati

(omissis)

Art. 62

Anagrafe nazionale della popolazione residente – ANPR

1. è istituita presso il Ministero dell'interno l'ANPR, quale base di dati di interesse nazionale, ai sensi dell'articolo 60, che subentra all'Indice nazionale delle anagrafi (INA), istituito ai sensi del comma 5 dell'articolo 1 della legge 24 dicembre 1954, n. 1228, recante "Ordinamento delle anagrafi della popolazione residente" e all'Anagrafe della popolazione italiana residente all'estero (AIRE), istituita ai sensi della legge 27 ottobre 1988, n. 470, recante "Anagrafe e censimento degli italiani all'estero. Tale base di dati è sottoposta ad un audit di sicurezza con cadenza annuale in conformità alle regole tecniche dell'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del arante per la Protezione dei dati personali.

2. Ferme restando le attribuzioni del sindaco di cui all'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali, approvato con il decreto legislativo 18 agosto 2000, n. 267, l'ANPR subentra altresì alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Con il decreto di cui al comma 6 è definito un piano per il graduale subentro dell'ANPR alle citate anagrafi, da completare entro il 31 dicembre 2014. Fino alla completa attuazione di detto piano, l'ANPR acquisisce automaticamente in via telematica i dati contenuti nelle anagrafi tenute dai comuni per i quali non è ancora avvenuto il subentro. L'ANPR è organizzata secondo modalità funzionali e operative che garantiscono la univocità dei dati stessi.

2-bis. L'ANPR contiene altresì l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni e fornisce i dati ai fini della tenuta delle liste di cui all'articolo 1931 del codice dell'ordinamento militare di cui al decreto legislativo 15 marzo 2010, n. 66, secondo le modalità definite con uno dei decreti di cui al comma 6, in cui è stabilito anche un programma di integrazione da completarsi entro il 31 dicembre 2018.

3. L'ANPR assicura ai comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, e mette a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale. Al fine dello svolgimento delle proprie funzioni, il Comune può utilizzare i dati anagrafici eventualmente detenuti localmente e costantemente allineati con ANPR al fine esclusivo di erogare o usufruire di servizi o funzionalità non fornite da ANPR. L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafi ci nel rispetto di quanto previsto dall'articolo 33 del d.P.R. 30 maggio 1989, n. 223, anche in modalità telematica. I comuni, inoltre, possono consentire anche mediante apposite convenzioni la fruizione dei dati anagrafici da parte dei soggetti aventi diritto. L'ANPR assicura ai soggetti di cui all'articolo 2, comma 2, lettere a) e b), l'accesso ai dati contenuti nell'ANPR.

4. Con il decreto di cui al comma 6 sono disciplinate le modalità di integrazione nell'ANPR dei dati dei cittadini attualmente registrati in anagrafi istituite presso altre amministrazioni nonché dei dati relativi al numero e alla data di emissione e di scadenza della carta di identità della popolazione residente.

5. Ai fini della gestione e della raccolta informatizzata di dati dei cittadini, i soggetti di cui all'articolo 2, comma 2, lettere a) e b), si avvalgono esclusivamente dell'ANPR, che viene integrata con gli ulteriori dati a tal fine necessari.

6. Con uno o più decreti del Presidente del Consiglio dei Ministri, su proposta del Ministro dell'interno, del Ministro per la pubblica amministrazione e la semplificazione e del Ministro delegato all'innovazione tecnologica, di concerto con il Ministro dell'economia e delle finanze, d'intesa con l'Agenzia per l'Italia digitale e con la Conferenza Stato - città, di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, per gli aspetti d'interesse dei comuni, sentita l'ISTAT e acquisito il parere del Garante per la protezione dei dati personali, sono stabiliti i tempi e le modalità di attuazione delle disposizioni del presente articolo, anche con riferimento:

a) alle garanzie e alle misure di sicurezza da adottare nel trattamento dei dati personali, alle modalità e ai tempi di conservazione dei dati e all'accesso ai dati da parte delle pubbliche amministrazioni per le proprie finalità istituzionali secondo le modalità di cui all'articolo 50;

b) ai criteri per l'interoperabilità dell'ANPR con le altre banche dati di rilevanza nazionale e regionale, secondo le regole tecniche del sistema pubblico di connettività di cui al capo VIII del presente Codice in modo che le informazioni di anagrafe, una volta rese dai cittadini, si intendano acquisite dalle pubbliche amministrazioni senza necessità di ulteriori adempimenti o duplicazioni da parte degli stessi;

c) all'erogazione di altri servizi resi disponibili dall'ANPR, tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita ai sensi dell'articolo 30, comma 4, del d.P.R. 3 novembre

2000, n. 396, e della dichiarazione di morte ai sensi degli articoli 72 e 74 dello stesso decreto nonché della denuncia di morte prevista dall'articolo 1 del regolamento di polizia mortuaria di cui al d.P.R. 10 settembre 1990, n. 285, compatibile con il sistema di trasmissione di cui al decreto del Ministro della salute in data 26 febbraio 2010, pubblicato nella Gazzetta Ufficiale n. 65 del 19 marzo 2010.

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)
(torna all'art. 16ter d.l. 179 del 2012)

(omissis)

SEZIONE III
Identità digitali, istanze e servizi on-line

(omissis)

Art. 64
Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.
2. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.
2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di soggetti giuridici, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di soggetti giuridici (SPID).
2-ter. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con il decreto di cui al comma 2-sexies, identificano gli utenti per consentire loro l'accesso ai servizi in rete.
2-quater. L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies. Resta fermo quanto previsto dall'articolo 3-bis, comma 01.
2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta ai soggetti privati, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera i predetti soggetti da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.
2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:
a) al modello architetturale e organizzativo del sistema;
b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;
c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di soggetti giuridici;
d) alle modalità di adesione da parte di soggetti giuridici in qualità di utenti di servizi in rete;
e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;
f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.
2-septies. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
2-octies. (COMMA ABROGATO dal D.LGS 13 DICEMBRE 2017, N. 217).
2-novies. L'accesso di cui al comma 2-quater può avvenire anche con la carta di identità elettronica e la carta nazionale dei servizi.
2-decies. Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati.
3. (COMMA ABROGATO DAL D.LGS. 30 DICEMBRE 2010, N. 235).

3-bis. Con decreto del Presidente del Consiglio dei ministri o del Ministro per la semplificazione e la pubblica amministrazione, è stabilità la data a decorrere dalla quale i soggetti di cui all'articolo 2, comma 2, utilizzano esclusivamente le identità digitali ai fini dell'identificazione degli utenti dei propri servizi on-line.

Art. 64-bis
Accesso telematico ai servizi della Pubblica Amministrazione.

1. I soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle Linee guida, tramite il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica.
1-bis. Al fine di rendere effettivo il diritto di cui all'articolo 7, comma 01, i soggetti di cui all'articolo 2, comma 2, i fornitori di identità digitali e i prestatori dei servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con il servizio di cui al comma 1, espongono per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida.

Art. 65
Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

1. Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici ai sensi dell'articolo 38, commi 1 e 3, del d.P.R. 28 dicembre 2000, n. 445, sono valide:
a) se sottoscritte mediante una delle forme di cui all'articolo 20, il cui certificato è rilasciato da un certificatore qualificato;
b) ovvero, quando l'istante o il dichiarante è identificato attraverso il sistema pubblico di identità digitale (SPID), nonché attraverso uno degli altri strumenti di cui all'articolo 64, comma 2-novies, nei limiti ivi previsti;
c) ovvero sono sottoscritte e presentate unitamente alla copia del documento d'identità;
c-bis) ovvero se trasmesse dall'istante o dal dichiarante dal proprio domicilio digitale purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con Linee guida, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce elezione di domicilio speciale ai sensi dell'articolo 47 del Codice civile. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.
1-bis. *(abrogato)*
1-ter. Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate ai sensi e con le modalità di cui al comma 1, comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso.
2. Le istanze e le dichiarazioni di cui al comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.
3. *(abrogato)*
4. Il comma 2 dell'articolo 38 del d.P.R. 28 dicembre 2000, n. 445, è sostituito dal seguente: *«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82»*.

SEZIONE IV
Carte elettroniche

Art. 66
Carta d'identità elettronica e carta nazionale dei servizi

(omissis)

CAPO VII
REGOLE TECNICHE

Art. 71
Regole tecniche

1. L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice. Le Linee guida divengono efficaci dopo la loro pubblicazione nell'apposita area del sito Internet istituzionale dell'AgID e di essa ne è data notizia nella Gazzetta Ufficiale della Repubblica italiana. Le Linee guida sono aggiornate o modificate con la procedura di cui al primo periodo.[28]
1-bis. *(abrogato)*
1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.
2. (COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)[29]

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

CAPO VIII
Sistema pubblico di connettività

Art. 72
(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)

Art. 73
Sistema pubblico di connettività (SPC)
1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione, e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente Capo definisce e disciplina il Sistema pubblico di connettività e cooperazione (SPC), quale insieme di infrastrutture tecnologiche e di regole tecniche che assicura l'interoperabilità tra i sistemi informativi delle pubbliche amministrazioni, permette il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea ed è aperto all'adesione da parte dei gestori di servizi pubblici e dei soggetti privati.
2. Il SPC garantisce la sicurezza e la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascun soggetto aderente.
3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:
a) sviluppo architetturale e organizzativo atto a garantire la federabilità dei sistemi;
b) economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa;
b-bis) aggiornamento continuo del sistema e aderenza alle migliori pratiche internazionali;
c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.
3-bis. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.
3-ter. Il SPC è costituito da un insieme di elementi che comprendono: a) infrastrutture, architetture e interfacce tecnologiche; b) linee guida e regole per la cooperazione e l'interoperabilità; c) catalogo di servizi e applicazioni. 3-quater. Ai sensi dell'articolo 71 sono dettate le regole tecniche del Sistema pubblico di connettività e cooperazione, al fine di assicurarne: l'aggiornamento rispetto alla evoluzione

[28] L'art. 65, ult. comma, del D.lvo 217/2017 ha stabilito che "Le regole tecniche emanate ai sensi dell'articolo 71 del decreto legislativo n. 82 del 2005, nel testo vigente prima dell'entrata in vigore del presente decreto, restano efficaci fino all'eventuale modifica o abrogazione da parte delle Linee guida di cui al predetto articolo 71, come modificato dal presente decreto".
[29] L'art. 61 del D.lvo 26 agosto 2016, n. 179, così come modificato dall'art. 64 del D.lvo 217/2017, ha dettato "Disposizioni di coordinamento": "**1.** Fino all'adozione delle Linee guida di cui all'articolo 71 del decreto legislativo n. 82 del 2005, l'obbligo per le amministrazioni pubbliche di adeguare i propri sistemi di gestione informatica dei documenti, di cui all'articolo 17 del decreto del Presidente del Consiglio dei ministri 13 novembre 2014, è sospeso, salva la facoltà per le amministrazioni medesime di adeguarsi anteriormente. Fino all'adozione del decreto del Presidente del Consiglio dei ministri di cui all'articolo 29, comma 3, del decreto legislativo n. 82 del 2005, come modificato dall'articolo 25 del presente decreto, restano efficaci le disposizioni dell'articolo 29, comma 3, dello stesso decreto nella formulazione previgente all'entrata in vigore del presente decreto. 2. (omissis)".

della tecnologia; l'aderenza alle linee guida europee in materia di interoperabilità; l'adeguatezza rispetto alle esigenze delle pubbliche amministrazioni e dei suoi utenti; la piu' efficace e semplice adozione da parte di tutti i soggetti, pubblici e privati, il rispetto di necessari livelli di sicurezza.

Art. 74
(ARTICOLO ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179)

Art. 75
Partecipazione al Sistema pubblico di connettività

1. I soggetti di cui all'articolo 2, comma 2, partecipano al SPC, salve le esclusioni collegate all'esercizio delle funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali.
2. Chiunque può partecipare al SPC nel rispetto delle regole tecniche di cui all'articolo 73, comma 3-quater.
3. AgID rende gratuitamente disponibili specifiche delle interfacce tecnologiche, le linee guida, le regole di cooperazione e ogni altra informazione necessaria a garantire l'interoperabilità del SPC con ogni soluzione informatica sviluppata autonomamente da privati o da altre amministrazioni che rispettano le regole definite ai sensi dell'articolo 73, comma 3-quater.
3-bis. COMMA ABROGATO DAL D.LGS. 26 AGOSTO 2016, N. 179.

CAPO IX
Disposizioni transitorie finali e abrogazioni

Art. 91
Abrogazioni

1. Dalla data di entrata in vigore del presente testo unico sono abrogati:
a) il decreto legislativo 23 gennaio 2002, n. 10;
b) gli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 2, comma 1, ultimo periodo, 6; 8; 9; 10; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 36, commi 1, 2, 3, 4, 5 e 6; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A);
c) l'articolo 26 comma 2, lettera a), e), h), della legge 27 dicembre 2002, n. 289; d) articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3; ; e) gli articoli 16, 17, 18 e 19 della legge 29 luglio 2003, n. 229.
2. Le abrogazioni degli articoli 2, comma 1, ultimo periodo, 6, commi 1 e 2; 10; 36, commi 1, 2, 3, 4, 5 e 6; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto legislativo 28 dicembre 2000, n. 443 (Testo B).
3. Le abrogazioni degli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 6, commi 3 e 4; 8; 9; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).
3-bis. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59, è abrogato.
3-ter. Il decreto legislativo 28 febbraio 2005, n. 42, è abrogato.

(omissis)

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)

DPCM 2 novembre 2005 - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (GU n. 266 del 15-11-2005)

(ritorna all'indice cronologico)

Articolo 1 – Definizioni

1. Ai fini del presente decreto si applicano le definizioni contenute nell'Articolo 1 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, citato nelle premesse. Si intende, inoltre, per:

a. PUNTO DI ACCESSO: il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto;

b. punto di ricezione: il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto;

c. punto di consegna: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna;

d. firma del gestore di posta elettronica certificata: la firma elettronica avanzata, basata
su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.

e. ricevuta di accettazione: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata;

f. avviso di non accettazione: l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario;

g. ricevuta di presa in carico: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;

h. ricevuta di avvenuta consegna: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario;

i. ricevuta completa di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale;

l. ricevuta breve di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;

m. ricevuta sintetica di avvenuta consegna: la ricevuta che contiene i dati di certificazione;

n. avviso di mancata consegna: l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario;

o. messaggio originale: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene;

p. busta di trasporto: la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il
messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione;

q. busta di anomalia: la busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia;

r. dati di certificazione: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore

di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto;
s. gestore di posta elettronica certificata: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;
t. titolare: il soggetto a cui è assegnata una casella di posta elettronica certificata;
u. dominio di posta elettronica certificata: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata;
v. indice dei gestori di posta elettronica certificata: il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.
z. casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;
aa. marca temporale: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.

Articolo 2 - Obiettivi e finalità
1. Il presente decreto definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata di cui al decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 3 - Norme tecniche di riferimento
1. Sono di seguito elencati gli standard di riferimento delle norme tecniche, le cui specifiche di dettaglio vengono riportate in allegato al presente decreto:
a. RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);
b. RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
c. RFC 1912 (Common DNS Operational and Configuration Errors);
d. RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
e. RFC 2315 (PKCS \ 7: Cryptographic Message Syntax Version 1.5);
f. RFC 2633 (S/MIME Version 3 Message Specification);
g. RFC 2660 (The Secure HyperText Transfer Protocol);
h. RFC 2821 (Simple Mail Transfer Protocol);
i. RFC 2822 (Internet Message Format);
l. RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification);
m. RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
n. RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
o. RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile).

Articolo 4 - Compatibilità operativa degli standard
1. Il Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato CNIPA, verifica, in funzione dell'evoluzione tecnologica, la coerenza operativa degli standard così come adottati nelle specifiche tecniche, dando tempestiva informazione delle eventuali variazioni nel proprio sito istituzionale

Articolo 5 - Comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata
1. La dichiarazione di cui all'art. 4, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del decreto del Presidente della Repubblica n. 445 del 2000.

2. La dichiarazione di cui al comma 1 è resa anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima.

Articolo 6 - Caratteristiche dei messaggi gestiti dai sistemi di posta elettronica certificata

1. I sistemi di posta elettronica certificata generano messaggi conformi allo standard internazionale S/MIME, così come descritto dallo standard RFC 2633.
2. I messaggi di cui al comma 1 si dividono in tre categorie:
a. ricevute;
b. avvisi;
c. buste.
3. La differenziazione dei messaggi, come indicato nel comma 2, è realizzata dai sistemi di posta elettronica certificata utilizzando la struttura header, prevista dallo standard S/MIME, da impostare per ogni tipologia di messaggio in conformità a quanto previsto dalle specifiche tecniche di cui all'allegato.
4. I sistemi di posta elettronica certificata in relazione alla tipologia di messaggio da gestire realizzano funzionalità distinte e specifiche.
5. L'elaborazione dei messaggi di posta elettronica certificata avviene anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.
6. Le ricevute generate dai sistemi di posta elettronica certificata sono le seguenti:
a. ricevuta di accettazione;
b. ricevuta di presa in carico;
c. ricevuta di avvenuta consegna completa, breve, sintetica.
7. La ricevuta di avvenuta consegna è rilasciata per ogni destinatario al quale il messaggio è consegnato.
8. Gli avvisi generati dai sistemi di posta elettronica certificata sono i seguenti:
a. avviso di non accettazione per eccezioni formali ovvero per virus informatici;
b. avviso di rilevazione di virus informatici;
c. avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici.
9. Le buste generate dai sistemi di posta elettronica certificata sono le seguenti:
a. busta di trasporto;
b. busta di anomalia.
10. La busta di trasporto è consegnata immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

Articolo 7 - Firma elettronica dei messaggi di posta elettronica certificata

1. I messaggi di cui all'art. 6, generati dai sistemi di posta elettronica certificata, sono sottoscritti dai gestori mediante la firma del gestore di posta elettronica certificata, in conformità a quanto previsto dall'allegato.
2. I certificati di firma di cui al comma 1 sono rilasciati dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata e sino ad un numero massimo di dieci firme per ciascun gestore.
3. Qualora un gestore abbia ravvisato la necessità di utilizzare un numero di certificati di firma superiore a dieci, può richiederli al CNIPA documentando tale necessità. Il CNIPA, previa valutazione della richiesta, stabilisce se fornire o meno al gestore ulteriori certificati di firma.

Articolo 8 - Interoperabilità

1. Le specifiche tecniche finalizzate a garantire l'interoperabilità sono definite nell'allegato.

Articolo 9 - Riferimento temporale

1. A ciascuna trasmissione è apposto un unico riferimento temporale, secondo le modalità indicate nell'allegato.
2. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

Articolo 10 - Conservazione dei log dei messaggi

1. Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, ogni gestore provvede a:
a. definire un intervallo temporale unitario non superiore alle ventiquattro ore;

b. eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale come sopra definito.
2. Ai file generati da ciascuna operazione di salvataggio deve essere associata la relativa marca temporale.

Articolo 11 - Conservazione dei messaggi contenenti virus e relativa informativa al mittente
1. Il gestore è tenuto a trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato.
2. Il gestore è tenuto ad informare il mittente che il messaggio inviato contiene virus.
3. Il gestore è tenuto a conservare il messaggio contenente virus per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico.

Articolo 12 - Livelli di servizio
1. Il gestore di posta elettronica certificata può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata.
2. In ogni caso il gestore di posta elettronica certificata deve garantire la possibilità dell'invio di un messaggio:
a. almeno fino a cinquanta destinatari;
b. per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i trenta megabytes.
3. La disponibilità nel tempo del servizio di posta elettronica certificata deve essere maggiore o uguale al 99,8% del periodo temporale di riferimento.
4. Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.
5. La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata deve essere minore, o uguale, al 50% del totale previsto per l'intervallo di tempo di riferimento.
6. Nell'ambito dell'intervallo di disponibilità di cui al comma 3, la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.
7. Al fine di assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute, il gestore di posta elettronica certificata descrive nel manuale operativo, di cui all'art. 23, le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, ai sensi di quanto previsto dall'art. 11, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente articolo.

Articolo 13 - Avvisi di mancata consegna
1. Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.
2. Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio, così come previsto dal decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 14 - Norme di garanzia sulla natura della posta elettronica ricevuta
1. Il gestore di posta elettronica certificata del destinatario ha l'obbligo di segnalare a quest'ultimo se la posta elettronica in arrivo non è qualificabile come posta elettronica certificata, secondo quanto prescritto dal decreto del Presidente della Repubblica n. 68 del 2005, nonché dal presente decreto e relativo allegato.
2. I messaggi relativi all'invio e alla consegna di documenti attraverso la posta elettronica certificata sono rilasciati indipendentemente dalle caratteristiche e dal valore giuridico dei documenti trasmessi.

Articolo 15 - Limiti di utilizzo
1. La pubblica amministrazione che intende iscriversi all'elenco dei gestori di posta elettronica certificata, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, è tenuta a presentare al

CNIPA una relazione tecnica che illustri le misure adottate affinché l'utilizzo di caselle di posta elettronica rilasciate a privati dall'amministrazione medesima:
a. costituisca invio valido ai sensi dell'art. 16, comma 2, del decreto del Presidente della Repubblica n. 68 del 2005;
b. avvenga limitatamente ai rapporti di cui al medesimo art. 16, comma 2.

Articolo 16 - Modalità di iscrizione all'elenco dei gestori di posta elettronica certificata
1. I soggetti che presentano domanda di iscrizione all'elenco pubblico, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, forniscono inoltre al CNIPA le informazioni e i documenti di seguito indicati, anche su supporto elettronico, ad eccezione del documento di cui alla lettera e):
a. denominazione sociale;
b. sede legale;
c. sedi presso le quali è erogato il servizio;
d. rappresentante legale;
e. piano per la sicurezza, contenuto in busta sigillata;
f. manuale operativo di cui all'art. 23;
g. dichiarazione di impegno al rispetto delle disposizioni del decreto del Presidente della Repubblica n. 68 del 2005;
h. dichiarazione di conformità ai requisiti previsti nel presente decreto e suo allegato;
i. relazione sulla struttura organizzativa.
2. I soggetti che rivestono natura giuridica privata trasmettono, inoltre, copia cartacea di una polizza assicurativa o di un certificato provvisorio impegnativo di copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali, a norma delle vigenti disposizioni.

Articolo 17 - Equivalenza dei requisiti dei gestori stranieri
1. Il gestore di posta elettronica certificata stabilito in altri Stati membri dell'Unione europea che si trovi nelle condizioni di cui all'art. 15 del decreto del Presidente della Repubblica n. 68 del 2005 ed intenda esercitare il servizio di posta elettronica certificata in Italia, comunica in via preventiva al CNIPA tale intenzione ed ogni notizia utile al fine della verifica di cui al citato art. 15. La comunicazione costituisce domanda di iscrizione nell'elenco di gestori di posta elettronica certificata; sono applicabili le disposizioni procedimentali di cui all'art. l4 del decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 18 - Indice ed elenco pubblico dei gestori di posta elettronica certificata
1. I gestori di posta elettronica certificata si attengono alle regole riportate nell'allegato per accedere all'indice dei gestori di posta elettronica certificata.
2. Il certificato elettronico, da utilizzare per la funzione di accesso di cui al comma 1, è rilasciato dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.
3. L'elenco pubblico dei gestori di posta elettronica certificata tenuto dal CNIPA contiene, per ogni gestore, le seguenti indicazioni:
a. denominazione sociale;
b. sede legale;
c. rappresentante legale;
d. indirizzo internet;
e. data di iscrizione all'elenco;
f. data di cessazione ed eventuale gestore sostitutivo.
4. L'elenco pubblico è sottoscritto con firma digitale dal CNIPA, che lo rende disponibile per via telematica.

Articolo 19 - Disciplina dei compiti del CNIPA
1. Il CNIPA definisce con circolari le modalità di inoltro della domanda e le modalità dell'esercizio dei compiti di vigilanza e controllo di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.

Articolo 20 - Sistema di qualità del gestore
1. Entro un anno dall'iscrizione del gestore all'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, il gestore medesimo fornisce copia della certificazione di conformità del

proprio sistema di qualità alle norme UNI EN ISO 9001:2000 e successive evoluzioni relativamente a tutti i processi connessi al servizio di posta elettronica certificata.
2. Il manuale della qualità è depositato presso il CNIPA e reso disponibile presso il gestore.

Articolo 21 - Organizzazione e funzioni del personale del certificatore
1. L'organizzazione del personale addetto al servizio di posta elettronica certificata prevede almeno la presenza di responsabili preposti allo svolgimento delle seguenti attività e funzioni:
a. registrazione dei titolari;
b. servizi tecnici;
c. verifiche e ispezioni (auditing);
d. sicurezza;
e. sicurezza dei log dei messaggi;
f. sistema di riferimento temporale.
2. É possibile attribuire al medesimo soggetto più responsabilità tra quelle previste dalle lettere d), e) ed f).

Articolo 22 - Requisiti di competenza ed esperienza del personale
1. Il personale cui sono attribuite le funzioni previste dall'art. 21 deve aver maturato un'esperienza almeno quinquennale nelle attività di analisi, progettazione, commercializzazione e conduzione di sistemi informatici.
2. Per ogni aggiornamento apportato al sistema di posta elettronica certificata, il gestore eroga, alle figure professionali interessate, apposita attività di addestramento.

Articolo 23 - Manuale operativo
1. Il manuale operativo definisce e descrive le procedure applicate dal gestore di posta elettronica certificata nello svolgimento della propria attività.
2. Il manuale operativo è depositato presso il CNIPA.
3. Il manuale contiene:
a. i dati identificativi del gestore;
b. i dati identificativi della versione del manuale operativo;
c. l'indicazione del responsabile del manuale operativo;
d. l'individuazione, l'indicazione e la definizione degli obblighi del gestore di posta elettronica certificata e dei titolari;
e. la definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f. l'indirizzo del sito web del gestore ove sono pubblicate le informazioni relative ai servizi offerti;
g. le modalità di protezione della riservatezza dei dati;
h. le modalità per l'apposizione e la definizione del riferimento temporale.

(ritorna all'indice cronologico)

Decreto 31 ottobre 2006 - Individuazione dei siti internet destinati all'inserimento degli avvisi di vendita di cui all'articolo 490 del codice di procedura civile ***(pubblicato nella Gazzetta Ufficiale n.297 del 22 dicembre 2006)***

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)

IL MINISTRO DELLA GIUSTIZIA

Visto l'art. 490, secondo comma, del codice di procedura civile, come modificato dall'art. 2, comma 3, lettera e) del decreto-legge n. 35 del 2005, convertito, con modificazioni, dalla legge 14 maggio 2005, n. 80, secondo cui «in caso di espropriazione di beni mobili registrati per un valore superiore a 25.000 euro, e di beni immobili, lo stesso avviso, unitamente a copia dell'ordinanza del giudice e della relazione di stima redatta ai sensi dell'art. 173-bis delle disposizioni di attuazione del presente codice, è altresì inserito in appositi siti internet almeno quarantacinque giorni prima del termine per la presentazione delle offerte o della data dell'incanto»;
Visto l'art. 173-ter delle disposizioni di attuazione del codice di procedura civile, aggiunto dall'art. 2, comma 3-ter, del decreto-legge n. 35 del 2005, convertito, con modificazioni, dalla legge 14 maggio 2005, n. 80, rubricato «Pubblicità degli avvisi tramite internet», secondo il quale «il Ministro della giustizia stabilisce con proprio decreto i siti internet destinati all'inserimento degli avvisi di cui all'art. 490 del codice e i criteri e le modalità con cui gli stessi sono formati e resi disponibili»;
Visto altresì l'art. 159 delle disposizioni di attuazione del codice di procedura civile nel quale vengono individuati gli istituti autorizzati all'incanto dei beni mobili e all'amministrazione giudiziaria dei beni immobili;
Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di dei dati personali»;
Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;
Vista la legge 9 gennaio 2004, n. 4, recante «disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici»;
Visto il decreto legislativo 7 marzo 2005, n. 82, recante «codice dell'amministrazione digitale» e successive modificazioni;
Visto il decreto del Presidente della Repubblica 1° marzo 2005, n. 75, recante «regolamento di attuazione della legge 9 gennaio 2004, n. 4»;
Visto il decreto ministeriale 8 luglio 2005, recante «requisiti tecnici e i diversi livelli per l'accessibilità per gli strumenti informatici»;
Ritenuta la necessità di individuare i siti internet destinati all'inserimento degli avvisi di vendita di cui all'art. 490 codice di procedura civile;
Sentito il Ministro per le riforme e le innovazioni nella pubblica amministrazione;

DECRETA

Art. 1
Criteri e modalità di individuazione dei siti internet

1. Il presente decreto stabilisce i criteri e le modalità con cui sono individuati i siti internet destinati all'inserimento degli avvisi di vendita di cui all'art. 490 del codice di procedura civile.

Art. 2
Elenco

1. I siti internet gestiti dai soggetti in possesso dei requisiti professionali di cui all'art. 3 e dotati dei requisiti tecnici di cui all'art. 4, sono inseriti nell'elenco tenuto presso il Dipartimento per gli affari di giustizia del Ministero, Direzione generale della giustizia civile e possono effettuare gli avvisi di vendita di cui all'art. 1.
2. I soggetti che gestiscono i siti di cui al comma 1 devono avere forma societaria e possono richiedere l'iscrizione per effettuare la pubblicità in uno o più distretti di Corte d'appello.
3. (I soggetti di cui al comma 1 costituiti in società di persone, società per azioni o in accomandita per azioni, società a responsabilità limitata, società cooperativa o consortile devono possedere un patrimonio netto pari almeno a euro 50.000,00 se richiedono l'iscrizione per un distretto di Corte di appello ed un patrimonio netto almeno pari a euro 450.000,00 se richiedono l'iscrizione per due o più distretti di Corte di appello o per uno dei seguenti distretti: Milano, Napoli, Roma e Palermo. Ai fini del presente comma,

il patrimonio netto è composto all'attivo esclusivamente da capitale sociale, riserve da utili, riserva legale ed eventuali riserve statutarie.)[30]
4. Entro il termine di otto mesi dalla chiusura di ciascun esercizio successivo all'iscrizione nell'elenco, le società di cui al comma 3 trasmettono al Dipartimento per gli affari di giustizia del Ministero, Direzione generale della giustizia civile, che verifica la sussistenza del requisito di cui al medesimo comma, copia del bilancio depositato nel registro delle imprese relativo all'esercizio precedente.
5. I siti internet gestiti dagli istituti autorizzati all'incanto e all'amministrazione dei beni a norma dell'art. 159 delle disposizioni di attuazione del codice di procedura civile, sono iscritti di diritto nell'elenco per le circoscrizioni per le quali sono abilitati, limitatamente alla pubblicità dei beni mobili. Per l'abilitazione alla pubblicità dei beni immobili, devono possedere i requisiti professionali e tecnici di cui agli articoli 3 e 4, e presentare domanda di iscrizione nell'elenco, ai sensi dell'art. 5.

Art. 3
Requisiti professionali e incompatibilità

1. I soci delle società di persone o i legali rappresentanti e i soggetti preposti all'amministrazione di società di capitali, che gestiscono i siti internet che chiedono l'iscrizione nell'elenco di cui all'art. 2, debbono possedere i requisiti di onorabilità di cui all'art. 26 del testo unico delle leggi in materia bancaria e creditizia di cui al decreto legislativo 1° settembre 1993, n. 385 e successive modificazioni.
2. I soggetti che richiedono l'iscrizione nell'elenco di cui all'art. 2 devono essere iscritti al registro degli operatori di comunicazione di cui all'art. 1, comma 6, lettera a), n. 5 delle legge 31 luglio 1997, n. 249.
3. È incompatibile la qualità di socio, di legale rappresentate o di amministratore di società di persone, società cooperative e società a responsabilità limitata con la funzione di giudice, di dirigente amministrativo e di funzionario di cancelleria in servizio presso gli uffici giudiziari del distretto di Corte d'appello per il quale la società è iscritta nell'elenco.
4. È incompatibile la qualità di socio di società per azioni o in accomandita per azioni con la funzione di giudice, di dirigente amministrativo e di funzionario di cancelleria in servizio presso il distretto di Corte d'appello per il quale la società è iscritta nell'elenco, se le azioni possedute eccedono il 10% del capitale sociale o la somma di euro 50.000,00.
5. Le norme di cui ai commi 2, 3 e 4 si applicano anche ai consulenti tecnici di ufficio e ai delegati alle operazioni di vendita di cui all'art. 591-bis del codice di procedura civile, incaricati o delegati nelle procedure pendenti davanti agli uffici giudiziari del distretto di Corte d'appello per il quale la società è iscritta, nonché ai parenti ed affini fino al terzo grado, dei giudici, dirigenti amministrativi, funzionari di cancelleria, consulenti tecnici di ufficio e delegati del giudice.

Art. 4
Requisiti tecnici

1. I siti iscritti nell'elenco garantiscono un livello di disponibilità del servizio pari al 99 per cento su base quadrimestrale, nei giorni feriali e del 95 per cento su base quadrimestrale nei giorni festivi, dalle ore 5 alle ore 24.
2. I siti si dotano di un manuale operativo dei servizi, in cui vengono descritti le modalità di comunicazione con gli uffici giudiziari o i soggetti delegati, di acquisizione dei dati, e di esecuzione dei servizi, nonché i prezzi praticati per ciascun servizio, con indicazione di eventuali differenziazioni per distretto o circondario. Le modalità di esecuzione dei servizi e i relativi prezzi dovranno essere pubblicati sui siti, in pagine con accesso riservato all'autorità giudiziaria.
3. I siti si dotano di un piano in cui vengono descritte tutte le azioni e le procedure di sicurezza in conformità con quanto previsto dal decreto legislativo 30 giugno 2003, n. 196.
4. La frequenza di salvataggio dei dati è almeno giornaliera.
5. I siti sono conforme ai requisiti tecnici di cui al decreto del Ministro delegato per l'innovazione e le tecnologie emanato ai sensi dell'art. 11 della legge 9 gennaio 2004, n. 4 e superano la valutazione di accessibilità applicando la metodologia per la verifica tecnica di cui all'allegato A al suddetto decreto.

Art. 5
Modalità di iscrizione

1. Le società che intendono effettuare gli avvisi di vendita di cui all'art. 1 inoltrano al Dipartimento per gli affari di giustizia del Ministero, Direzione generale della giustizia civile domanda di iscrizione nell'elenco, contenente l'indicazione del distretto o dei distretti di Corte d'appello in cui effettuare la

[30] Comma annullato dal TAR Lazio con sentenza n. 8114 del 6 giugno 2007.

pubblicità, corredata a dichiarazione di possesso dei requisiti di professionalità e tecnici e dall'assenza di incompatibilità, nonché copia del manuale operativo e del piano della sicurezza del sito.
2. Il Ministero della giustizia, Direzione generale della giustizia civile, decide, acquisito il parere della Direzione generale dei sistemi informativi automatizzati, sulla domanda con provvedimento motivato, anche sulla base di apposite verifiche che, nel caso in cui non risulti possibile utilizzare personale dell'amministrazione, possono essere effettuate anche da esperti informatici esterni, dalla stessa delegati e con costi a carico del richiedente.
3. Il Ministero della giustizia verifica l'adempimento degli obblighi assunti dai siti anche a mezzo dei servizi attivati con il portale di cui all'art. 7.

Art. 6
Acquisizione dei dati

1. Il sito acquisisce i dati relativi alla pubblicazione tramite collegamento telematico con l'Ufficio giudiziario e secondo quanto previsto dal decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, con modalità operative definite dal Ministero della giustizia - Direzione generale dei sistemi informativi automatizzati.
2. Il sito, se l'Ufficio giudiziario non dispone del software di gestione ufficiale, acquisisce i dati per posta ordinaria, a mezzo fax, su supporto elettronico o per posta telematica, con modalità che garantiscono la esattezza delle informazioni che devono essere pubblicate, tali modalità vengono definite dall'Ufficio giudiziario previa comunicazione al Ministero della giustizia - Direzione generale dei sistemi informativi automatizzati, che può disporne la modifica per garantire la sicurezza del sistema di pubblicità e l'esattezza e regolarità delle pubblicazioni.

Art. 7
Portale vendite giudiziarie

1. Il Ministero della giustizia attiva il Portale vendite giudiziarie per la ricerca e il monitoraggio dei dati pubblicati sui siti, al fine di consentire una visione completa ed unitaria di tutte le vendite forzate in corso.
2. Il portale è realizzato nel rispetto dei criteri dettati, per i siti delle pubbliche amministrazioni, dal codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, come modificato e integrato dal decreto legislativo 4 aprile 2006, n. 159.
3. Il Ministero della giustizia, Direzione generale dei sistemi informativi automatizzati, stabilisce le informazioni minime relative ai dati da pubblicare sui siti.
4. Il Ministero della giustizia verifica, tramite il Portale, il regolare funzionamento dei siti, nel rispetto dei requisiti tecnici di cui all'art. 4 e secondo le modalità contenute nelle disposizioni di cui all'art. 4, comma 3.
5. Il Ministero della giustizia certifica, tramite il Portale, l'inizio di ciascuna inserzione pubblicitaria, la sua durata e gli eventi significativi.
6. La certificazione viene inviata, attraverso la posta certificata del processo telematico, all'Ufficio giudiziario il giorno precedente a quello fissato per l'esperimento di vendita.
7. L'indirizzo, cui è inviata la certificazione, è unico per ogni Ufficio giudiziario o per ogni sezione dell'Ufficio giudiziario.
8. Il Portale pubblica, in area riservata accessibile al Ministero della giustizia e all'ufficio giudiziario che ha disposto le inserzioni pubblicitarie, i dati statistici relativi all'accesso ai siti.

Art. 8
Cancellazione dall'elenco

1. L'accertamento dell'assenza o del venire meno dei requisiti e delle condizioni di cui agli articoli 2, 3 e 4, comporta la cancellazione d'ufficio del sito internet dall'elenco di cui all'art. 2.
2. Sono cancellati dall'elenco i siti che effettuano la pubblicità di atti relativi a procedure esecutive pendenti davanti agli uffici giudiziari di distretti di Corti d'appello diversi da quelli per i quali sono iscritti. Il presente decreto sarà trasmesso ai competenti organi di controllo e sarà pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)

Decreto Legge 25 giugno 2008, n. 112, convertito con modificazioni, dalla legge 6 agosto 2008, n. 133, e modificato dal decreto-legge 29 dicembre 2009, n. 193, convertito con modificazioni, dalla legge 22 febbraio 2010, n. 24. (Estratto)

(ritorna all'indice cronologico)
(leggi l'Avvertenza)

ART. 51
Comunicazioni e notificazioni per via telematica

[1. A decorrere dal quindicesimo giorno successivo a quello della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dei decreti di cui al comma 2, negli uffici giudiziari indicati negli stessi decreti, le notificazioni e le comunicazioni di cui al primo comma dell'articolo 170 del codice di procedura civile, la notificazione di cui al primo comma dell'articolo 192 del codice di procedura civile e ogni altra comunicazione al consulente sono effettuate per via telematica all'indirizzo di posta elettronica certificata di cui all'articolo 16 del decreto-legge 29 novembre 2008, n. 185 , convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 . Allo stesso modo si procede per le notificazioni e le comunicazioni previste dal regio decreto 16 marzo 1942, n. 267, e per le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale. La notificazione o comunicazione che contiene dati sensibili è effettuata solo per estratto con contestuale messa a disposizione, sul sito internet individuato dall'amministrazione, dell'atto integrale cui il destinatario accede mediante gli strumenti di cui all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82.] [31]

[2. Con uno o più decreti aventi natura non regolamentare, da adottarsi entro il 1° settembre 2010, sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati, il Ministro della giustizia, previa verifica, accerta la funzionalità dei servizi di comunicazione, individuando gli uffici giudiziari nei quali trovano applicazione le disposizioni di cui al comma 1.] [32]

[3. A decorrere dalla data fissata ai sensi del comma 1, le notificazioni e comunicazioni nel corso del procedimento alle parti che non hanno provveduto ad istituire e comunicare l'indirizzo elettronico di cui al medesimo comma, sono fatte presso la cancelleria o segreteria dell'ufficio giudiziario.] [33]

[4. A decorrere dalla data fissata ai sensi del comma 1, le notificazioni e le comunicazioni di cui ai commi 1 e 2 dell'articolo 17 del decreto legislativo 17 gennaio 2003 n. 5, si effettuano ai sensi dell'articolo 170 del codice di procedura civile.][34]

5. All'articolo 16 del regio decreto legge 27 novembre 1933, n. 1578, convertito, con modificazioni, dalla legge 22 gennaio 1934, n. 36, sono apportate le seguenti modificazioni:

a) dopo il primo comma è aggiunto il seguente: "Nell'albo è indicato l'indirizzo elettronico attribuito a ciascun professionista dal punto di accesso ai sensi dell'articolo 7 del regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2001, n. 123" [35];

b) il quarto comma è sostituito dal seguente: "A decorrere dalla data fissata dal Ministro della giustizia con decreto emesso sentiti i Consigli dell'Ordine, gli albi riveduti debbono essere comunicati per via

---

[31] Il testo originario del primo comma dell'art. 51, così come modificato dall'art. 1, co. 1, legge 6 agosto 2008, n. 133, era il seguente: "1. A decorrere dalla data fissata con uno o piu' decreti del Ministro della giustizia, le notificazioni e comunicazioni di cui al primo comma dell'articolo 170 del codice di procedura civile, la notificazione di cui al primo comma dell'articolo 192 del codice di procedura civile e ogni altra comunicazione al consulente sono effettuate per via telematica all'indirizzo elettronico comunicato ai sensi dell'articolo 7 del regolamento di cui al decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, nel rispetto della normativa, anche regolamentare, relativa al processo telematico, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici". Successivamente il comma è stato sostituito dall'articolo 4, comma 3, lettera a), del D.L. 29 dicembre 2009, n. 193, convertito con modificazioni in Legge 22 febbraio 2010, n. 24 (testo tra le parentesi quadre) e da ultimo abrogato dall'articolo 16, comma 11, del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni in Legge 17 dicembre 2012, n. 221.

[32] Comma sostituito dall'articolo 4, comma 3, lettera a), del D.L. 29 dicembre 2009, n. 193, convertito con modificazioni in Legge 22 febbraio 2010, n. 24 (testo tra le parentesi quadre) e successivamente abrogato dall'articolo 16, comma 11, del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni in Legge 17 dicembre 2012, n. 221.

[33] Comma sostituito dall'articolo 4, comma 3, lettera a), del D.L. 29 dicembre 2009, n. 193, convertito con modificazioni in Legge 22 febbraio 2010, n. 24 (testo tra le parentesi quadre) e successivamente abrogato dall'articolo 16, comma 11, del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni in Legge 17 dicembre 2012, n. 221.

[34] Comma abrogato dal D.L. 18 ottobre 2012, n. 179, convertito con modificazioni in Legge 17 dicembre 2012, n. 221.

[35] Lettera modificata dall'articolo 1, comma 1, della Legge 6 agosto 2008, n. 133, in sede di conversione.

telematica, a cura del Consiglio, al Ministero della giustizia nelle forme previste dalle regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile".

(ritorna all'indice cronologico)

(*ritorna all'indice per argomenti*)

Decreto Legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 - Obbligo delle imprese, dei professionisti e della Pubbliche Amministrazioni di comunicare il proprio indirizzo PEC [36]

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 16

(Riduzione dei costi amministrativi a carico delle imprese)

1-5 (*omissis*).

6. Le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese *o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali.* Entro tre anni dalla data di entrata in vigore *del presente decreto* tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, comunicano al registro delle imprese l'indirizzo di posta elettronica certificata. L'iscrizione dell'indirizzo di posta elettronica certificata nel registro delle imprese e le sue successive eventuali variazioni sono esenti dall'imposta di bollo e dai diritti di segreteria.

6*bis*. L'ufficio del registro delle imprese che riceve una domanda di iscrizione da parte di un'impresa costituita in forma societaria che non ha iscritto il proprio indirizzo di posta elettronica certificata, in luogo dell'irrogazione della sanzione prevista dall'articolo 2630 del codice civile, sospende la domanda per tre mesi, in attesa che essa sia integrata con l'indirizzo di posta elettronica certificata[37].

7. I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata *o analogo indirizzo di posta elettronica di cui al comma 6* entro un anno dalla data di entrata in vigore *del presente decreto. Gli ordini e i collegi pubblicano in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.*

8. Le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, qualora non abbiano provveduto ai sensi dell'articolo 47, comma 3, lettera *a)*, del Codice dell'Amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, istituiscono una casella di posta certificata *o analogo indirizzo di posta elettronica di cui al comma 6* per ciascun registro di protocollo e ne danno comunicazione al Centro nazionale per l'informatica nella pubblica amministrazione, che provvede alla pubblicazione di tali caselle in un elenco consultabile per via telematica. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e si deve provvedere nell'ambito delle risorse disponibili.

9. Salvo quanto stabilito dall'articolo 47, commi 1 e 2, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, le comunicazioni tra i soggetti *di cui ai commi 6, 7 e* 8 del presente articolo, che abbiano provveduto agli adempimenti ivi previsti, possono essere inviate attraverso la posta elettronica certificata *o analogo indirizzo di posta elettronica di cui al comma 6*, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.

10. La consultazione per via telematica dei singoli indirizzi di posta elettronica certificata *o analoghi indirizzi di posta elettronica di cui al comma 6* , nel registro delle imprese o negli albi o elenchi costituiti *ai sensi* del presente articolo avviene liberamente e senza oneri. L'estrazione di elenchi di indirizzi è consentita alle sole pubbliche amministrazioni per le comunicazioni relative agli adempimenti amministrativi di loro competenza.

(*omissis*)

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)
(torna all'art. 16ter d.l. 179 del 2012)

[36] Per le ditte individuali cfr: art. 5 d.l. 179/2012.

[37] Comma introdotto dall'art. 37 del decreto legge 9 febbraio 2012, n. 5 convertito, con modificazioni nella legge 4 aprile 2012, n. 35.

D.M. 27 aprile 2009 - Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia (G.U. 11 maggio 2009, n. 107)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

IL MINISTRO DELLA GIUSTIZIA

Vista la legge 2 dicembre 1991, n. 399, recante: «Delegificazione delle norme concernenti i registri che devono essere tenuti presso gli uffici giudiziari e l'amministrazione penitenziaria»;
Visto l'*art. 206 del decreto legislativo 28 luglio 1989, n. 271* recante le Norme di attuazione, di coordinamento e transitorie del Codice di Procedura Penale;
Visto il decreto legislativo 12 febbraio 1993, n. 39, recante: «Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, ai sensi dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421»;
Visto il decreto del Presidente della Repubblica 28 ottobre 1994, n. 748, recante il regolamento sulle modalità applicative del decreto legislativo 12 febbraio 1993, n. 39, in relazione all'amministrazione della giustizia;
Visto il decreto legislativo 30 giugno 2003, n. 196, recante: «Codice in materia di protezione dei dati personali»;
Visto il decreto legislativo 7 marzo 2005, n. 82, recante: «Codice dell'Amministrazione digitale»;
Visto il decreto 27 marzo 2000, n. 264, del Ministro della giustizia, pubblicato nella Gazzetta Ufficiale del 26 settembre 2000, n. 225, recante il regolamento sulla tenuta dei registri presso gli uffici giudiziari;
Visto l'art. 1, comma 1, lettera f), del citato decreto n. 264 del 2000, che prevede l'emanazione di regole procedurali;
Visto il decreto ministeriale 24 maggio 2001 concernente: «Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia», pubblicato nella Gazzetta Ufficiale del 5 giugno 2001, n. 128;
Visto il parere reso dal Centro per l'informatica nella pubblica amministrazione in data 29 maggio 2008;
Consultato il Garante per la protezione dei dati personali;
Decreta:

Art. 1.

1. Il presente decreto fissa, in sostituzione del decreto ministeriale 24 maggio 2001 , le regole procedurali per la gestione del sistema informatico del Ministero della giustizia e per la tenuta informatizzata dei registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero ai registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'amministrazione della giustizia, come previsti dall' art. 1 del decreto ministeriale 27 marzo 2000, n. 264 .
2. Per le modalità di tenuta informatizzata dei registri e per la sottoscrizione con firma digitale dei documenti informatici si tiene conto anche delle regole tecniche emanate ai sensi del decreto legislativo 7 marzo 2005, n. 82 «Codice dell'Amministrazione digitale».
3. Le regole procedurali di cui al comma 1 sono riportate nell'allegato al presente decreto.

Allegato *ex* art. 1
Regole procedurali per la tenuta dei registri informatizzati degli uffici

Art. 1
Definizioni

1. Ai fini del presente decreto si intende per:
a) Sistema informativo: l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione (sia in formato cartaceo sia elettronico) che, nel loro complesso, consentono qualunque operazione o complesso di operazioni, concernenti il trattamento dei dati e delle informazioni anche personali relativi alla tenuta dei registri connessi all'espletamento delle attribuzioni e dei servizi svolti dalla Amministrazione della giustizia.
b) Sistema informatico: la parte del sistema informativo che gestisce informazioni con tecnologia informatica e, per estensione, le sale server ovvero i locali attrezzati che ospitano i sistemi server.
c) Risorse informatiche: hardware, software, apparati di rete e cablaggi, sale server.

d) Servizi informatici: le risorse informatiche e i servizi per loro tramite forniti, sia di natura applicativa sia sistemistica.
e) Amministrazione: il Ministero della giustizia.
f) D.G.S.I.A.: la Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della giustizia.
g) Responsabile S.I.A.: il responsabile per i sistemi informativi automatizzati ai sensi dell' articolo 10 del decreto legislativo 12 febbraio 1993, n. 39 , quale direttore generale della D.G.S.I.A.
h) C.I.S.I.A.: Coordinamento Interdistrettuale per i Sistemi Informativi Automatizzati, articolazione territoriale della D.G.S.I.A., come prevista dal *D.M. 18 dicembre 2001* e successive modifiche.
i) Dirigente informatico: il dirigente amministrativo in possesso dei requisiti di cui all' art. 11 del decreto legislativo 12 febbraio 1993, n. 39 e preposto alla direzione di un C.I.S.I.A. o i un ufficio della D.G.S.I.A.
j) ADSI: l'amministratore dei servizi informatici.
k) Fornitore qualificato: il fornitore ricompreso negli elenchi di fornitori a livello nazionale e regionale di cui all' art. 82 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.
l) Struttura per la sicurezza del distretto: organizzazione per la sicurezza informatica degli uffici giudiziari del distretto.

Art. 2
Requisiti del sistema informatico

1. Il sistema informatico soddisfa i seguenti requisiti:
a) disponibilità: i dati sono formati, raccolti, conservati, resi disponibili e accessibili in modo da assicurarne l'uso interno e la fruizione, anche in caso di eventi interruttivi del funzionamento dei sistemi, compatibilmente con i livelli di servizio prestabiliti;
b) integrità: i dati sono trattati in modo da assicurarne precisione, completezza e inalterabilità;
c) autenticità: la provenienza dei dati è garantita e asseverata;
d) controllo degli accessi fisici e logici: le informazioni possono essere fruite solo ed esclusivamente dalle persone autorizzate a compiere tale operazione.

Art. 3
Organizzazione del sistema informatico

1. Il sistema informatico del Ministero della giustizia è articolato a livello nazionale, interdistrettuale, distrettuale e locale.
2. Il livello nazionale è costituito dalle componenti relative agli uffici dell'Amministrazione centrale, della Corte di Cassazione, della Procura Generale presso la Corte di Cassazione, del Tribunale Superiore delle Acque Pubbliche e della Direzione Nazionale antimafia e da quelle relative all'erogazione di servizi comuni o centralizzati.
3. Il livello interdistrettuale è costituito dalle componenti relative agli uffici di più distretti di Corte di Appello e da quelle relative all'erogazione di servizi comuni agli ambiti di uffici di più distretti.
4. Il livello distrettuale è costituito dalle componenti relative agli uffici della sede di distretto di Corte di Appello e da quelle relative all'erogazione di servizi comuni agli ambiti distrettuale e locale.
5. Il livello locale è costituito dalle componenti relative agli uffici periferici del distretto di Corte di Appello.
6. Le strutture elaborative serventi sono allocate in corrispondenza delle componenti di cui ai commi precedenti.
7. Il Responsabile S.I.A. emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul portale internet dell'Amministrazione.

Art. 4
Amministratore dei servizi informatici

1. L'amministratore dei servizi informatici (ADSI) assicura la conduzione operativa di specifiche componenti del sistema informatico, effettuando, anche mediante accesso remoto, tutte le operazioni necessarie a garantire i requisiti di cui all' art. 2 .
2. Un coordinatore degli ADSI viene nominato qualora vi sia la necessità che più amministratori operino su componenti identiche o affini del sistema informatico.
3. É in ogni caso prevista la nomina di un coordinatore degli ADSI per ciascuna delle sale server nazionali, interdistrettuali e distrettuali.

4. Il Responsabile S.I.A., su proposta del dirigente informatico competente per territorio o per settore, designa i soggetti di cui ai commi 1, 2 e 3, individuandoli fra gli esperti informatici dell'Amministrazione ovvero, se non sono disponibili tali risorse, ricorrendo a personale esterno qualificato.
5. L'amministratore dei servizi informatici, se nominato responsabile del trattamento da parte dei titolari delle banche dati, pone in essere le iniziative necessarie per il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri, anche alla luce delle direttive concordemente emanate dai titolari delle banche dati.
6. In ogni caso, l'amministratore dei servizi informatici garantisce che il capo dell'ufficio giudiziario, o un suo delegato, possa accedere alla infrastruttura logistica condivisa per verificare il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri.

Art. 5
Identificazione delle componenti del sistema informatico

1. La D.G.S.I.A. produce e mantiene aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informatico.
2. La D.G.S.I.A. definisce la struttura dell'inventario ed i criteri di accesso e conservazione delle informazioni in esso contenute.
3. L'amministratore dei servizi informatici predispone un dettagliato inventario delle componenti del sistema informatico di sua competenza secondo la struttura di cui al comma 2 e lo mantiene aggiornato ogni qualvolta si verifica una variazione.
4. L'inventario di cui al comma 1 è reso disponibile a tutti gli uffici interessati.

Art. 6
Piano di distribuzione delle risorse informatiche

1. L'amministratore dei servizi informatici redige il piano delle risorse informatiche da dedicare all'erogazione dei servizi messi a disposizione degli uffici e lo trasmette al dirigente informatico competente ed agli uffici interessati.
2. La D.G.S.I.A. pianifica la destinazione delle risorse che compongono il sistema informatico in coerenza con i servizi che devono essere erogati, tenendo conto dei piani di cui al comma 1.

Art. 7
Gestione della sicurezza del sistema informativo

1. Il Responsabile S.I.A. predispone il documento programmatico della sicurezza di cui all' art. 34 del decreto legislativo 30 giugno 2003, n. 196 , relativamente alle componenti del sistema informatico dell'Amministrazione, che sono centralmente gestite e controllate.
2. Gli uffici, con la collaborazione tecnica del CISIA competente, predispongono il documento programmatico della sicurezza di cui all' art. 34 del decreto legislativo 30 giugno 2003, n. 196 , relativamente al sistema informativo di propria competenza e lo rendono disponibile al Responsabile S.I.A.
3. Per le infrastrutture logistiche comuni il piano è predisposto in modo condiviso dagli uffici.
4. La vigilanza sulla applicazione dei documenti di cui ai precedenti commi 1 e 2, è esercitata dal Responsabile S.I.A., o da suoi delegati, che segnala eventuali difformità comportamentali ai capi degli uffici ed adotta, in caso di urgenza, le misure e i provvedimenti necessari ad assicurare il corretto funzionamento del sistema informatico.

Art. 8
Politica di gestione degli accessi

1. Ogni utente, preliminarmente all'accesso alle risorse del sistema informatico, è identificato tramite procedure di autenticazione, definita e gestita dal Responsabile S.I.A.
2. Il Responsabile S.I.A. individua ed aggiorna periodicamente, con proprio decreto, la procedura di autenticazione. L'autenticazione prevede, come misura minima per l'identificazione, la conoscenza di una coppia di informazioni (username e password), secondo quanto previsto dal disciplinare tecnico di cui all' Allegato B del Codice in materia di protezione dei dati personali.
3. Ogni utente ottiene, tramite la procedura di autorizzazione, uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo di autorizzazione, rispetto alle risorse del sistema informatico.
4. A ciascun insieme omogeneo di utenti è associato un solo profilo; a ciascun utente può essere assegnato uno o più profili.

5. Ogni profilo è definito in modo tale da assegnare a ciascun utente solo ed esclusivamente i privilegi strettamente necessari per l'espletamento delle attività di propria competenza.
6. La struttura per la sicurezza del distretto individua i referenti degli uffici per l'assegnazione agli utenti dei profili relativi al trattamento dei dati.
7. Il Responsabile S.I.A., o suoi delegati, assegna agli amministratori dei servizi informatici uno o più profili volti alla conduzione, anche remota, dei sistemi e delle postazioni di lavoro e ne dà comunicazione agli uffici interessati.

Art. 9
Salvataggio e conservazione dei dati

1. Il Responsabile S.I.A. definisce, con proprio decreto, le politiche e le procedure per il salvataggio (backup) e per il recupero (recovery) dei dati.
2. Nell'ambito delle misure di cui al comma 1, la frequenza del salvataggio dei dati avviene con cadenza almeno giornaliera.
3. Le procedure di backup consentono di conservare i dati secondo le regole tecniche emanate ai sensi degli articoli 22 e 71 del decreto legislativo 7 marzo 2005, n. 82 .
4. Le procedure di backup consentono di effettuare, con frequenza almeno triennale, una copia storica dei dati, che dovrà essere conservata secondo le modalità di cui al comma 3. Eseguita tale operazione, dal registro in uso possono essere eliminati i dati relativi agli affari esauriti da almeno due anni.
5. Il sistema di consultazione della copia storica dei dati ne garantisce la leggibilità nel tempo e l'autenticità, secondo le regole tecniche emanate ai sensi degli articoli 22 e 71 del decreto legislativo 7 marzo 2005, n. 82 .

Art. 10
Monitoraggio del sistema

1. Le attività relative all'utilizzo e alla gestione del sistema informatico, anche da remoto, sono sottoposte ad un processo continuo di controllo e verifica della loro corretta e completa esecuzione. Il processo di controllo e verifica si attua anche attraverso l'utilizzo di appositi strumenti di controllo a livello di sistema, di database management system, di applicativo e di postazione di lavoro.
2. Il sistema informatico prevede, a garanzia della autenticità e della integrità dei dati e come misura minima di monitoraggio, la registrazione di tutti gli accessi, anche di carattere tecnico, ivi compresi quelli non riusciti o falliti, e di tutte le operazioni effettuate sui dati.
3. La D.G.S.I.A. si dota degli strumenti di monitoraggio di cui al comma 1, per consentire al personale tecnico di svolgere le opportune verifiche. La D.G.S.I.A. è responsabile delle attività di cui al comma 1 e vigila sullo svolgimento delle stesse, anche se affidate a personale esterno specificamente individuato.
4. Le registrazioni dei log delle attività di cui al comma 1, devono essere trascritte con cadenza almeno settimanale su supporti non riscrivibili da conservare unitamente ai backup.
5. La struttura per la sicurezza del distretto, i titolari ed i responsabili per il trattamento dei dati hanno facoltà di esaminare, nell'ambito delle rispettive competenze, le registrazioni di cui al comma 4.

Art. 11
Infrastruttura logistica

1. Il Responsabile S.I.A. predispone, con proprio decreto, le linee guida per l'allestimento dei locali adibiti a sale server.
2. Le linee guida di cui al comma 1, prevedono almeno le indicazioni relative alla localizzazione e predisposizione tecnologica delle sale server, alle procedure per l'accesso alle sale server ed alle procedure per la conservazione fisica dei supporti di backup.
3. Il Responsabile S.I.A., se non vi è disponibilità di locali di proprietà o messi a disposizione dell'Amministrazione giudiziaria, ha facoltà di utilizzare sale server di fornitori qualificati che rispondono alle linee guida di cui al comma 1.
4. Il dirigente informatico è responsabile della gestione delle sale server nel territorio o settore di sua competenza. Egli può delegare alcune di tali attività ad un ADSI.
5. Il dirigente informatico, o persona dallo stesso delegata, partecipa alle riunioni della Commissione di manutenzione di cui alla legge 24 aprile 1941, n. 392 , nel territorio assegnato alla sua competenza.

Art. 12
Software

1. É consentito installare ed utilizzare unicamente il software preventivamente approvato dal Responsabile S.I.A. secondo quanto previsto dall' articolo 3, comma 2, del decreto ministeriale 27 marzo 2000, n. 264.
2. L'elenco dei software nazionali con le relative funzionalità fornite è pubblicato sul sito dell'Amministrazione.
3. Non è consentito utilizzare o sperimentare software, in deroga a quanto previsto al comma 1, salvo specifica autorizzazione del Responsabile S.I.A.
4. Il software è installato esclusivamente a partire da supporti fisici originali, ovvero per i quali sia nota e sicura la provenienza.
5. Il software e la relativa documentazione, realizzati per conto della D.G.S.I.A., sono prodotti in maniera conforme alle regole tecniche dettate dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

Art. 13
Dati in formato elettronico

1. L'accesso ai dati da parte degli utenti avviene esclusivamente per il tramite del software di cui all' articolo 12.
2. Tutte le operazioni di manutenzione effettuate sui dati sono soggette ad autorizzazione e registrazione secondo quanto previsto dall' articolo 10.
3. Il dirigente o responsabile dell'ufficio è responsabile della qualità dei dati e ne verifica periodicamente, anche attraverso il personale dell'ufficio all'uopo incaricato ed anche utilizzando strumenti automatici, correttezza ed aggiornamento, assumendo le conseguenti iniziative.
4. Il dirigente o responsabile dell'ufficio può nominare uno o più delegati per le attività di controllo sui dati di propria competenza.
5. La delega di cui al comma precedente è attribuita al personale dell'ufficio o, nel caso previsto dall' articolo 3 , di altro ufficio.

Art. 14
Applicativi per la tenuta dei registri

1. L'applicativo è accompagnato da apposita documentazione di utilizzo, costituita da un manuale di amministrazione ed un manuale di utilizzo, disponibile sia in forma cartacea che in forma elettronica.
2. Il Responsabile S.I.A. predispone, con proprio decreto, le linee guida per la redazione della documentazione di cui al comma precedente.
Art. 15 Disposizioni per la salvaguardia dei dati
1. Il Responsabile S.I.A. definisce, con proprio decreto, la politica della sicurezza dei sistemi informatici della giustizia.
2. Il Responsabile S.I.A. adotta, con il decreto di cui al comma 1, o con successivo provvedimento, le linee guida relative, fra l'altro, a:
a) modalità di gestione delle utenze;
b) modalità di comportamento delle utenze agli effetti della sicurezza informatica;
c) controllo fisico e logico degli accessi ai sistemi informatici;
d) politiche, modalità esecutive e strumenti per la salvaguardia dei dati (backup, disaster recovery, ecc.);
e) politiche e modalità esecutive per la conservazione e la riproduzione dei supporti fisici dei dati;
f) gestione dei sistemi di protezione dagli attacchi informatici (antivirus, antispam, firewall, IDS, IPS, ecc.);
g) modalità e strumenti di supporto per il controllo e il monitoraggio della sicurezza informatica;
h) procedure di verifica e controllo dei livelli di sicurezza informatica;
i) politiche per la formazione degli utenti in tema di sicurezza informatica.

(ritorna all'indice cronologico)

Decreto Legge 29 dicembre 2009, n. 193, convertito con modificazioni nella legge 22 febbraio 2010, n. 24 - Interventi urgenti in materia di funzionalità del sistema giudiziario. (G.U. 30 dicembre, n. 302) (Estratto)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

ART. 4

Misure urgenti per la digitalizzazione della giustizia

1. Con uno o più decreti del Ministro della giustizia, di concerto con il Ministro per la pubblica amministrazione e l'innovazione, sentito il Centro nazionale per l'informatica nella pubblica amministrazione e il Garante per la protezione dei dati personali, adottati, ai sensi dell'articolo 17 comma 3, della legge 23 agosto 1988, n. 400, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono individuate le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni. Le vigenti regole tecniche del processo civile telematico continuano ad applicarsi fino alla data di entrata in vigore dei decreti di cui ai commi 1 e 2.

2. Nel processo civile e nel processo penale, tutte le comunicazioni e notificazioni per via telematica si effettuano [, nei casi consentiti], mediante posta elettronica certificata, ai sensi del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e delle regole tecniche stabilite con i decreti previsti dal comma 1. Fino alla data di entrata in vigore dei predetti decreti, le notificazioni e le comunicazioni sono effettuate nei modi e nelle forme previste dalle disposizioni vigenti alla data di entrata in vigore del presente decreto.

3-8ter (*omissis*)

9. Per consentire il pagamento, da parte dei privati, con sistemi telematici di pagamento ovvero con carte di debito, di credito o prepagate o con altri mezzi di pagamento con moneta elettronica disponibili nei circuiti bancario e postale, del contributo unificato, del diritto di copia, del diritto di certificato, delle spettanze degli ufficiali giudiziari relative ad attività di notificazione ed esecuzione, delle somme per il recupero del patrocinio a spese dello Stato, delle spese processuali, delle spese di mantenimento, delle pene pecuniarie, delle sanzioni amministrative pecuniarie e delle sanzioni pecuniarie il Ministero della giustizia si avvale, senza nuovi o maggiori oneri a carico del bilancio dello Stato, di intermediari abilitati che, ricevuto il versamento delle somme, ne effettuano il riversamento alla Tesoreria dello Stato, registrando in apposito sistema informatico a disposizione dell'amministrazione i pagamenti eseguiti e la relativa causale, la corrispondenza di ciascun pagamento, i capitoli e gli articoli d'entrata. Entro 60 giorni dalla data di entrata in vigore del presente decreto il Ministro della giustizia, di concerto con il Ministro dell'economia e delle finanze, determina con proprio decreto, sentito il Centro nazionale per l'informatica nella pubblica amministrazione, le modalità tecniche per il riversamento, la rendicontazione e l'interconnessione dei sistemi di pagamento, nonché il modello di convenzione che l'intermediario abilitato deve sottoscrivere per effettuare servizio. Il Ministero della giustizia, di concerto con il Ministero dell'economia e delle finanze, stipula apposite convenzioni a seguito di procedura di gara ad evidenza pubblica per la fornitura dei servizi e delle infrastrutture senza nuovi o maggiori oneri a carico del bilancio dello Stato. Le convenzioni di cui al presente articolo prevedono che gli oneri derivanti dall'allestimento e dal funzionamento del sistema informatico sono a carico degli intermediari abilitati.

(torna all'Avvertenza)

(ritorna all'indice cronologico)
(*torna all'indice per argomenti*)

D.M. 21 febbraio 2011 n. 44 - Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24 (G.U. 18 aprile, n. 89)

(ritorna all'indice cronologico)

IL MINISTRO DELLA GIUSTIZIA
di concerto con
IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE E L'INNOVAZIONE
(omissis)
a d o t t a il seguente regolamento:

CAPO I
PRINCIPI GENERALI

Art. 1
Ambito di applicazione

1. Il presente decreto stabilisce le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione ai sensi dell'articolo 4, comma 1, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24, recante «Interventi urgenti in materia di funzionalità del sistema giudiziario» ed in attuazione del decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale» e successive modificazioni.

Art. 2
Definizioni

1. Ai fini del presente decreto si intendono per:
a) **dominio giustizia**: l'insieme delle risorse hardware e software, mediante il quale il Ministero della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura;
b) **portale dei servizi telematici**: struttura tecnologica-organizzativa che fornisce l'accesso ai servizi telematici resi disponibili dal dominio giustizia, secondo le regole tecnico-operative riportate nel presente decreto;
c) **punto di accesso**: struttura tecnologica-organizzativa che fornisce ai soggetti abilitati esterni al dominio giustizia i servizi di connessione al portale dei servizi telematici, secondo le regole tecnico-operative riportate nel presente decreto;
d) **gestore dei servizi telematici**: sistema informatico, interno al dominio giustizia, che consente l'interoperabilità tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia;
e) **posta elettronica certificata**: sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;
f) **identificazione informatica**: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, mediante un certificato di autenticazione, secondo la definizione di cui al decreto legislativo 7 marzo 2005, n. 82;
g) **firma digitale**: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 7 marzo 2005, n. 82;
h) **fascicolo informatico**: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, oppure le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo, ai sensi del codice dell'amministrazione digitale;
i) **codice dell'amministrazione digitale (CAD)**: decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;
l) **codice in materia di protezione dei dati personali**: decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modificazioni;

m) **soggetti abilitati**: i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:
1) **soggetti abilitati interni**: i magistrati, il personale degli uffici giudiziari e degli UNEP;
2) **soggetti abilitati esterni**: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;
3) **soggetti abilitati esterni privati**: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;
4) **soggetti abilitati esterni pubblici**: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali, regionali, metropolitane, provinciali e comunali;
n) **utente privato**: la persona fisica o giuridica, quando opera al di fuori dei casi previsti dalla lettera m);
o) **certificazione del soggetto abilitato esterno privato**: attestazione di iscrizione all'albo, all'albo speciale, al registro ovvero di possesso della qualifica che legittima l'esercizio delle funzioni professionali e l'assenza di cause ostative all'accesso;
p) **certificazione del soggetto abilitato esterno pubblico**: attestazione di appartenenza del soggetto all'amministrazione pubblica e dello svolgimento di funzioni tali da legittimare l'accesso;
q) **specifiche tecniche**: le disposizioni di carattere tecnico emanate, ai sensi dell'articolo 34, dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e il Garante per la protezione dei dati personali, limitatamente ai profili inerenti la protezione dei dati personali;
r) **spam**: messaggi indesiderati;
s) **software antispam**: software studiato e progettato per rilevare ed eliminare lo spam;
t) **log**: documento informatico contenente la registrazione cronologica di una o più operazioni informatiche, generato automaticamente dal sistema informatico;
u) **richiesta di pagamento telematico (RPT)**: struttura standardizzata che definisce gli elementi necessari a caratterizzare il pagamento e qualifica il versamento con un identificativo univoco, nonché contiene i dati identificativi, variabili secondo il tipo di operazione, e una parte riservata per inserire informazioni elaborabili automaticamente dai sistemi informatici;
v) **ricevuta telematica (RT)**: struttura standardizzata, emessa a fronte di una RPT, che definisce gli elementi necessari a qualificare il pagamento e trasferisce inalterate le informazioni della RPT relative alla parte riservata;
z) **identificativo univoco di erogazione del servizio (CRS)**: identifica univocamente una richiesta di erogazione del servizio ed è associato alla RPT e alla RT al fine di qualificare in maniera univoca il versamento;
aa) **prestatore dei servizi di pagamento**: gli istituti di credito, Poste Italiane e gli altri soggetti che, ai sensi del decreto legislativo 27 gennaio 2010 n. 11 e successive modifiche ed integrazioni, mettono a disposizione strumenti atti ad effettuare pagamenti.

CAPO II
SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Art. 3
Funzionamento dei sistemi del dominio giustizia

1. I sistemi del dominio giustizia sono strutturati in conformità al codice dell'amministrazione digitale, alle disposizioni del Codice in materia di protezione dei dati personali e in particolare alle prescrizioni in materia di sicurezza dei dati, nonché al decreto ministeriale emanato a norma dell'articolo 1, comma 1, lettera f), del decreto del Ministro della giustizia 27 marzo 2000, n. 264.
2. Il responsabile per i sistemi informativi automatizzati del Ministero della giustizia è responsabile dello sviluppo, del funzionamento e della gestione dei sistemi informatici del dominio giustizia.
3. I dati sono custoditi in infrastrutture informatiche di livello distrettuale o interdistrettuale, secondo le specifiche di cui all'articolo 34.

Art. 4
Gestore della posta elettronica certificata del Ministero della giustizia

1. Salvo quanto previsto all'articolo 19, il Ministero della giustizia si avvale di un proprio servizio di posta elettronica certificata conforme a quanto previsto dal codice dell'amministrazione digitale.
2. Gli indirizzi di posta elettronica certificata degli uffici giudiziari e degli UNEP, da utilizzare unicamente per i servizi di cui al presente decreto, sono pubblicati sul portale dei servizi telematici e rispettano le specifiche tecniche stabilite ai sensi dell'articolo 34.

3. Il Ministero della giustizia garantisce la conservazione dei log dei messaggi transitati attraverso il proprio gestore di posta elettronica certificata per cinque anni.

Art. 5
Gestore dei servizi telematici

1. Il gestore dei servizi telematici assicura l'interoperabilità tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia.

Art. 6
Portale dei servizi telematici

1. Il portale dei servizi telematici consente l'accesso da parte dell'utente privato alle informazioni, ai dati e ai provvedimenti giudiziari secondo quanto previsto dall'articolo 51 del codice in materia di protezione dei dati personali.
2. L'accesso di cui al comma 1 avviene a norma dell'articolo 64 del codice dell'amministrazione digitale e secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. Il portale dei servizi telematici mette a disposizione dei soggetti abilitati esterni i servizi di consultazione, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Il portale dei servizi telematici mette a disposizione i servizi di pagamento telematico, secondo quanto previsto dal capo V del presente decreto.
5. Il portale dei servizi telematici mette a disposizione dei soggetti abilitati e degli utenti privati, in un'apposita area, i documenti che contengono dati sensibili oppure che eccedono le dimensioni del messaggio di posta elettronica certificata di cui all'articolo 13, comma 8, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26.
6. Il portale dei servizi telematici consente accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione, alle informazioni ed alla documentazione sui servizi telematici del dominio giustizia, alle raccolte giurisprudenziali e alle informazioni essenziali sullo stato dei procedimenti pendenti, che vengono rese disponibili in forma anonima.

(*torna all'indice per argomenti*)

Art. 7
Registro generale degli indirizzi elettronici

1. Il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia, contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei soggetti abilitati esterni di cui al comma 3 e degli utenti privati di cui al comma 4.
2. Per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, il registro generale degli indirizzi elettronici è costituito mediante i dati contenuti negli elenchi riservati di cui all'articolo 16, comma 7, del Decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009 n. 2, inviati al Ministero della giustizia secondo le specifiche tecniche di cui all'articolo 34.
3. Per i soggetti abilitati esterni non iscritti negli albi di cui al comma 2, il registro generale degli indirizzi elettronici è costituito secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Per le persone fisiche, quali utenti privati, che non operano nelle qualità di cui ai commi 2 e 3, gli indirizzi sono consultabili ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
5. Per le imprese, gli indirizzi sono consultabili, senza oneri, ai sensi dell'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009 n. 2, con le modalità di cui al comma 10 del medesimo articolo e secondo le specifiche tecniche di cui all'articolo 34.
6. Il registro generale degli indirizzi elettronici è accessibile ai soggetti abilitati mediante le specifiche tecniche stabilite ai sensi dell'articolo 34.

(*torna all'indice per argomenti*)
(*torna all'art. 16ter d.l. 179 del 2012*)

Art. 8
Sistemi informatici per i soggetti abilitati interni

1. I sistemi informatici del dominio giustizia mettono a disposizione dei soggetti abilitati interni le funzioni di ricezione, accettazione e trasmissione dei dati e dei documenti informatici nonché di consultazione e gestione del fascicolo informatico, secondo le specifiche di cui all'articolo 34.

2. L'accesso dei soggetti abilitati interni è effettuato con le modalità definite dalle specifiche tecniche di cui all'articolo 34, che consentono l'accesso anche dall'esterno del dominio giustizia.
3. Nelle specifiche di cui al comma 2 sono disciplinati i requisiti di legittimazione e le credenziali di accesso al sistema da parte delle strutture e dei soggetti abilitati interni.

Art. 9
Sistema informatico di gestione del fascicolo informatico

1. Il Ministero della giustizia gestisce i procedimenti utilizzando le tecnologie dell'informazione e della comunicazione, raccogliendo in un fascicolo informatico gli atti, i documenti, gli allegati, le ricevute di posta elettronica certificata e i dati del procedimento medesimo da chiunque formati, ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.
2. Il sistema di gestione del fascicolo informatico è la parte del sistema documentale del Ministero della giustizia dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno, secondo le specifiche tecniche di cui all'articolo 34.
3. La tenuta e conservazione del fascicolo informatico equivale alla tenuta e conservazione del fascicolo d'ufficio su supporto cartaceo, fermi restando gli obblighi di conservazione dei documenti originali unici su supporto cartaceo previsti dal codice dell'amministrazione digitale e dalla disciplina processuale vigente.
4. Il fascicolo informatico reca l'indicazione:
a) dell'ufficio titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) dell'oggetto del procedimento;
c) dell'elenco dei documenti contenuti.
5. Il fascicolo informatico è formato in modo da garantire la facile reperibilità ed il collegamento degli atti ivi contenuti in relazione alla data di deposito, al loro contenuto, ed alle finalità dei singoli documenti.
6. Con le specifiche tecniche di cui all'articolo 34 sono definite le modalità per il salvataggio dei log relativi alle operazioni di accesso al fascicolo informatico.

(*torna all'indice per argomenti*)

Art. 10
Infrastruttura di comunicazione

1. I sistemi informatici del dominio giustizia utilizzano l'infrastruttura tecnologica resa disponibile nell'ambito del Sistema Pubblico di Connettività per le comunicazioni con l'esterno del dominio giustizia.

CAPO III
TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Art. 11
Formato dell'atto del processo in forma di documento informatico

1. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto nei formati previsti dalle specifiche tecniche di cui all'articolo 34; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, pubblicate sul portale dei servizi telematici.
2. La nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale; le relative informazioni sono contenute nelle informazioni strutturate di cui al primo comma, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

Art. 12
Formato dei documenti informatici allegati

1. I documenti informatici allegati all'atto del processo sono privi di elementi attivi e hanno i formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.
2. È consentito l'utilizzo dei formati compressi, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, purché contenenti solo file nei formati previsti dal comma precedente.

Art. 13
Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati

1. I documenti informatici di cui agli articoli 11 e 12 sono trasmessi da parte dei soggetti abilitati esterni e degli utenti privati mediante l'indirizzo di posta elettronica certificata risultante dal registro generale degli

indirizzi elettronici, all'indirizzo di posta elettronica certificata dell'ufficio destinatario, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. I documenti informatici di cui al comma 1 si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della giustizia.
3. Nel caso previsto dal comma 2 la ricevuta di avvenuta consegna attesta, altresì, l'avvenuto deposito dell'atto o del documento presso l'ufficio giudiziario competente. Quando la ricevuta è rilasciata dopo le ore 14 il deposito si considera effettuato il giorno feriale immediatamente successivo.[38]
4. [Ai fini della comunicazione prevista dall'articolo 170, quarto comma, del codice di procedura civile, la parte che procede al deposito invia ai procuratori delle parti costituite copia informatica dell'atto e dei documenti allegati con le modalità previste dall'articolo 18 del presente decreto.] [Fuori del caso di rifiuto per omessa sottoscrizione,] il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dalla vigente normativa processuale.[39]
5. La certificazione dei professionisti abilitati e dei soggetti abilitati esterni pubblici è effettuata dal gestore dei servizi telematici sulla base dei dati presenti nel registro generale degli indirizzi elettronici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
6. Al fine di garantire la riservatezza dei documenti da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
7. Il gestore dei servizi telematici restituisce al mittente l'esito dei controlli effettuati dal dominio giustizia nonché dagli operatori della cancelleria o della segreteria, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
8. La dimensione massima del messaggio è stabilita nelle specifiche tecniche di cui all'articolo 34. Se il messaggio eccede tale dimensione, il gestore dei servizi telematici genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
9. I soggetti abilitati esterni possono avvalersi dei servizi del punto di accesso, di cui all'articolo 23, per la trasmissione dei documenti; in tale caso il punto di accesso si attiene alle modalità di trasmissione dei documenti di cui al presente articolo.

Art. 14
Documenti probatori e allegati non informatici

1. I documenti probatori e gli allegati depositati in formato non elettronico sono identificati e descritti in una apposita sezione delle informazioni strutturate di cui all'articolo 11, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare copia informatica dei documenti probatori e degli allegati su supporto cartaceo e ad inserirla nel fascicolo informatico, apponendo la firma digitale ai sensi e per gli effetti di cui all'articolo 22, comma 3, del codice dell'amministrazione digitale.

(*torna all'indice per argomenti*)

Art. 15
Deposito dell'atto del processo da parte dei soggetti abilitati interni

1. L'atto del processo, redatto in formato elettronico da un soggetto abilitato interno e sottoscritto con firma digitale, è depositato telematicamente nel fascicolo informatico.
2. In caso di atto formato da organo collegiale l'originale del provvedimento è sottoscritto con firma digitale anche dal presidente.
3. Quando l'atto è redatto dal cancelliere o dal segretario dell'ufficio giudiziario questi vi appone la propria firma digitale e ne effettua il deposito nel fascicolo informatico.
4. Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia informatica nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34 e provvede a depositarlo nel fascicolo informatico, apponendovi la propria firma digitale.

(*torna all'indice per argomenti*)

[38] Ma vedi ora art. 16bis, co. 7, d.l: 179/2012, conv. con modificazione dalla legge n. 221/2012, come modificato dall'art. 51 d.l. 90/2014 conv. con modificazioni nella legge 114/2014 che ha previsto che "Il deposito è tempestivo quando è eseguito entro la fine del giorno di scadenza".
[39] Comma così modificato dal D.M. 209/2012.

Art. 16
Comunicazioni per via telematica

1. La comunicazione per via telematica dall'ufficio giudiziario ad un soggetto abilitato esterno o all'utente privato avviene mediante invio di un messaggio dall'indirizzo di posta elettronica certificata dell'ufficio giudiziario mittente all'indirizzo di posta elettronica certificata del destinatario, indicato nel registro generale degli indirizzi elettronici, ovvero per la persona fisica consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 e per l'impresa indicato nel registro delle imprese, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare una copia informatica dei documenti cartacei da comunicare nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34, che conserva nel fascicolo informatico.
3. La comunicazione per via telematica si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario e produce gli effetti di cui agli articoli 45 e 48 del codice dell'amministrazione digitale.
4. Fermo quanto previsto dall'articolo 20, comma 6, e salvo il caso fortuito o la forza maggiore, negli uffici giudiziari individuati con il decreto di cui all'articolo 51, comma 2, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, nel caso in cui viene generato un avviso di mancata consegna previsto dalle regole tecniche della posta elettronica certificata, si procede ai sensi del comma 3 del medesimo articolo 51 e viene pubblicato nel portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, un apposito avviso di avvenuta comunicazione o notificazione dell'atto nella cancelleria o segreteria dell'ufficio giudiziario, contenente i soli elementi identificativi del procedimento e delle parti e loro patrocinatori. Tale avviso è visibile solo dai soggetti abilitati esterni legittimati ai sensi dell'articolo 27, comma 1, del decreto ministeriale 21 febbraio 2011 n. 44.
5. Le ricevute di avvenuta consegna e gli avvisi di mancata consegna vengono conservati nel fascicolo informatico.
6. La comunicazione che contiene dati sensibili è effettuata per estratto con contestuale messa a disposizione dell'atto integrale nell'apposita area del portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26, con modalità tali da garantire l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività.
7. Nel caso previsto dal comma 6, si applicano le disposizioni di cui ai commi 2 e 3, ma la comunicazione si intende perfezionata il giorno feriale successivo al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario.
8. Si applica, in ogni caso, il disposto dell'articolo 49 del codice dell'amministrazione digitale.

(*torna all'indice per argomenti*)

Art. 17
Notificazioni per via telematica

1. Al di fuori dei casi previsti dall'articolo 51, del decreto legge 25 giugno 2008 n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, e successive modificazioni, le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Le richieste di altri soggetti sono inoltrate all'UNEP tramite posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. La notificazione per via telematica da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da un ufficio giudiziario verso i soggetti abilitati esterni di cui all'articolo 16.
4. Il sistema informatico dell'UNEP individua l'indirizzo di posta elettronica del destinatario dal registro generale degli indirizzi elettronici, dal registro delle imprese o dagli albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché per il cittadino dall'elenco reso consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 in base alle specifiche tecniche stabilite ai sensi dell'articolo 34.
5. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette per via telematica a chi ha richiesto il servizio il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

6. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, effettua la copia cartacea del documento informatico, attestandone la conformità all'originale, e provvede a notificare la copia stessa con le modalità previste dalla normativa processuale vigente.

(*torna all'indice per argomenti*)

Art. 18
Notificazioni per via telematica eseguite dagli avvocati[40]

1. L'avvocato che procede alla notificazione con modalità telematica ai sensi dell'articolo 3-bis della legge 21 gennaio 1994, n. 53, allega al messaggio di posta elettronica certificata documenti informatici o copie informatiche, anche per immagine, di documenti analogici privi di elementi attivi e redatti nei formati consentiti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Quando il difensore procede alla notificazione delle comparse o delle memorie, ai sensi dell'articolo 170, quarto comma, del codice di procedura civile, la notificazione è effettuata mediante invio della memoria o della comparsa alle parti costituite ai sensi del comma 1.
3. La parte rimasta contumace ha diritto a prendere visione degli atti del procedimento tramite accesso al portale dei servizi telematici e, nei casi previsti, anche tramite il punto di accesso.
4. L'avvocato che estrae copia informatica per immagine dell'atto formato su supporto analogico, compie l'asseverazione prevista dall'articolo 22, comma 2, del codice dell'amministrazione digitale, inserendo la dichiarazione di conformità all'originale nella relazione di notificazione, a norma dell'articolo 3-bis, comma 5, della legge 21 gennaio 1994, n. 53.
5. La procura alle liti si considera apposta in calce all'atto cui si riferisce quando è rilasciata su documento informatico separato allegato al messaggio di posta elettronica certificata mediante il quale l'atto è notificato. La disposizione di cui al periodo precedente si applica anche quando la procura alle liti è rilasciata su foglio separato del quale è estratta copia informatica, anche per immagine.
6. La ricevuta di avvenuta consegna prevista dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53 è quella completa, di cui all'articolo 6, comma 4, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

(ritorna all'indice cronologico)

(*ritorna all'indice per argomenti*)

Art. 19
Disposizioni particolari per la fase delle indagini preliminari

(omissis)

Art. 20
Requisiti della casella di PEC del soggetto abilitato esterno

1. Il gestore di posta elettronica certificata del soggetto abilitato esterno, fermi restando gli obblighi previsti dal decreto del Presidente della Repubblica 11 febbraio 2005, n.68 e dal decreto ministeriale 2 novembre 2005, recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata», è tenuto ad adottare software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.
2. Il soggetto abilitato esterno è tenuto a dotare il terminale informatico utilizzato di software idoneo a verificare l'assenza di virus informatici per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.
3. Il soggetto abilitato esterno è tenuto a conservare, con ogni mezzo idoneo, le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia.
4. La casella di posta elettronica certificata deve disporre di uno spazio disco minimo definito nelle specifiche tecniche di cui all'articolo 34.
5. Il soggetto abilitato esterno è tenuto a dotarsi di servizio automatico di avviso dell'imminente saturazione della propria casella di posta elettronica certificata e a verificare la effettiva disponibilità dello spazio disco a disposizione.
6. La modifica dell'indirizzo elettronico può avvenire dall'1 al 31 gennaio e dall'1 al 31 luglio.
7. La disposizione di cui al comma 6 non si applica qualora la modifica dell'indirizzo si renda necessaria per cessazione dell'attività da parte del gestore di posta elettronica certificata.

[40] Articolo così modificato dal D.M.G. 48/2013.

Art. 21
Richiesta delle copie di atti e documenti

1. Il rilascio della copia di atti e documenti del processo avviene, previa verifica del regolare pagamento dei diritti previsti, tramite invio all'indirizzo di posta elettronica certificata del richiedente, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. L'atto o il documento che contiene dati sensibili o di grandi dimensioni è messo a disposizione nell'apposita area del portale dei servizi telematici, nel rispetto dei requisiti di sicurezza stabiliti ai sensi dell'articolo 34.
3. Nel caso di richiesta di copia informatica, anche parziale, conforme al documento originale in formato cartaceo, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.

CAPO IV
CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Art. 22
Servizi di consultazione

1. Ai fini di cui agli articoli 50, comma 1, 52 e 56 del codice dell'amministrazione digitale, l'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene tramite un punto di accesso o tramite il portale dei servizi telematici, nel rispetto dei requisiti di sicurezza di cui all'articolo 26.

Art. 23
Punto di accesso

1. Il punto di accesso può essere attivato esclusivamente dai soggetti indicati dai commi 6 e 7.
2. Il punto di accesso fornisce un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema, nel rispetto dei requisiti tecnici di cui all'articolo 26.
3. Il punto di accesso fornisce adeguati servizi di formazione e assistenza ai propri utenti, anche relativamente ai profili tecnici.
4. La violazione da parte del gestore di un punto di accesso dei livelli di sicurezza e di servizio comporta la sospensione dell'autorizzazione ad erogare i servizi fino al ripristino di tali livelli.
5. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.
6. Possono gestire uno o più punti di accesso:
a) i consigli degli ordini professionali, i collegi ed i Consigli nazionali professionali, limitatamente ai propri iscritti;
b) il Consiglio nazionale forense, ove delegato da uno o più consigli degli ordini degli avvocati, limitatamente agli iscritti del consiglio delegante;
c) il Consiglio nazionale del notariato, limitatamente ai propri iscritti;
d) l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;
e) le Regioni, le città metropolitane, le provincie ed i Comuni, o enti consorziati tra gli stessi.
f) Le Camere di Commercio, per le imprese iscritte nel relativo registro.
7. I punti di accesso possono essere altresì gestiti da società di capitali in possesso di un capitale sociale interamente versato non inferiore a un milione di euro.

Art. 24
Elenco pubblico dei punti di accesso

1. L'elenco pubblico dei punti di accesso attivi presso il Ministero della giustizia comprende le seguenti informazioni:
a) identificativo del punto di accesso;
b) sede legale del soggetto titolare del punto di accesso;
c) indirizzo internet;
d) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo di posta elettronica certificata, numero di telefono e di fax;
e) recapiti relativi ai referenti tecnici da contattare in caso di problemi.

Art. 25
Iscrizione nell'elenco pubblico dei punti di accesso

1. Il soggetto che intende costituire un punto di accesso inoltra domanda di iscrizione nell'elenco pubblico dei punti di accesso secondo il modello e con le modalità stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia con apposito decreto, da adottarsi entro sessanta giorni dall'entrata in vigore del presente decreto.
2. Il Ministero della giustizia decide sulla domanda entro trenta giorni, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.
3. Con il provvedimento di cui al comma 2, il Ministero della giustizia delega la responsabilità del processo di identificazione dei soggetti abilitati esterni al punto di accesso. Il Ministero della giustizia può delegare la responsabilità del processo di identificazione degli utenti privati agli enti pubblici di cui all'articolo 23, comma 6, lettera e).
4. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'articolo 23, comma 3.

Art. 26
Requisiti di sicurezza

1. L'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene mediante identificazione sul punto di accesso o sul portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Il punto di accesso stabilisce la connessione con il portale dei servizi telematici mediante un collegamento sicuro con mutua autenticazione secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. A seguito dell'identificazione viene in ogni caso trasmesso al gestore dei servizi telematici il codice fiscale del soggetto che effettua l'accesso.
4. I punti di accesso garantiscono un'adeguata sicurezza del sistema con le modalità tecniche specificate in un apposito piano depositato unitamente all'istanza di cui all'articolo 25, a pena di inammissibilità della stessa.

Art. 27
Visibilità delle informazioni

1. Ad eccezione della fase di cui all'articolo 19, il dominio giustizia consente al soggetto abilitato esterno l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito o svolge attività di esperto o ausiliario. L'utente privato accede alle informazioni contenute nei fascicoli dei procedimenti in cui è parte mediante il portale dei servizi telematici e, nei casi previsti dall'articolo 23, comma 6, lettere e) ed f), e comma 7, mediante il punto di accesso.
2. È sempre consentito l'accesso alle informazioni necessarie per la costituzione o l'intervento in giudizio in modo tale da garantire la riservatezza dei nomi delle parti e limitatamente ai dati identificativi del procedimento.
3. In caso di delega, rilasciata ai sensi dell'articolo 9 regio decreto legge 27 novembre 1933, n. 1578, il dominio giustizia consente l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dal delegante, previa comunicazione, a cura di parte, di copia della delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della revoca della delega.
4. La delega, sottoscritta con firma digitale, è rilasciata in conformità alle specifiche di strutturazione di cui all'articolo 35, comma 4.
5. Gli esperti e gli ausiliari del giudice accedono ai servizi di consultazione nel limite dell'incarico ricevuto e della autorizzazione concessa dal giudice.
6. Salvo quanto previsto dal comma 2, gli avvocati e i procuratori dello Stato accedono alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione la cui difesa in giudizio è stata assunta dal soggetto che effettua l'accesso.

Art. 28
Registrazione dei soggetti abilitati esterni e degli utenti privati

1. L'accesso ai servizi di consultazione resi disponibili dal dominio giustizia si ottiene previa registrazione presso il punto di accesso autorizzato o presso il portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.

2. I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ad i propri utenti registrati, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.

Art. 29
Orario di disponibilità dei servizi di consultazione

1. Il portale dei servizi telematici e il gestore dei servizi telematici garantiscono la disponibilità dei servizi secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. In ogni caso è garantita la disponibilità dei servizi di consultazione nei giorni feriali dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentun dicembre.

CAPO V
PAGAMENTI TELEMATICI

Art. 30
Pagamenti

1. Il pagamento del contributo unificato e degli altri diritti e spese è effettuato nelle forme previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni. La ricevuta e la attestazione di pagamento o versamento è allegata alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, ed è conservata dall'interessato per essere esibita a richiesta dell'ufficio.
2. Il pagamento di cui al comma 1 può essere effettuato per via telematica con le modalità e gli strumenti previsti dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni e dalle altre disposizioni normative e regolamentari relative al riversamento delle entrate alla Tesoreria dello Stato.
3. L'interazione tra le procedure di pagamento telematico messe a disposizione dal prestatore del servizio di pagamento, il punto di accesso e il portale dei servizi telematici avviene su canale sicuro, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Il processo di pagamento telematico assicura l'univocità del pagamento mediante l'utilizzo della richiesta di pagamento telematico (RPT), della ricevuta telematica (RT) e dell'identificativo univoco di erogazione del servizio (CRS) che impediscono, mediante l'annullamento del CRS, un secondo utilizzo della RT. Le specifiche tecniche sono definite ai sensi dell'articolo 34.
5. La ricevuta telematica, firmata digitalmente dal prestatore del servizio di pagamento che effettua la riscossione o da un soggetto da questo delegato, costituisce prova del pagamento alla Tesoreria dello Stato ed è conservata nel fascicolo informatico.
6. L'ufficio verifica periodicamente con modalità telematiche la regolarità delle ricevute o attestazioni e il buon esito delle transazioni di pagamento telematico.

(*torna all'indice per argomenti*)

Art. 31
Diritto di copia

1. L'interessato, all'atto della richiesta di copia, richiede l'indicazione dell'importo del diritto corrispondente che gli è comunicato senza ritardo con mezzi telematici dall'ufficio, secondo le specifiche stabilite ai sensi dell'articolo 34.
2. Alla richiesta di copia è associato un identificativo univoco che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel sistema informatico per consentire il versamento secondo le modalità previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni.
3. La ricevuta telematica è associata all'identificativo univoco.

Art. 32
Registrazione, trascrizione e voltura degli atti

1. La registrazione, la trascrizione e la voltura degli atti avvengono in via telematica nelle forme previste dall'articolo 73 del decreto del Presidente della Repubblica 30 maggio 2002, n.115, e successive modificazioni.

Art. 33
Pagamento dei diritti di notifica

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'articolo 30.

2. L'UNEP rende pubblici gli importi dovuti a titolo di anticipazione. Eseguita la notificazione, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previo versamento del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

(*torna all'indice per argomenti*)

CAPO VI
DISPOSIZIONI FINALI E TRANSITORIE

Art. 34
Specifiche tecniche

1. Le specifiche tecniche sono stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e, limitatamente ai profili inerenti alla protezione dei dati personali, sentito il Garante per la protezione dei dati personali.
2. Le specifiche di cui al comma precedente vengono rese disponibili mediante pubblicazione nell'area pubblica del portale dei servizi telematici.
3. Fino all'emanazione delle specifiche tecniche di cui al comma 1, continuano ad applicarsi, in quanto compatibili, le disposizioni anteriormente vigenti.

Art. 35
Disposizioni finali e transitorie

1. L'attivazione della trasmissione dei documenti informatici da parte dei soggetti abilitati esterni è preceduta da un decreto dirigenziale che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.
2. L'indirizzo elettronico già previsto dal decreto del Ministro della Giustizia, 17 luglio 2008 recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile» è utilizzabile per un periodo transitorio non superiore a sei mesi dalla data di entrata in vigore del presente decreto.
3. La data di attivazione dell'indirizzo di posta elettronica certificata di cui all'articolo 4, comma 2, è stabilita, per ciascun ufficio giudiziario, con apposito decreto dirigenziale del responsabile per i sistemi informativi automatizzati del Ministero della giustizia che attesta la funzionalità del sistema di posta elettronica certificata del Ministero della giustizia.
4. Le caratteristiche specifiche della strutturazione dei modelli informatici sono definite con decreto del responsabile per i sistemi informativi automatizzati del Ministero della giustizia e pubblicate nell'area pubblica del portale dei servizi telematici.
5. Fino all'emanazione dei provvedimenti di cui al comma 4, conservano efficacia le caratteristiche di strutturazione dei modelli informatici di cui al decreto del Ministro della giustizia 10 luglio 2009, recante "Nuova strutturazione dei modelli informatici relativa all'uso di strumenti informatici e telematici nel processo civile e introduzione dei modelli informatici per l'uso di strumenti informatici e telematici nelle procedure esecutive individuali e concorsuali", pubblicato nella Gazzetta Ufficiale n. 165 del 18 luglio 2009 - s.o. n. 120.

Art. 36
Adeguamento delle regole tecnico-operative

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 37
Efficacia

1. Il presente decreto acquista efficacia il trentesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.
2. Dalla data di cui al comma 1, cessano di avere efficacia nel processo civile le disposizioni del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e del decreto del Ministro della giustizia 17 luglio 2008.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

(torna all'Avvertenza)

(ritorna all'indice cronologico)

D.P.C.M. 27 settembre 2012 - Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo 65, comma 1, lettera c-bis), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

IL PRESIDENTE DEL
CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82 recante «Codice dell'amministrazione digitale» (di seguito «CAD»), e, in particolare, gli articoli 65, comma 1, lettera c-bis) e 71;
Visto il decreto legislativo 30 giugno 2003, n. 196 recante «Codice in materia di protezione dei dati personali»;
Visto il decreto legislativo 1° dicembre 2009, n. 177 recante «Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'art. 24 della legge 18 giugno 2009, n. 69»;
Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese», con cui è stato soppresso DigitPA, le cui funzioni sono state attribuite all'Agenzia per l'Italia digitale;
Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 - «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3»;
Visto il decreto del Presidente del Consiglio dei Ministri 1° aprile 2008 recante «Regole tecniche e di sicurezza del sistema pubblico di connettività (SPC)», pubblicato nella Gazzetta Ufficiale del 21 giugno 2008, n. 144;
Visto il decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 - «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.», pubblicato nella Gazzetta Ufficiale del 15 novembre 2005, n. 266;
Visto il decreto del Presidente della Repubblica in data 29 novembre 2011, con il quale il Presidente Filippo Patroni Griffi è stato nominato Ministro senza portafoglio;
Visto il decreto del Presidente del Consiglio dei Ministri del 4 dicembre 2011, con il quale al predetto Ministro senza portafoglio è stato conferito l'incarico per la pubblica amministrazione e la semplificazione;
Visto il decreto del Presidente del Consiglio dei Ministri 13 dicembre 2011 recante delega di funzioni del Presidente del Consiglio dei Ministri al Ministro senza portafoglio, Presidente Filippo Patroni Griffi, in materia di pubblica amministrazione e semplificazione, tra cui, in raccordo con il Ministro delegato per l'innovazione tecnologica e lo sviluppo della società dell'informazione, prof. Francesco Profumo, le funzioni in materia di disciplina delle innovazioni connesse all'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni e nei relativi sistemi informatici e di telecomunicazione, nonché di adeguamento, per amministrazioni ed enti pubblici, della normativa vigente relativa all'organizzazione e alle procedure in ragione dell'uso delle predette tecnologie;
Acquisito il parere tecnico di DigitPA;
Sentita la Conferenza Unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281; Sentito il Garante per la protezione dei dati personali;
Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, recepita con legge 21 giugno 1986, n. 317 e modificata dal decreto Legislativo 23 novembre 2000, n. 427;
Di concerto con il Ministro dell'istruzione, dell'università e della ricerca;

Decreta:

Art. 1
Definizioni

1. Ai fini del presente decreto, si intende per:
a) Gestore: il soggetto di cui all'art. 2, comma 1, lettera c), del decreto del Presidente della Repubblica n. 68 del 2005, che eroga il servizio di cui all'art. 65, comma 1, lettera c-bis), del CAD;

b) Titolare: il soggetto di cui all'art. 1, comma 1, lettera t), del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005 che fruisce del servizio di cui all'art. 65, comma 1, lettera c-bis), del CAD attraverso la casella di cui alla lettera k);
c) CIE: la Carta d'Identità Elettronica di cui all'art. 1, comma 1, lettera c) del CAD;
d) CNS: la Carta Nazionale dei Servizi di cui all'art. 1, comma 1, lettera d) del CAD;
e) Token crittografico: dispositivo elettronico portatile per la generazione di password monouso;
f) password monouso: password utilizzabile una sola volta, costruita secondo opportuni algoritmi, che può essere conosciuta dall'utente in diversi modi, anche attraverso un canale di comunicazione diverso da quello in uso per l'utilizzo del servizio;
g) SAML: Security Assertion Markup Language definito dall'OASIS Security Services Technical Committee (SSTC) nella versione 2.0;
h) Identità digitale: è la rappresentazione informatica della corrispondenza biunivoca tra una persona fisica ed i suoi dati d'identità;
i) Identity provider: entità abilitata a creare, gestire e mantenere informazioni sull'identità digitale di soggetti che operano telematicamente, allo scopo di fornire supporto alla loro identificazione informatica, di cui all'art. 1, comma 1, lettera u-ter) del CAD, finalizzata alla fruizione di servizi erogati in rete;
j) servizio PEC-ID: il servizio di cui all'art. 65, comma 1, lettera c-bis), del CAD;
k) casella PEC-ID: la casella PEC rilasciata dal Gestore al Titolare, identificato con le modalità di cui al presente decreto;
l) Busta di Trasporto: il messaggio di cui all'art. 1, comma 1, lettera p) del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005;
m) casella PEC: la casella di cui all'art. 1, comma 1, lettera z) del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005.

Art. 2
Ambito di applicazione e finalità

1. Il presente decreto definisce le regole tecniche di cui all'art. 65, comma 1, lettera c-bis) del CAD relative alle modalità di identificazione del Titolare della casella PEC- ID valide per la presentazione, in via telematica, di istanze e dichiarazioni alle pubbliche amministrazioni.
2. Nei casi in cui l'amministrazione destinataria dell'istanza o della dichiarazione aderisca al Sistema Pubblico di Connettività (di seguito: «SPC»), si applicano, in quanto compatibili con il presente decreto, le relative regole tecniche di cui agli articoli 72 e seguenti del CAD, nonché le relative regole di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 1° aprile 2008.

Art. 3
Ambito soggettivo di applicazione

1. Le disposizioni di cui al presente decreto si applicano:
a) al Gestore;
b) al Titolare;
c) alle pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 e successive modificazioni.

Art. 4
Obblighi relativi ai Gestori

1. Il soggetto iscritto nell'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005 che intenda erogare il servizio PEC-ID si uniforma alle regole tecniche contenute nel presente decreto ed opera in qualità di Identity Provider per i Titolari delle caselle dallo stesso gestite.
2. L'Agenzia per l'Italia digitale gestisce, nell'ambito delle infrastrutture nazionali condivise del SPC, il Registro delle Identity Provider. A tale scopo, l'Agenzia per l'Italia digitale può utilizzare altri registri, da esso gestiti, che, forniscono un'analoga funzionalità. L'iscrizione nel Registro avviene secondo le modalità previste per il SPC dalla Commissione di cui all'art. 79 del CAD.
3. Le caratteristiche, i requisiti e le procedure tecnico-organizzative previsti per gli Identity Provider sono stabiliti dall'Agenzia per l'Italia digitale con apposita delibera.
4. Il Gestore aggiorna il manuale operativo di cui all'art. 23 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005, istituendo una specifica sezione contenente le procedure per l'identificazione dei Titolari nel rispetto delle presenti regole tecniche, nonché un'ulteriore sezione per le operazioni di gestione delle caselle PEC-ID.

Art. 5
Modalità di identificazione dei Titolari di caselle PEC-ID

1. Le operazioni di identificazione del Titolare sono curate dal Gestore nell'ambito delle attività e delle funzioni per la registrazione di cui all'art. 21, comma 1, lettera a) del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005.
2. L'identificazione di cui all'art. 65, comma 1, lettera c-bis) del CAD avviene, in occasione di ogni attribuzione di credenziali di accesso, in uno dei seguenti modi:
a) mediante la sottoscrizione del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD ed esibizione al Gestore, da parte del Titolare, di un valido documento d'identità e del codice fiscale;
b) tramite la compilazione del modulo di adesione disponibile in rete, previa identificazione informatica tramite CIE o CNS;
c) mediante la sottoscrizione con firma digitale, di cui all'art. 1, comma 1, lettera s) del CAD, del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD;
d) a mezzo di apparecchiature che utilizzino necessariamente una SIM/USIM dotate di codici PIN/PUK o loro evoluzioni tecnologiche rilasciate previa identificazione del titolare delle medesime nel rispetto delle disposizioni vigenti.
3. Il Gestore verifica la corrispondenza dei dati forniti dal Titolare con le generalità indicate nel documento d'identità o associate alla SIM/USIM e conserva la relativa documentazione per il periodo di durata del servizio PEC-ID e per un periodo pari a ventiquattro mesi successivi alla cessazione del servizio PEC_ID.
4. Nel modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD il Titolare manifesta l'eventuale assenso di cui all'art. 6 del CAD.

Art. 6
Identificazione

1. Ai fini dell'identificazione per l'accesso al servizio PEC-ID, il Gestore predispone una delle seguenti modalità:
a) identificazione tramite Certificato di autenticazione della CNS;
b) identificazione tramite Certificato di autenticazione della CIE;
c) identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) trasmessa attraverso sistemi di telefonia mobile;
d) identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) generata dal token crittografico rilasciato dal Gestore medesimo.

Art. 7
Modalità di attestazione dell'identità del Titolare

1. Ai fini del presente decreto l'identità del Titolare viene rappresentata attraverso il Codice fiscale dello stesso.
2. Il Gestore attesta l'identità di cui al comma 1 attraverso un'asserzione di autenticazione, conforme allo standard SAML, inserita in un apposito allegato alla busta di trasporto.
3. Il nome dell'allegato di cui al comma 2 corrisponde al Codice fiscale di cui al comma 1.

Art. 8
Divieto di riassegnazione di indirizzo PEC-ID

1. L'indirizzo di una casella PEC -ID è assegnato in via esclusiva al Titolare.

Art. 9
Blocco della casella di PEC-ID

1. L'accesso alla casella di PEC-ID è bloccato dal Gestore su richiesta del Titolare secondo le modalità indicate nel Manuale operativo di cui al decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005.
2. Il Gestore conserva un registro di tutte le operazioni di blocco effettuate per un periodo non inferiore a sessanta mesi.

Art. 10
Estensione del servizio PEC-ID a caselle PEC

1. Il Gestore estende il servizio PEC-ID alla casella PEC già assegnata al Titolare che ne faccia esplicita richiesta. In tal caso, il richiedente è identificato secondo le modalità previste dall'art. 5, comma 2, e allo stesso viene rilasciata una tipologia delle credenziali d'accesso al servizio ai sensi dell'art. 6.

Art. 11
Vigilanza

1. L'Agenzia per l'Italia digitale svolge funzioni di vigilanza e controllo, di cui all'art. 14, comma 13, del decreto del Presidente della Repubblica n. 68 del 2005, sull'attività esercitata dai Gestori ai sensi del presente decreto. Il presente decreto è inviato ai competenti organi di controllo e sarà pubblicato nella Gazzetta Ufficiale della Repubblica italiana.
Roma, 27 settembre 2012

p. il Presidente del Consiglio dei Ministri, il Ministro per la pubblica amministrazione e la semplificazione Patroni Griffi
Il Ministro dell'istruzione, dell'università e della ricerca Profumo

Registrato alla Corte dei conti il 22 novembre 2012 Presidenza del Consiglio dei Ministri, registro n. 9, foglio n. 318

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Decreto Legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221 – Ulteriori misure urgenti per la crescita del Paese (Estratto) [41]

(ritorna all'indice cronologico)

Art. 4
(Domicilio digitale del cittadino)

1. Dopo l'articolo 3 del decreto legislativo 7 marzo 2005, n. 82, é inserito il seguente:
«ART. 3-bis. - (Domicilio digitale del cittadino).
Omissis».

(*per leggere il testo vai all'art. 3bis del CAD*)

Art. 5
(Posta elettronica certificata - indice nazionale degli indirizzi delle imprese e dei professionisti).

1. L'obbligo di cui all'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, come modificato dall'articolo 37 del decreto-legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35, è esteso alle imprese individuali ((che presentano domanda di prima iscrizione)) al registro delle imprese o all'albo delle imprese artigiane successivamente alla data di entrata in vigore della legge di conversione del presente decreto.
2. Le imprese individuali attive e non soggette a procedura concorsuale, sono tenute a depositare, presso l'ufficio del registro delle imprese competente, il proprio indirizzo di posta elettronica certificata entro il 30 giugno 2013. L'ufficio del registro delle imprese che riceve una domanda di iscrizione da parte di un'impresa individuale che non ha iscritto il proprio indirizzo di posta elettronica certificata, in luogo dell'irrogazione della sanzione prevista dall'articolo 2630 del codice civile, sospende la domanda fino ad integrazione della domanda con l'indirizzo di posta elettronica certificata e comunque per quarantacinque giorni; trascorso tale periodo, la domanda si intende non presentata.
3. Al decreto legislativo 7 marzo 2005, n. 82, dopo l'articolo 6, é inserito il seguente: « ART. 6-bis. - (Indice nazionale degli indirizzi PEC delle imprese e dei professionisti) (omissis).

Art. 16
(Biglietti di cancelleria, comunicazioni e notificazioni per via telematica).

1. All'articolo 136, primo comma, del codice di procedura civile, le parole: «in carta non bollata» sono soppresse.
2. All'articolo 149-bis, secondo comma, del codice di procedura civile, dopo le parole: «pubblici elenchi» sono inserite le seguenti: «o comunque accessibili alle pubbliche amministrazioni».
3. All'articolo 45 delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie sono apportate le seguenti modificazioni: a) al primo comma sono premesse le seguenti parole: «Quando viene redatto su supporto cartaceo»; b) al secondo comma le parole «Esse contengono» sono sostituite dalle seguenti: «Il biglietto contiene»; c) al secondo comma le parole «ed il nome delle parti» sono sostituite dalle seguenti: «il nome delle parti ed il testo integrale del provvedimento comunicato»; d) dopo il terzo comma é aggiunto il seguente: «Quando viene trasmesso a mezzo posta elettronica certificata il biglietto di cancelleria é costituito dal messaggio di posta elettronica certificata, formato ed inviato nel rispetto della normativa, anche regolamentare, concernente la trasmissione e la ricezione dei documenti informatici.».
4. Nei procedimenti civili le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale. La relazione di notificazione é redatta in forma automatica dai sistemi informatici in dotazione alla cancelleria.

[41] Testo aggiornato al d.l. 83/2015 conv., con modificazioni, dalla legge n. 132/2015.

5. La notificazione o comunicazione che contiene dati sensibili è effettuata solo per estratto con contestuale messa a disposizione, sul sito internet individuato dall'amministrazione, dell'atto integrale cui il destinatario accede mediante gli strumenti di cui all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82.
6. Le notificazioni e comunicazioni ai soggetti per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, che non hanno provveduto ad istituire o comunicare il predetto indirizzo, sono eseguite esclusivamente mediante deposito in cancelleria. Le stesse modalità si adottano nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario.
7. Nei procedimenti civili nei quali sta in giudizio personalmente la parte il cui indirizzo di posta elettronica certificata non risulta da pubblici elenchi, la stessa può indicare l'indirizzo di posta elettronica certificata al quale vuole ricevere le comunicazioni e notificazioni relative al procedimento. In tale caso le comunicazioni e notificazioni a cura della cancelleria, si effettuano ai sensi del comma 4 e si applicano i commi 6 e 8. Tutte le comunicazioni e le notificazioni alle pubbliche amministrazioni che stanno in giudizio avvalendosi direttamente di propri dipendenti sono effettuate esclusivamente agli indirizzi di posta elettronica comunicati a norma del comma 12.
8. Quando non é possibile procedere ai sensi del comma 4 per causa non imputabile al destinatario, nei procedimenti civili si applicano l'articolo 136, terzo comma, e gli articoli 137 e seguenti del codice di procedura civile e, nei procedimenti penali, si applicano gli articoli 148 e seguenti del codice di procedura penale.
9. Le disposizioni dei commi da 4 a 8 acquistano efficacia: a) a decorrere dalla data di entrata in vigore del presente decreto, per le comunicazioni e le notificazioni a cura della cancelleria di cui sono destinatari i difensori, nei procedimenti civili pendenti dinanzi ai tribunali e alle corti d'appello che, alla predetta data sono già stati individuati dai decreti ministeriali previsti dall'articolo 51, comma 2, del decreto-legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133; b) a decorrere dal sessantesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto per le comunicazioni e le notificazioni di cui alla lettera a), per i procedimenti civili pendenti dinanzi ai tribunali ed alle corti di appello che alla data di entrata in vigore del presente decreto non sono stati individuati dai decreti ministeriali previsti dall'articolo 51, comma 2, del decreto-legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133; c) a decorrere dal trecentesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto per le comunicazioni e le notificazioni di cui ai commi 4 e 7, dirette a destinatari diversi dai difensori nei procedimenti civili pendenti dinanzi ai tribunali ed alle corti di appello; d) a decorrere dal quindicesimo giorno successivo a quello della pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dei decreti di cui al comma 10 per le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale, e per gli uffici giudiziari diversi dai tribunali e dalle corti d'appello.
10. Con uno o più decreti aventi natura non regolamentare, sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense e i consigli dell'ordine degli avvocati interessati, il Ministro della giustizia, previa verifica, accerta la funzionalità dei servizi di comunicazione, individuando: a) gli uffici giudiziari diversi dai tribunali e dalle corti di appello nei quali trovano applicazione le disposizioni del presente articolo; b) gli uffici giudiziari in cui le stesse disposizioni operano per le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale.
11. I commi da 1 a 4 dell'articolo 51 del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, sono abrogati.
12. Al fine di favorire le comunicazioni e notificazioni per via telematica alle pubbliche amministrazioni, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, comunicano al Ministero della giustizia, con le regole tecniche adottate ai sensi dell'articolo 4, comma 1, del decreto-legge 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla legge 22 febbraio 2010, n. 24, entro il 30 novembre 2014 l'indirizzo di posta elettronica certificata conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e successive modificazioni, a cui ricevere le comunicazioni e notificazioni. L'elenco formato dal Ministero della giustizia è consultabile solo dagli uffici giudiziari e dagli uffici notificazioni, esecuzioni e protesti e dagli avvocati[42].

[42] L'art. 66, co. 6, del D.lvo 217/2017 stabilisce che "Con decreto del Presidente del Consiglio dei ministri o del Ministro delegato, di concerto con il Ministro della giustizia, sono stabiliti le modalità e i tempi per la confluenza

13. In caso di mancata comunicazione entro il termine di cui al comma 12, si applicano i commi 6 e 8.
14. All'articolo 40 del testo unico delle disposizioni legislative e regolamentari in materia di spese di giustizia, di cui al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, dopo il comma 1-bis è aggiunto, in fine, il seguente: «1-ter. L'importo del diritto di copia, aumentato di dieci volte, è dovuto per gli atti comunicati o notificati in cancelleria nei casi in cui la comunicazione o la notificazione al destinatario non si é resa possibile per causa a lui imputabile».
15. Per l'adeguamento dei sistemi informativi hardware e software presso gli uffici giudiziari nonché per la manutenzione dei relativi servizi e per gli oneri connessi alla formazione del personale amministrativo è autorizzata la spesa di euro 1.320.000,00 per l'anno 2012 e di euro 1.500.000 a decorrere dall'anno 2013.
16. Al relativo onere si provvede con quota parte delle maggiori entrate derivanti dall'applicazione delle disposizioni di cui all'articolo 28, comma 2, della legge 12 novembre 2011, n. 183, che sono conseguentemente iscritte nello stato di previsione dell'entrata ed in quello del Ministero della giustizia.
17. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.
17-bis. Le disposizioni di cui ai commi 4, 6, 7, 8, 12 e 13 si applicano anche nel processo amministrativo.

(*torna all'indice per argomenti*)
(***torna all'art. 16ter d.l. 179 del 2012***)

Art. 16bis[43]
(Obbligatorietà del deposito telematico degli atti processuali).

1. Salvo quanto previsto dal comma 5, a decorrere dal 30 giugno 2014 nei procedimenti civili, contenziosi o di volontaria giurisdizione, innanzi al tribunale, il deposito degli atti processuali e dei documenti da parte dei difensori delle parti precedentemente costituite ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per il deposito degli atti e dei documenti da parte dei soggetti nominati o delegati dall'autorità giudiziaria. Le parti provvedono, con le modalità di cui al presente comma. a depositare gli atti e i documenti provenienti dai soggetti da esse nominati. Per difensori non si intendono i dipendenti di cui si avvalgono le pubbliche amministrazioni per stare in giudizio personalmente. In ogni caso, i medesimi dipendenti possono depositare, con le modalità previste dal presente comma, gli atti e i documenti di cui al medesimo comma.
1-bis. Nell'ambito dei procedimenti civili, contenziosi e di volontaria giurisdizione innanzi ai tribunali e, a decorrere dal 30 giugno 2015, innanzi alle corti di appello é sempre ammesso il deposito telematico di ogni atto diverso da quelli previsti dal comma 1 e dei documenti che si offrono in comunicazione, da parte del difensore o del dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente, con le modalità previste dalla normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. In tal caso il deposito si perfeziona esclusivamente con tali modalità.[44]
2. Nei processi esecutivi di cui al libro III del codice di procedura civile la disposizione di cui al comma 1 si applica successivamente al deposito dell'atto con cui inizia l'esecuzione. A decorrere dal 31 marzo 2015, il deposito nei procedimenti di espropriazione forzata della nota di iscrizione a ruolo ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Unitamente alla nota di iscrizione a ruolo sono depositati, con le medesime modalità, le copie conformi degli atti indicati dagli articoli 518, sesto comma, 543, quarto comma e 557, secondo comma, del codice di procedura civile. Ai fini del

---

dell'elenco di cui all'articolo 16, comma 12, del decreto-legge n. 179 del 2012 in una sezione speciale dell'elenco di cui all'articolo 6-ter del decreto legislativo n. 82 del 2005, consultabile esclusivamente dagli uffici giudiziari, dagli uffici notificazioni, esecuzioni e protesti e dagli avvocati. Con il medesimo decreto sono altresì stabilite le modalità con le quali le pubbliche amministrazioni che non risultino già iscritte nell'elenco di cui all'articolo 16, comma 12, del decreto-legge n. 179 del 2012, comunicano l'indirizzo di posta elettronica certificata da inserire nella sezione speciale di cui al presente comma. A decorrere dalla data fissata nel suddetto decreto, ai fini di cui all'articolo 16-ter del decreto-legge n. 179 del 2012, si intende per pubblico elenco anche la predetta sezione dell'elenco di cui all'articolo 6-ter del decreto legislativo n. 82 del 2005.

[43] Testo aggiornato alle modifiche apportate dal d.l. 59/2016.

[44] Comma inserito dall'art. 19 del decreto legge 27 giugno 2015, n. 83, convertito, con modificazioni, dalla legge 6 agosto 2015, n. 132.

presente comma, il difensore attesta la conformità delle copie agli originali, anche fuori dai casi previsti dal comma 9-bis e dall'articolo 16-decies.[45]
3. Nelle procedure concorsuali la disposizione di cui al comma 1 si applica esclusivamente al deposito degli atti e dei documenti da parte del curatore, del commissario giudiziale, del liquidatore, del commissario liquidatore e del commissario straordinario.
4. A decorrere dal 30 giugno 2014, per il procedimento davanti al tribunale di cui al libro IV, titolo I, capo I del codice di procedura civile, escluso il giudizio di opposizione, il deposito dei provvedimenti, degli atti di parte e dei documenti ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Il presidente del tribunale può autorizzare il deposito di cui al periodo precedente con modalità non telematiche quando i sistemi informatici del dominio giustizia non sono funzionanti e sussiste una indifferibile urgenza. Resta ferma l'applicazione della disposizione di cui al comma 1 al giudizio di opposizione al decreto d'ingiunzione.
5. Con uno o più decreti aventi natura non regolamentare, da adottarsi sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati, il Ministro della giustizia, previa verifica, accertata la funzionalità dei servizi di comunicazione, può individuare i tribunali nei quali viene anticipato, nei procedimenti civili iniziati prima del 30 giugno 2014 ed anche limitatamente a specifiche categorie di procedimenti, il termine fissato dalla legge per l'obbligatorietà del deposito telematico.
6. Negli uffici giudiziari diversi dai tribunali le disposizioni di cui ai commi 1 e 4 si applicano a decorrere dal quindicesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dei decreti, aventi natura non regolamentare, con i quali il Ministro della giustizia, previa verifica, accerta la funzionalità dei servizi di comunicazione. I decreti previsti dal presente comma sono adottati sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati.
7. Il deposito con modalità telematiche si ha per avvenuto al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del ministero della giustizia. Il deposito é tempestivamente eseguito quando la ricevuta di avvenuta consegna é generata entro la fine del giorno di scadenza e si applicano le disposizioni di cui all'articolo 155, quarto e quinto comma, del codice di procedura civile. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nelle specifiche tecniche del responsabile per i sistemi informativi automatizzati del ministero della giustizia, il deposito degli atti o dei documenti può essere eseguito mediante gli invii di più messaggi di posta elettronica certificata. Il deposito é tempestivo quando é eseguito entro la fine del giorno di scadenza.[46]
8. Fermo quanto disposto al comma 4, secondo periodo, il giudice può autorizzare il deposito degli atti processuali e dei documenti di cui ai commi che precedono con modalità non telematiche quando i sistemi informatici del dominio giustizia non sono funzionanti.
9. Il giudice può ordinare il deposito di copia cartacea di singoli atti e documenti per ragioni specifiche. Fatto salvo quanto previsto dal periodo precedente, con decreto non avente natura regolamentare il Ministro della giustizia stabilisce misure organizzative per l'acquisizione anche di copia cartacea degli atti depositati con modalità telematiche nonché per la riproduzione su supporto analogico degli atti depositati con le predette modalità, nonché per la gestione e la conservazione delle predette copie cartacee. Con il medesimo decreto sono altresì stabilite le misure organizzative per la gestione e la conservazione degli atti depositati su supporto cartaceo a norma dei commi 4 e 8, nonché ai sensi del periodo precedente.[47]
9-bis. Le copie informatiche, anche per immagine, di atti processuali di parte e degli ausiliari del giudice nonché dei provvedimenti di quest'ultimo, presenti nei fascicoli informatici o trasmessi in allegato alle comunicazioni telematiche dei procedimenti indicati nel presente articolo, equivalgono all'originale anche se prive della firma digitale del cancelliere di attestazione di conformità all'originale. Il difensore, il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente, il consulente tecnico, il professionista delegato, il curatore ed il commissario giudiziale possono estrarre con modalità telematiche duplicati, copie analogiche o informatiche degli atti e dei provvedimenti di cui al periodo precedente ed attestare la conformità delle copie estratte ai corrispondenti atti contenuti nel fascicolo

[45] Il secondo, il terzo e quarto periodo del secondo comma sono stati aggiunti dall'art. 18, co. 4, del D.l. 132/2014 convertito, con modificazioni, dalla legge 10 novembre 2014, n. 162. Le parole "e dall'articolo 16-decies." sono state inserite dall'art. 19 del d.l. 83/2015 convertito, con modificazioni, dalla legge 132/2015.
[46] Comma così modificato dall'art. 51 del d.l. 90/2014, conv. con modif., dalla legge 114/2014.
[47] Il secondo periodo di questo comma è stato inserito dalla legge n. 132/2015 di conversione del d.l. n. 83 del 2015 (art. 19).

informatico. Le copie analogiche ed informatiche, anche per immagine, estratte dal fascicolo informatico e munite dell'attestazione di conformità a norma del presente comma, equivalgono all'originale. Il duplicato informatico di un documento informatico deve essere prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso contenga la stessa sequenza di bit del documento informatico di origine. Le disposizioni di cui al presente comma non si applicano agli atti processuali che contengono provvedimenti giudiziali che autorizzano il prelievo di somme di denaro vincolate all'ordine del giudice.[48]

9-ter. A decorrere dal 30 giugno 2015 nei procedimenti civili, contenziosi o di volontaria giurisdizione, innanzi alla corte di appello, il deposito degli atti processuali e dei documenti da parte dei difensori delle parti precedentemente costituite ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per il deposito degli atti e dei documenti da parte dei soggetti nominati o delegati dall'autorità giudiziaria. Le parti provvedono, con le modalità di cui al presente comma, a depositare gli atti e i documenti provenienti dai soggetti da esse nominati. Con uno o più decreti aventi natura non regolamentare, da adottarsi sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati, il Ministro della giustizia, previa verifica, accertata la funzionalità dei servizi di comunicazione, può individuare le corti di appello nelle quali viene anticipato, nei procedimenti civili iniziati prima del 30 giugno 2015 ed anche limitatamente a specifiche categorie di procedimenti, il termine fissato dalla legge per l'obbligatorietà del deposito telematico.[49]

9-quater. Unitamente all'istanza di cui all'articolo 119, primo comma, del regio decreto 16 marzo 1942, n. 267, il curatore deposita un rapporto riepilogativo finale redatto in conformità a quanto previsto dall'articolo 33, quinto comma, del medesimo regio decreto. Conclusa l'esecuzione del concordato preventivo con cessione dei beni, si procede a norma del periodo precedente, sostituendo il liquidatore al curatore.[50]

9-quinquies. Il commissario giudiziale della procedura di concordato preventivo di cui all'articolo 186-bis del regio decreto 16 marzo 1942, n. 267 ogni sei mesi successivi alla presentazione della relazione di cui all'articolo 172, primo comma, del predetto regio decreto redige un rapporto riepilogativo secondo quanto previsto dall'articolo 33, quinto comma, dello stesso regio decreto e lo trasmette ai creditori a norma dell'articolo 171, secondo comma, del predetto regio decreto. Conclusa l'esecuzione del concordato si applica il comma 9-quater, sostituendo il commissario al curatore.[51]

9-sexies. Il professionista delegato a norma dell'articolo 591-bis del codice di procedura civile, entro dieci giorni dalla pronuncia dell'ordinanza di vendita, deposita un rapporto riepilogativo iniziale delle attività svolte. A decorrere dal deposito del rapporto riepilogativo iniziale, il professionista deposita, con cadenza semestrale, un rapporto riepilogativo periodico delle attività svolte. Entro dieci giorni dall'approvazione del progetto di distribuzione, il professionista delegato deposita un rapporto riepilogativo finale delle attività svolte successivamente al deposito del rapporto di cui al periodo precedente.[52]

9-septies. I rapporti riepilogativi periodici e finali previsti per le procedure concorsuali e i rapporti riepilogativi previsti per i procedimenti di esecuzione forzata devono essere depositati con modalità telematiche nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici, nonché delle apposite specifiche tecniche del responsabile per i sistemi informativi automatizzati del Ministero della giustizia. I relativi dati sono estratti ed elaborati, a cura del Ministero della giustizia, anche nell'ambito di rilevazioni statistiche nazionali. I rapporti riepilogativi di cui al presente comma devono contenere i dati identificativi dell'esperto che ha effettuato la stima. Le disposizioni di cui al presente comma si applicano anche ai prospetti riepilogativi delle stime e delle vendite di cui all'articolo 169-quinquies delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie. Il prospetto riepilogativo deve

[48] Le parole “il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente” sono state inserire dall’art. 19 del decreto legge 27 giugno 2015, n. 83, mentre, al primo comma, le parole “trasmessi in allegato alle comunicazioni telematiche” e “attestazione di conformità all’originale” sono state inserite dalla legge n. 132/2015 di conversione del predetto decreto legge.

[49] Comma inserito dall’art. 44 del d.l. 90/2014 convertito con modificazioni dalla legge 114/2014.

[50] Comma inserito dal d.l. 132/2014, convertito con modificazioni dalla L. 10 novembre 2014, n. 162.

[51] Comma inserito dal d.l. 132/2014, convertito con modificazioni dalla L. 10 novembre 2014, n. 162.

[52] Comma inserito dal d.l. 132/2014, convertito con modificazioni dalla L. 10 novembre 2014, n. 162, e così da ultimo modificato dall’art. 4 del d.l. 59/2016.

contenere anche i dati identificativi dell'ufficiale giudiziario che ha attribuito il valore ai beni pignorati a norma dell'articolo 518 del codice di procedura civile.[53]
9-octies. Gli atti di parte e i provvedimenti del giudice depositati con modalità telematiche sono redatti in maniera sintetica.[54]

(*torna all'indice per argomenti*)

Art. 16-ter.
Pubblici elenchi per notificazioni e comunicazioni

1. A decorrere dal 15 dicembre 2013, ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale si intendono per pubblici elenchi quelli previsti dagli articoli 6-bis, 6-quater e 62 del decreto legislativo 7 marzo 2005, n. 82, dall'articolo 16, comma 12, del presente decreto, dall'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia. [55]
1-bis. (omissis)

(*ritorna all'indice cronologico*)
(*torna all'indice per argomenti*)

(omissis)

Art. 16-sexies[56]
Domicilio digitale

1. Salvo quanto previsto dall'art. 366 del codice di procedura civile[57], quando la legge prevede che le notificazioni degli atti in materia civile al difensore siano eseguite, ad istanza di parte, presso la cancelleria dell'ufficio giudiziario, alla notificazione con le predette modalità può procedersi esclusivamente quando non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo di posta elettronica certificata, risultante dagli elenchi di cui all'art. 6-*bis* del decreto legislativo 7 marzo 2005, n. 82, nonché dal registro generale degli indirizzi elettronici, gestito dal ministero della giustizia.

(*torna all'indice per argomenti*)

Art. 16-septies[58]
Tempo delle notificazioni con modalità telematiche

1. La disposizione dell'art. 147 del codice di procedura civile si applica anche alle notificazioni eseguite con modalità telematiche[59]. Quando è eseguita dopo le ore 21, la notificazione si considera perfezionata alle ore 7 del giorno successivo[60].

---

[53] Comma inserito dal d.l. 132/2014, convertito con modificazioni dalla L. 10 novembre 2014, n. 162, modificato poi dal d.l. 83/2015 e così da ultimo modificato dall'art. 4 del d.l. 59/2016.
[54] Comma inserito dall'art. 19 del d.l. 83/2015 convertito con modificazioni dalla legge 6 agosto 2015, n. 132.
[55] Comma così modificato dall'art. 65 del D.lvo 217/2017. Si riporta il testo previgente: "1. A decorrere dal 15 dicembre 2013, ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa e stragiudiziale si intendono per pubblici elenchi quelli previsti dagli articoli 4 e 16, comma 12, del presente decreto; dall'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, dall'articolo 6-bis del decreto legislativo 7 marzo 2005, n. 82, nonché il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia".
[56] Articolo inserito dal d.l. 90/2014 convertito nella legge 114/14.
[57] Art. 366 c.p.c.: "Il ricorso deve contenere, a pena di inammissibilità: 1) l'indicazione delle parti; 2) l'indicazione della sentenza o decisione impugnata; 3) l'esposizione sommaria dei fatti della causa; 4) i motivi per i quali si chiede la cassazione, con l'indicazione delle norme di diritto su cui si fondano, secondo quanto previsto dall'articolo 366-bis; 5) l'indicazione della procura, se conferita con atto separato e, nel caso di ammissione al gratuito patrocinio, del relativo decreto; 6) la specifica indicazione degli atti processuali, dei documenti e dei contratti o accordi collettivi sui quali il ricorso si fonda. Se il ricorrente non ha eletto domicilio in Roma ovvero non ha indicato l'indirizzo di posta elettronica certificata comunicato al proprio ordine, le notificazioni gli sono fatte presso la cancelleria della Corte di cassazione. Nel caso previsto nell'articolo 360, secondo comma, l'accordo delle parti deve risultare mediante visto apposto sul ricorso dalle altre parti o dai loro difensori muniti di procura speciale, oppure mediante atto separato, anche anteriore alla sentenza impugnata, da unirsi al ricorso stesso. Le comunicazioni della cancelleria e le notificazioni tra i difensori di cui agli articoli 372 e 390 sono effettuate ai sensi dell'articolo 136, secondo e terzo comma".
[58] Articolo inserito dalla legge 114/14 di conversione del d.l. 90/2014.

(*torna all'indice per argomenti*)

Art. 16-novies[61]

Modalità informatiche per le domande di iscrizione e per la tenuta dell'albo dei consulenti tecnici, dell'albo dei periti presso il tribunale, dell'elenco dei soggetti specializzati per la custodia e la vendita dei beni pignorati e dell'elenco dei professionisti disponibili a provvedere alle operazioni di vendita

1. Le domande di iscrizione all'albo dei consulenti tecnici di cui agli articoli 13 e seguenti delle disposizioni per l'attuazione del codice di procedura civile, all'elenco dei soggetti specializzati previsto dall'articolo 169-sexies delle medesime disposizioni e all'albo dei periti presso il tribunale, di cui agli articoli 67 e seguenti delle norme di attuazione del codice di procedura penale, sono inserite, a cura di coloro che le propongono, con modalità esclusivamente telematiche in conformità alle specifiche tecniche di cui al comma 5. Con le medesime modalità sono inseriti i documenti allegati alle domande.
2. Le disposizioni di cui al comma 1 si applicano anche alle domande e ai relativi documenti per l'iscrizione negli elenchi dei professionisti disponibili a provvedere alle operazioni di vendita di cui all'articolo 169-ter e all'articolo 179-ter, secondo comma, delle disposizioni per l'attuazione del codice di procedura civile.
3. Quando, per l'iscrizione negli albi e negli elenchi di cui al presente articolo, la legge prevede il pagamento di bolli, diritti o altre somme a qualsiasi titolo, il versamento è effettuato esclusivamente con sistemi telematici di pagamento ovvero con carte di debito, di credito o prepagate o con altri mezzi di pagamento con moneta elettronica disponibili nel circuito bancario o postale, a norma dell'articolo 4, comma 9, del decreto-legge 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla legge 22 febbraio 2010, n. 24. I versamenti di cui al presente comma hanno luogo nel rispetto della normativa, anche regolamentare, concernente i pagamenti telematici nel processo civile.
4. Gli albi e gli elenchi di cui ai commi 1 e 2 sono formati a norma delle disposizioni legislative che li regolano e tenuti, a cura del presidente del tribunale, con modalità esclusivamente informatiche in conformità alle specifiche tecniche di cui al comma 5. L'accesso ai dati contenuti negli albi e negli elenchi è consentito ai magistrati e al personale delle cancellerie e delle segreterie di tutti gli uffici giudiziari della giustizia ordinaria. Salvo quanto previsto dall'articolo 179-quater, terzo comma, delle disposizioni per l'attuazione del codice di procedura civile, la disposizione di cui al periodo precedente si applica anche agli elenchi previsti dagli articoli 169-ter e 179-ter delle medesime disposizioni.
5. La presentazione delle domande e la tenuta degli albi ed elenchi di cui al presente articolo sono effettuate in conformità alle specifiche tecniche stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, nel rispetto della disciplina prevista dal decreto legislativo 7 marzo 2005, n. 82, entro sei mesi dall'entrata in vigore del presente decreto. Le specifiche tecniche sono pubblicate nella Gazzetta Ufficiale della Repubblica Italiana e sul sito internet del Ministero della giustizia.
6. Le disposizioni del presente articolo acquistano efficacia decorsi trenta giorni dalla pubblicazione sul sito internet del Ministero della giustizia delle specifiche tecniche previste dal comma 5.
7. I soggetti di cui ai commi 1 e 2, che alla data di acquisto di efficacia delle disposizioni del presente articolo sono già iscritti negli albi ed elenchi previsti dai medesimi commi, inseriscono i propri dati, con modalità telematiche e in conformità alle specifiche tecniche di cui al comma 5, entro il termine perentorio di novanta giorni dalla pubblicazione sul sito internet del Ministero della giustizia delle medesime specifiche tecniche. A decorrere dalla data di scadenza del termine di cui al periodo precedente, gli albi ed elenchi già formati sono sostituiti ad ogni effetto dagli albi ed elenchi previsti dal presente articolo.

(*ritorna all'indice cronologico*)

---

[59] Art. 147 c.p.c.: "Le notificazioni non possono farsi prima delle ore 7 e dopo le ore 21".

[60] Con sentenza n. 75/2019 la Corte Costituzionale ha dichiarato l'illegittimità costituzionale dell'art. 16-septies del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, nella legge 17 dicembre 2012, n. 221, inserito dall'art. 45-bis, comma 2, lettera b), del decreto-legge 24 giugno 2014, n. 90 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari), convertito, con modificazioni, nella legge 11 agosto 2014, n. 114, nella parte in cui prevede che la notifica eseguita con modalità telematiche la cui ricevuta di accettazione è generata dopo le ore 21 ed entro le ore 24 si perfeziona per il notificante alle ore 7 del giorno successivo, anziché al momento di generazione della predetta ricevuta.

[61] Articolo inserito dall'art. 14 del decreto legge 27 giugno 2015, n. 83, convertito, con modificazioni, dalla legge 132/2015.

(*torna all'indice per argomenti*)

Art. 16-decies[62]
Potere di certificazione di conformità delle copie degli atti e dei provvedimenti

1. Il difensore, il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente, il consulente tecnico, il professionista delegato, il curatore ed il commissario giudiziale, quando depositano con modalità telematiche la copia informatica, anche per immagine, di un atto processuale di parte o di un provvedimento del giudice formato su supporto analogico e detenuto in originale o in copia conforme, attestano la conformità della copia al predetto atto. La copia munita dell'attestazione di conformità equivale all'originale o alla copia conforme dell'atto o del provvedimento.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 16-undecies[63]
Modalità dell'attestazione di conformità

1. Quando l'attestazione di conformità prevista dalle disposizioni della presente sezione, dal codice di procedura civile[64] e dalla legge 21 gennaio 1994, n. 53, si riferisce ad una copia analogica, l'attestazione stessa è apposta in calce o a margine della copia o su foglio separato, che sia però congiunto materialmente alla medesima.
2. Quando l'attestazione di conformità si riferisce ad una copia informatica, l'attestazione stessa è apposta nel medesimo documento informatico.
3. Nel caso previsto dal comma 2, l'attestazione di conformità può alternativamente essere apposta su un documento informatico separato e l'individuazione della copia cui si riferisce ha luogo esclusivamente secondo le modalità stabilite nelle specifiche tecniche stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia. Se la copia informatica è destinata alla notifica, l'attestazione di conformità è inserita nella relazione di notificazione.[65]
3-bis. I soggetti di cui all'articolo 16-decies, comma 1, che compiono le attestazioni di conformità previste dalle disposizioni della presente sezione, dal codice di procedura civile e dalla legge 21 gennaio 1994, n. 53, sono considerati pubblici ufficiali ad ogni effetto.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

[62] Articolo inserito dall'art. 19 del decreto legge 27 giugno 2015, n. 83, convertito, con modificazioni, dalla legge 132/2015.
[63] Articolo inserito dall'art. 19 del decreto legge 27 giugno 2015, n. 83, convertito, con modificazioni, dalla legge 132/2015.
[64] art. 518 c.p.c. (Forma del pignoramento), art. 521-bis c.p.c. (Pignoramento e custodia di autoveicoli, motoveicoli e rimorchi), art. 543 c.p.c. (Forma del pignoramento) e art. 557 c.p.c. (Deposito dell'atto di pignoramento).
[65] Vedi art. 19ter Provv. DGSIA 16 aprile 2015 inserito dal DM 28 dicembre 2015 ed in vigore del 9 gennaio 2016.

Provvedimento Responsabile DGSIA 16 aprile 2014 - Specifiche tecniche previste dall'art. 34, c1 del d.m. 21 febbraio 2011 n. 44, regolamento concernente le regole tecniche per l'adozione, nel processo civile e penale, delle tecnologie dell'informazione e della comunicazione. Testo aggiornato con le modifiche apportate dal DM 28 dicembre 2015.

(ritorna all'indice cronologico)

Titolo completo: Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel pro-cesso civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24

Direzione generale per i sistemi informativi automatizzati Il responsabile per i sistemi informativi automatizzati
Visto il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44 (pubblicato sulla Gazzetta Ufficiale n. 89 del 18 aprile 2011), recante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24", come modificato dal decreto ministeriale 15 ottobre 2012 n. 209 e dal decreto ministeriale 3 aprile 2013 n. 48;
Visto il decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221 e successivamente modificato dalla legge 24 dicembre 2012, n. 228;
Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni;
Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;
Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della L. 16 gennaio 2003, n. 3»;
Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2013;
Visto il decreto ministeriale 27 aprile 2009, recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»;
Rilevata la necessità di aggiornare le specifiche tecniche previste dall'articolo 34, comma 1, del citato decreto ministeriale 21 febbraio 2011, n. 44;
Acquisito il parere espresso in data 23 dicembre 2013 dal Garante per la protezione dei dati personali;
Acquisito il parere espresso in data 4 febbraio 2014 dall'Agenzia per l'Italia Digitale;

EMANA IL SEGUENTE PROVVEDIMENTO:

CAPO I – PRINCIPI GENERALI

Art. 1
Ambito di applicazione

Il presente provvedimento stabilisce le specifiche tecniche previste dall'articolo 34, comma 1, del regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24.

Art. 2
Definizioni

Ai fini del presente provvedimento, oltre alle definizioni contenute nell'articolo 2 del regolamento, si intende:
a) **regolamento**: il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, portante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del

decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24" e successive modifica-zioni;
b) **CAD**: codice dell'amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni);
c) **CNS**: Carta Nazionale dei Servizi;
d) **CSV**: *Comma-separated values*;
e) **DTD**: *Document Type Definition*;
f) **DGSIA**: Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia;
g) **GSU**: Sistema di gestione informatizzata dei registri per gli uffici notifiche e protesti;
h) **HSM**: *Hardware Security Module*;
i) **HTTPS**: *HyperText Transfer Protocol over Secure Socket Layer*;
j) **IMAP**: *Internet Message Access Protocol*;
k) **PdA**: Punto di Accesso, come definito all'art. 23 del regolamento;
l) **PEC**: Posta Elettronica Certificata;
m) **POP**: *Post Office Protocol*;
n) **PP.AA.**: Pubbliche Amministrazioni;
o) **RdA**: Ricevuta di Accettazione della Posta Elettronica Certificata;
p) **RdAC**: Ricevuta di Avvenuta Consegna della Posta Elettronica Certificata;
q) **ReGIndE**: Registro Generale degli Indirizzi Elettronici, come definito all'art. 7 del regolamento;
r) **SMTP**: *Simple Mail Transfer Protocol*;
s) **UU.GG.**: Uffici Giudiziari;
t) **WSDL**: *Web Services Definition Language*;
u) **XML**; *eXtensible Markup Language*;
v) **XSD**: *XML Schema Definition*;
w) **SPC**: Sistema Pubblico di Connettività;
x) **PKCS#11**: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite apposita sequenza di chia-mate al *token* per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di identificazione;
y) **CAdES (CMS *Advanced Electronic Signature***): formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 e basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni;
z) **PAdES (PDF *Advanced Electronic Signature***): formato di busta critto-grafica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;
aa) **OID (*Object IDentifier*)**: codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione uni-voca in ambito mondiale;
bb) **Autenticazione a due fattori**: metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia che combina un'informazione nota (ad esempio un nome utente e una *password*) con un oggetto a disposizione (ad esempio, una carta di credito, *token* o telefono cellulare);
cc) **Impronta**: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash.[66]
dd) **Funzione di hash**: una funzione matematica che genera, a partire da un documento informatico, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire il documento informatico originario e generare impronte uguali a partire da documenti informatici differenti.[67]

CAPO II – SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Art. 3

Infrastrutture informatiche – art. 3 del regolamento

Il sistema informatico del Ministero della giustizia è articolato, salvo le infrastrutture unitarie e comuni, a livello nazionale, interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale (di circondario).
Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.

[66] Definizione aggiunta dal DM 28 dicembre 2015.
[67] Definizione aggiunta dal Dm 28 dicembre 2015.

Il sistema di posta elettronica certificata è gestito dal fornitore presso la propria sala server, collegata ad SPC secondo le relative regole di interoperabilità e sicurezza, oppure presso una sala server del Ministero della giustizia.
Il dispiegamento di detti sistemi rispetta le disposizioni di cui al decreto del Ministro della giustizia in data 27 aprile 2009, recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".
Il Direttore Generale S.I.A. emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico, sentito il Garante per la protezione dei dati personali. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul sito internet dell'Amministrazione.
Le strutture elaborative serventi ed i dati sono allocati in corrispondenza delle componenti di cui ai commi precedenti.

Art. 4

Gestore della posta elettronica certificata del Ministero della giustizia – art. 4 del regolamento

Il Ministero della giustizia si avvale del proprio gestore di posta elettronica certificata, che rilascia e gestisce apposite caselle di PEC degli uffici giudiziari e degli UNEP da utilizzare esclusivamente per i servizi previsti dal regolamento, nel rispetto delle specifiche tecniche riportate nel presente provvedimento.
Le caselle appartengono ad apposito sotto-dominio (civi-le.ptel.giustiziacert.it e penale.ptel.giustiziacert.it) e possono ricevere unicamente messaggi di posta elettronica certificata. I messaggi di posta elettronica ordinaria vengono automaticamente scartati.
Il gestore dei servizi telematici utilizza i protocolli POP3, POP3S, IMAP, IMAPS e SMTP per collegarsi al gestore di posta elettronica certificata del Ministero.
La codifica dei singoli uffici, comprensiva del relativo indirizzo di PEC, è contenuta nel catalogo dei servizi telematici di cui all'articolo 5, comma 3.
Non possono essere utilizzate caselle di PEC diverse da quelle di cui ai commi precedenti per la trasmissione e il deposito di atti processuali.
Il Ministero della giustizia conserva il log dei messaggi, transitati attraverso il proprio gestore di posta elettronica certificata, per cinque anni. A tal fine, il gestore di PEC del Ministero invia giornalmente, a una casella di posta di sistema, il log in formato CSV. Il log, sottoscritto con firma digitale o firma elettronica qualificata, è relativo a tutti gli indirizzi del sotto-dominio delle caselle del processo telematico e contiene tutti gli eventi relativi ai messaggi pervenuti, conservando le seguenti informazioni:
il codice identificativo univoco assegnato al messaggio originale;
la data e l'ora dell'evento;
il mittente del messaggio originale;
i destinatari del messaggio originale;
l'oggetto del messaggio originale;
il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
il gestore mittente.
Un apposito modulo nell'ambito del portale dei servizi telematici comprende i componenti funzionali necessari per l'acquisizione, il salvataggio e l'interrogazione dei log prodotti dal servizio di PEC.
I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.
Le comunicazioni di atti e documenti tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria nella fase delle indagini preliminari, avvengono mediante i gestori di posta elettronica certificata delle forze di polizia, le cui caselle sono rese disponibili unicamente agli utenti abilitati; in questo caso il gestore dei servizi telematici utilizza un canale sicuro protetto da un meccanismo di crittografia ai sensi di quanto previsto dall'articolo 20.

Art. 5

Portale dei servizi telematici – art. 6 del regolamento

Il portale dei servizi telematici è accessibile all'indirizzo http://pst.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".
L'"area pubblica", denominata "Servizi online Uffici Giudiziari", è composta da tutte le pagine web e i servizi del portale disponibili ad accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione; in essa sono disponibili le seguenti tipologie d'informazione:
Informazioni e documentazione sui servizi telematici del dominio giustizia;

Raccolte giurisprudenziali;
Informazioni essenziali sullo stato dei procedimenti pendenti, rese disponibili in forma anonima; in questo caso, i parametri e i risultati di ricerca riportano unicamente i dati identificativi dei procedimenti (numero di ruolo, numero di sentenza, ecc.), senza riferimenti in chiaro ai nomi o ai dati personali delle parti e tali per cui non sia possibile risalire all'identità dell'interessato. Il canale di comunicazione per l'accesso a tali informazioni è cifrato (HTTPS).
Nell'area pubblica è consultabile il catalogo dei servizi telematici, che si compone di una serie di file aventi lo scopo di censire, in forma strutturata, tutte le informazioni relative ai servizi telematici, secondo gli XSD di cui all'Allegato 10.
Per "area riservata" s'intende il contenitore di tutte le pagine e i servizi del portale disponibili previa identificazione informatica, come disciplinata dall'articolo 6.
Nell'area riservata sono disponibili informazioni, dati e provvedimenti giudiziari in formato elettronico, secondo quanto previsto all'art. 27 del regolamento, nonché i servizi di pagamento telematico e di richiesta copie.

(*torna all'indice per argomenti*)

Art. 6
Identificazione informatica – art. 6 del regolamento

L'identificazione informatica per i soggetti abilitati esterni e gli utenti privati avviene sul portale dei servizi telematici mediante carta d'identità elettronica o carta nazionale dei servizi e sul punto di accesso mediante autenticazione a due fattori oppure tramite token crittografico (smart card, chiavetta USB o altro dispositivo sicuro) in conformità all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82; in caso si utilizzi il token crittografico, l'identificazione avviene nel rispetto dei seguenti requisiti:
Il certificato deve essere rilasciato da un certificatore accreditato dall'Agenzia per l'Italia Digitale ai sensi dell'art 29 del CAD, che si fa garante dell'identità del soggetto.
Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all'Appendice 1 del documento rilasciato dal CNIPA: "Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi". L'estensione Certificate Policy (2.5.29.32) può essere valorizzata con un Object Identifier (OID) definito dalla CA.
In termini di sicurezza, i dispositivi ammessi sono i dispositivi personali consentiti per la firma elettronica qualificata e quindi smart card e token USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criteria EAL4+ con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie.
In termini d'interoperabilità, sono ammissibili dispositivi che consentano la disponibilità di entrambe le interfacce PKCS#11 e CSP; in particolare, entrambe le interfacce devono consentire l'accesso alla procedura d'identificazione forte mediante digitazione del PIN da parte dell'utente; il dispositivo deve inoltre rispettare la strutturazione del file system come da specifiche CNS.
In fase di identificazione tramite token crittografico, il punto di accesso o il portale dei servizi telematici verifica la validità del certificato presente nel token crittografico utilizzato dall'utente che accede; prima di consentire qualunque operazione, inoltre, il punto di accesso verifica che il token crittografico sia collegato alla postazione; in caso contrario, invalida e termina la sessione.
Il Ministero della giustizia verifica, anche attraverso opportune visite ispettive, che i punti di accesso rispettino i predetti requisiti.
La violazione di queste regole di sicurezza comporta per il punto di accesso la sospensione dell'autorizzazione a erogare i servizi, fino al definitivo rispetto dei requisiti.
L'identificazione informatica per i soggetti abilitati interni avviene ai sensi dell'articolo 10.

Art. 7
Registro generale degli indirizzi elettronici – art. 7 del regolamento

Il Registro Generale degli Indirizzi Elettronici (ReGIndE) è gestito dal Ministero della giustizia e contiene i dati identificativi nonché l'indirizzo di PEC dei soggetti abilitati esterni.
Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al presente regolamento.
I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l'inserimento manuale dei dati.
Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:

soggetti appartenenti ad un ente pubblico che svolgano uno specifico ruolo nell'ambito di procedimenti (ad esempio avvocati e funzionari dell'INPS e dell'Avvocatura dello Stato, avvocati e funzionari delle PP.AA.);
professionisti iscritti in albi ed elenchi istituiti con legge (ad esempio Consiglio dell'ordine degli avvocati o Consiglio nazionale del Notariato);
professionisti non iscritti ad alcun albo: tutti i soggetti nominati dal giudice come consulenti tecnici d'ufficio – o più in generale ausiliari del giudice – non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (ad eccezione degli avvocati).
Il ReGIndE non gestisce informazioni già presenti in registri disponibili alle PP.AA., qualora questi siano accessibili in via telematica ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008 n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009 n. 2, il cui contenuto occorre ai sistemi del dominio Giustizia; da tali registri – tra cui il registro delle imprese, l'indice nazionale delle imprese e dei professionisti (INI-PEC), l'anagrafe nazionale della popolazione residente (ANPR) e il domicilio digitale del cittadino di cui all'art 3-bis del CAD – sono recuperati gli indirizzi di PEC dei professionisti e delle imprese, nonché gli indirizzi dei cittadini ivi censiti.
Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.
Il ReGIndE è consultabile dai soggetti abilitati esterni tramite il proprio punto di accesso o tramite il Portale dei Servizi Telematici, su connessioni sicure (SSL v3), attraverso un apposito web service; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici.

(*torna all'indice per argomenti*)

Art. 8

Alimentazione del registro generale degli indirizzi elettronici – art. 7 del regolamento

L'alimentazione del ReGIndE avviene previo invio al responsabile per i sistemi informativi automatizzati di un documento di censimento contenente le informazioni necessarie ad identificare:
l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;
il nominativo e il codice fiscale del delegato all'invio dell'albo, che dovrà sottoscrivere con firma digitale o firma elettronica qualificata l'albo in trasmissione;
la casella di PEC utilizzata per l'invio dell'albo.
Il documento di censimento di cui al comma precedente aderisce al modello reperibile nell'area pubblica del portale e viene inviato all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.dog@giustiziacert.it.
Terminate le operazioni di censimento da parte del responsabile per i sistemi informativi automatizzati, l'ente mittente del documento di censimento riceve una risposta; in caso di esito positivo, l'ente può procedere all'invio dell'albo secondo le seguenti specifiche:
il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;
non vi sono vincoli sull'oggetto né sul corpo del messaggio;
l'indirizzo di PEC mittente deve essere censito tra quelli delegati all'invio e riportati nel documento di censimento;
deve essere allegato un solo file (ComunicazioniSoggetti.xml o, per le Pubbliche Amministrazioni, ComunicazioneSoggettiPPAA.xml), sotto-scritto con firma digitale o firma elettronica qualificata;
la firma digitale o firma elettronica qualificata deve appartenere al soggetto delegato di cui al comma 1, lettera b, sulla base del codice fiscale censito;
il file ComunicazioniSoggetti.xml o il file ComunicazioneSogget-tiPP.AA.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;
il codice ente specificato nel file deve essere tra quelli censiti.
Il mancato rispetto di uno o più dei vincoli di cui all'articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l'allegato ComunicazioniSoggetti.xml viene scartato.
A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso "– Esito" e riporta in allegato l'esito dell'elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell'Allegato 3.
L'esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come ad esempio codice fiscale inesistente), sia ad errori legati a vincoli e prerequisiti che

presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richiedente e dei soggetti abilitati all'invio dell'albo).
Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell'inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di PEC di cortesia in cui si attesta l'avvenuta registrazione.

Art. 9
Professionisti non iscritti in albi – art. 7 del regolamento

I professionisti non iscritti all'albo, oppure per i quali il proprio ordine di appartenenza non abbia provveduto all'invio di copia dell'albo (ad eccezione degli avvocati), si registrano al ReGIndE attraverso un Punto di Accesso (PdA) o attraverso il Portale dei Servizi Telematici, previa identificazione, effettuando altresì l'inserimento (upload) del file che contiene copia informatica, in formato PDF, dell'incarico di nomina da parte del giudice; tale file è sottoscritto con firma digitale o firma elettronica qualificata dal soggetto che intende iscriversi.
Il PdA provvede a trasmettere l'avvenuta registrazione con le medesime modalità di cui all'articolo precedente, con la differenza che il file ComunicazioniSoggetti.xml è digitalmente sottoscritto con firma digitale o firma elettronica qualificata dal PdA.
Qualora il professionista di cui al comma 1 s'iscriva ad un albo, oppure pervenga copia dell'albo da parte dell'ordine di appartenenza, prevalgono i dati trasmessi dall'ordine stesso; in questo caso il sistema cancella la prima iscrizione e invia un messaggio PEC di cortesia al professionista.

Art. 9 bis
Indirizzi di posta elettronica certificata delle pubbliche amministrazioni

La pubblica amministrazione che deve comunicare il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni, ai sensi dell'articolo 16, comma 12, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, procede inserendo tale indirizzo sul portale dei servizi telematici.
Ai fini di cui al comma precedente, la pubblica amministrazione invia all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati (prot.dgsia.dog@giustiziacert.it) un documento contenente le seguenti informazioni:
descrizione e codice fiscale della pubblica amministrazione;
nominativo, codice fiscale e recapiti del soggetto incaricato di inserire o modificare gli indirizzi di PEC della pubblica amministrazione sul portale dei servizi telematici;
Il soggetto incaricato di cui al comma precedente accede ad un'apposita area riservata del portale dei servizi telematici, previa identificazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica:
l'indirizzo di PEC della pubblica amministrazione;
il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti tramite i quali la pubblica amministrazione sta in giudizio personalmente; tali soggetti alimentano il Registro Generale degli Indirizzi Elettronici.
L'elenco degli indirizzi di PEC delle pubbliche amministrazioni è consultabile dagli uffici giudiziari e dagli uffici NEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni.
L'elenco degli indirizzi di PEC di cui al comma 3, lettera a, è consultabile dagli avvocati tramite il proprio punto di accesso o tramite il portale dei servizi telematici (area riservata), su connessioni sicure (SSL v3), attraverso un apposito web service, che verifica la presenza dell'avvocato sul ReGIndE; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici. L'accesso è tracciato in appositi log, che il Ministero della giustizia conserva per cinque anni, recanti: il punto di accesso attraverso cui è stato effettuato l'accesso, la data e l'ora dell'accesso.

(*torna all'indice per argomenti*)

Art. 10
Sistemi informatici per i soggetti abilitati interni – art. 8 del regolamento

I sistemi informatici a disposizione dei soggetti abilitati interni sono conformi alle regole di cui al D.M. 27 aprile 2009 e mettono a disposizione le funzioni relative a:
ricezione, accettazione e trasmissione dei dati e dei documenti informatici;
consultazione e gestione del fascicolo informatico.

Per l'accesso ai sistemi di cui al comma precedente dall'interno degli uffici giudiziari, l'identificazione è effettuata mediante coppia di credenziali "nome utente/password" oppure mediante autenticazione a due fattori.
Per l'accesso ai sistemi di cui al comma 1 dall'esterno della Rete Giustizia, l'identificazione è effettuata dal portale dei servizi telematici sulla base del sistema "Active Directory Nazionale" (ADN) tramite autenticazione a due fattori; ai soli fini del recupero dall'esterno delle informazioni di registro da parte dei sistemi a disposizione dei magistrati in ambito civile, è sufficiente l'identificazione sulla base del sistema ADN purché l'interrogazione dei dati finalizzati al recupero preveda l'indicazione del numero di ruolo generale nonché del codice fiscale dell'attore principale e del convenuto principale del procedimento.

Art. 11
Fascicolo informatico – art. 9 del regolamento

Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.
Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutti i metodi – esposti attraverso appositi web service – necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione.
Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:
il codice fiscale del soggetto che ha effettuato l'accesso;
il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);
la data e l'ora dell'accesso.
Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni.

(*torna all'indice per argomenti*)

CAPO III – TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Art. 12
Formato dell'atto del processo in forma di documento informatico – art. 11 del regolamento

L'atto del processo in forma di documento informatico, da depositare telematicamente all'ufficio giudiziario, rispetta i seguenti requisiti:
è in formato PDF;
è privo di elementi attivi;
è ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;
è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata.
La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CA-dES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo "firme multiple indipendenti" o parallele, e prevede che uno o più soggetti firmino, ognuno con la propria chiave privata, lo stesso documento (o contenuto della busta). L'ordine di apposizione delle firme dei firmatari non è significativo e un'alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica; nel caso del formato CAdES il file generato si presenta con un'unica estensione p7m. Il meccanismo qui descritto è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

Le applicazioni di generazione della firma digitale o qualificata per la sottoscrizione dei documenti informatici devono utilizzare la funzione di hash di cui all'art 4, comma 2, del Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013.

Art. 13
Formato dei documenti informatici allegati – art. 12 del regolamento

I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:
.pdf
.rtf
.txt
.jpg
.gif
.tiff
.xml
.eml, purché contenenti file nei formati di cui alle lettere precedenti.
.msg, purché contenenti file nei formati di cui alle lettere da a ad h.
È consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti al comma precedente:
.zip
.rar
.arj.
Gli allegati possono essere sottoscritti con firma digitale o firma elettronica qualificata; nel caso di formati compressi la firma digitale, se presente, deve essere applicata dopo la compressione.

(*torna all'indice per argomenti*)

Art. 14
Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati – art. 13 del regolamento

L'atto e gli allegati sono contenuti nella cosiddetta "busta telematica", ossia un file in formato MIME che riporta tutti i dati necessari per l'elaborazione da parte del sistema ricevente (gestore dei servizi telematici); in particolare la busta contiene il file Atto.enc, ottenuto dalla cifratura del file Atto.msg, il quale contiene a sua volta:
IndiceBusta.xml: il DTD è riportato nell'Allegato 4. Tale file deve essere omesso qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b).
DatiAtto.xml: gli XSD sono riportati nell'Allegato 5.
<nome file (libero)>: atto vero e proprio, in formato PDF, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 12 comma 2.
AllegatoX.xxx: uno o più allegati nei formati di file di cui all'articolo 13, eventualmente sottoscritti con firma digitale o firma elettronica qualificata; il nome del file può essere scelto liberamente.
La cifratura di Atto.msg è eseguita con la chiave di sessione (ChiaveSessione) cifrata con il certificato del destinatario; IssuerDname è il Distinguished Name della CA che ha emesso il certificato dell'ufficio giudiziario o dell'UNEP destinatario, SerialNumber è il numero seriale del certificato dell'ufficio giudiziario o dell'UNEP destinatario; l'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione sono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario; le chiavi di cifratura degli uffici giudiziari sono disponibili nell'area pubblica del portale dei servizi telematici (il relativo percorso e nome file è indicato nel catalogo dei servizi telematici).
La dimensione massima consentita per la busta telematica è pari a 30 Megabyte.
La busta telematica viene trasmessa all'ufficio giudiziario destinatario in allegato ad un messaggio di posta elettronica certificata che rispetta le specifiche su mittente, destinatario, oggetto, corpo e allegati come riportate nell'Allegato 6.
Il gestore dei servizi telematici scarica il messaggio dal gestore della posta elettronica certificata del Ministero della giustizia ed effettua le verifiche formali sul messaggio; le eccezioni gestite sono le seguenti:
T001: l'indirizzo del mittente non è censito in ReGIndE;
T002: Il formato del messaggio non è aderente alle specifiche;
T003: la dimensione del messaggio eccede la dimensione massima consentita.

Il gestore dei servizi telematici, nel caso in cui il mittente sia un avvocato, effettua l'operazione di certificazione, ossia recupera lo status del difensore da ReGIndE; nel caso in cui lo status non sia "attivo", viene segnalato alla cancelleria.
Il gestore dei servizi telematici effettua i controlli automatici (formali) sulla busta telematica; le possibili anomalie all'esito dell'elaborazione della busta telematica sono codificate secondo le seguenti tipologie:
WARN (WARNING): anomalia non bloccante; si tratta in sostanza di segnalazioni, tipicamente di carattere giuridico (ad esempio manca la procura alle liti allegata all'atto introduttivo);
ERROR: anomalia bloccante, ma lasciata alla determinazione dell'ufficio ricevente, che può decidere di intervenire forzando l'accettazione o rifiutando il deposito (esempio: certificato di firma non valido o mittente non firmatario dell'atto);
FATAL: eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fondamentali per l'elaborazione).
La codifica puntuale degli errori indicati al comma precedente è pubblicata e aggiornata nell'area pubblica del portale dei servizi telematici.
All'esito dei controlli di cui ai commi precedenti, il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata riportante eventuali eccezioni riscontrate.
Il gestore dei servizi telematici, all'esito dell'intervento dell'ufficio, invia al depositante un messaggio di posta elettronica certificata contenente l'esito dell'intervento di accettazione operato dalla cancelleria o dalla segreteria dell'ufficio giudiziario destinatario.
La busta telematica è conservata nel sistema documentale di cui all'art. 11 comma 2.[68]

(*torna all'indice per argomenti*)

Art. 15
Documenti probatori e allegati non informatici – art. 14 del regolamento

I documenti probatori e gli allegati depositati in formato analogico, sono identificati e descritti in un'apposita sezione dell'atto del processo in forma di documento informatico e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati:
numero di ruolo della causa;
progressivo dell'allegato;
indicazione della prima udienza successiva al deposito.

(*torna all'indice per argomenti*)

Art. 16
Deposito dell'atto del processo da parte dei soggetti abilitati interni – art. 15 del regolamento

I soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro trasmissione alla cancelleria o alla segreteria dell'ufficio giudiziario.
L'atto è inserito nella medesima busta telematica di cui all'articolo 14 e viene trasmesso su canale sicuro (SSL v3) al gestore dei servizi telematici, tramite collegamento sincrono (http/SOAP); si applicano le disposizioni di cui all'articolo 10, comma 2.
Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia per immagine in formato PDF, e lo sottoscrive con firma digitale o firma elettronica qualificata.

(*torna all'indice per argomenti*)

Art. 17
Comunicazioni e notificazioni per via telematica – art. 16 del regolamento

Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall'ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell'utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi ai sensi dell'art 16-ter del decreto legge del 30 ottobre 2012, n. 179 oppure ai sensi dell'art 16 comma 7 del medesimo decreto; il formato del messaggio è riportato nell'Allegato 8; la comunicazione o notificazione è riportata nel corpo del messaggio nonché nel file allegato Comunicazione.xml (il relativo DTD è riportato nell'Allegato 4).
La cancelleria o la segreteria dell'ufficio giudiziario, attraverso apposite funzioni messe a disposizione dai sistemi informatici di cui all'articolo 10, provvede ad effettuare una copia per immagine in formato

[68] Comma aggiunto dal DM 28 dicembre 2015.

PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.
Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni.

(*torna all'indice per argomenti*)

Art. 18

Comunicazioni e notificazioni contenenti dati sensibili – art. 16 del regolamento

La comunicazione o la notificazione che contiene dati sensibili è effettuata per estratto: in questo caso al destinatario viene recapitato l'avviso di disponibilità, secondo il formato riportato nell'Allegato 8; il destinatario effettua il prelievo dell'atto integrale accedendo all'indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso.
Il prelievo di cui al comma precedente avviene attraverso l'apposito servizio proxy del portale dei servizi telematici, su canale sicuro (protocollo SSL); tale servizio effettua l'identificazione informatica dell'utente, ai sensi dell'articolo 6; il prelievo è consentito unicamente se l'utente è registrato nel ReGIndE.
Il prelievo di cui al comma precedente avviene da un'apposita area di download del gestore dei servizi telematici, dove viene gestita e mantenuta un'apposita tabella recante le seguenti informazioni:
il codice fiscale del soggetto che ha effettuato il prelievo o la consultazione;
il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 4);
la data e l'ora di invio dell'avviso;
la data e l'ora del prelievo o della consultazione.
Le informazioni di cui al comma precedente vengono conservate per cinque anni.
Nel caso in cui il destinatario sia un'impresa iscritta nel relativo registro o una Pubblica Amministrazione, la comunicazione o la notificazione che contiene dati sensibili è effettuata ai sensi del comma 1; l'utente che accede all'indirizzo (URL) contenuto nel messaggio di PEC di avviso, su canale sicuro (protocollo SSL), viene identificato ai sensi dell'art 6 ed è abilitato ad accedere all'atto integrale solo se appartiene all'impresa destinataria come risultante dal registro delle imprese o se è un dipendente della Pubblica Amministrazione autorizzato.

(*torna all'indice per argomenti*)

Art. 19

Notificazioni per via telematica a cura degli uffici NEP – art. 17 del regolamento

Le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP in formato XML, attraverso un colloquio diretto, via web service, tra i rispettivi gestori dei servizi telematici, su canale sicuro (SSL v3), oppure tramite posta elettronica certificata.
Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tecnici di cui agli articoli 12, 13 e 14; all'interno della busta telematica è inserito il file RichiestaParte.xml, il cui XML-Schema è riportato nell'Allegato 5.
All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.
Alla notificazione per via telematica da parte dell'UNEP si applicano le specifiche della comunicazione per via telematica di cui all'articolo 17; il formato del messaggio di posta elettronica certificata è riportato nell'Allegato 7.
Ai fini della notificazione per via telematica, il sistema informatico dell'UNEP recupera l'indirizzo di posta elettronica del destinatario a seconda della sua tipologia:
soggetti abilitati esterni e professionisti iscritti in albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con legge del 28 gennaio 2009, n. 2: dal registro generale degli indirizzi elettronici, ai sensi dell'articolo 7, comma 6, nonché dall'indice nazionale delle imprese e dei professionisti (INI-PEC), sezione professionisti;
imprese iscritte nel relativo registro: ai sensi dell'articolo 7, comma 5;
cittadini: ai sensi dell'articolo 7, comma 5.
Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette - per via telematica a chi ha richiesto il servizio - il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale o firma elettronica qualificata e congiunta all'atto cui si riferisce, nonché le ricevute di posta

elettronica certificata. La relazione di notificazione è in formato XML e rispetta l'XML-Schema riportato nell'Allegato 5; se il richiedente è un soggetto abilitato esterno, la trasmissione avviene via posta elettronica certificata; il formato del messaggio è riportato nell'Allegato 7.

(*torna all'indice per argomenti*)

Art. 19-*bis*

Notificazioni per via telematica eseguite dagli avvocati – art. 18 del regolamento

Qualora l'atto da notificarsi sia un documento originale informatico, esso deve essere in formato PDF e ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è ammessa la scansione di immagini. Il documento informatico così ottenuto è allegato al messaggio di posta elettronica certificata.

Nei casi diversi dal comma 1, i documenti informatici o copie informatiche, anche per immagine, di documenti analogici, allegati al messaggio di posta elettronica certificata, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti in formato PDF.

Nei casi in cui l'atto da notificarsi sia l'atto del processo da trasmettere telematicamente all'ufficio giudiziario (esempio: atto di citazione), si procede ai sensi del precedente comma 1.

Qualora il documento informatico, di cui ai commi precedenti, sia sottoscritto con firma digitale o firma elettronica qualificata, si applica quanto previsto all'articolo 12, comma 2.

La trasmissione in via telematica all'ufficio giudiziario delle ricevute previste dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53, nonché della copia dell'atto notificato ai sensi dell'articolo 9, comma 1, della medesima legge, è effettuata inserendo l'atto notificato all'interno della busta telematica di cui all'art 14 e, come allegati, la ricevuta di accettazione e la ricevuta di avvenuta consegna relativa ad ogni destinatario della notificazione; i dati identificativi relativi alle ricevute sono inseriti nel file DatiAtto.xml di cui all'articolo 12, comma 1, lettera e.

(*torna all'indice per argomenti*)

Art. 19-*ter*[69]

Modalità dell'attestazione di conformità apposta su un documento informatico separato

1. Quando si deve procedere ad attestare la conformità di una copia informatica, anche per immagine, ai sensi del terzo comma dell'art.16-undecies del decreto legge 18 ottobre 2012, n.179, convertito con modificazioni dalla legge 17 dicembre 2012, n.212, l'attestazione è inserita in un documento informatico in formato PDF e contiene una sintetica descrizione del documento di cui si sta attestando la conformità nonché il relativo nome del file. Il documento informatico contenente l'attestazione è sottoscritto dal soggetto che compie l'attestazione con firma digitale o firma elettronica qualificata secondo quanto previsto all'articolo 12, comma 2.
2. Se la copia informatica è destinata ad essere depositata secondo le regole tecniche previste dall'art.4 del decreto legge 29 dicembre 2009, n.193, convertito con modificazioni dalla legge 22 febbraio 2010, n.24, il documento informatico contenente l'attestazione è inserito come allegato nella "busta telematica" di cui all'articolo 14; i dati identificativi del documento informatico contenente l'attestazione, nonché del documento cui essa si riferisce, sono anche inseriti nel file DatiAtto.xml di cui all'articolo 12, comma 1, lettera e.
3. Se la copia informatica è destinata ad essere notificata ai sensi dell'art.3bis della legge 21 gennaio 1994, n.53, gli elementi indicati al primo comma, sono inseriti nella relazione di notificazione.
4. Nelle ipotesi diverse dai commi 2 e 3, se la copia informatica è destinata ad essere trasmessa tramite posta elettronica certificata, l'attestazione di cui al primo comma è inserita come allegato al messaggio di posta elettronica certificata.
5. In ogni altra ipotesi, l'attestazione di conformità è inserita in un documento informatico in formato PDF contenente i medesimi elementi di cui al primo comma, l'impronta del documento informatico di cui si sta attestando la conformità e il riferimento temporale di cui all'articolo 4 comma 3 del D.P.C.M. 13 novembre 2014. Il documento informatico contenente l'attestazione è sottoscritto dal soggetto che compie l'attestazione con firma digitale o firma elettronica qualificata. L'impronta del documento può essere omessa in tutte le ipotesi in cui il documento informatico contenente l'attestazione di conformità è inserito, unitamente alla copia informatica del documento, in una struttura informatica idonea a garantire l'immodificabilità del suo contenuto.

[69] Articolo inserito dal DM 28 dicembre 2015 pubblicato sulla GU del 7 gennaio 2016 ed in vigore dal 9 gennaio 2016 a seguito della pubblicazione il giorno precedente nell'area pubblica del Portale dei Servizi Telematici del Ministero della Giustizia.

6. L'attestazione di conformità di cui ai commi precedenti può anche riferirsi a più documenti informatici.

(*torna all'indice per argomenti*)

Art. 20

Disposizioni particolari per la fase delle indagini preliminari – art. 19 del regolamento

(omissis)

Art. 21

Requisiti della casella di PEC del soggetto abilitato esterno – art. 20 del regolamento

La casella di posta elettronica certificata di un soggetto abilitato esterno deve disporre di uno spazio disco minimo pari a 1 Gigabyte.

(*torna all'indice per argomenti*)

Art. 22

Richiesta delle copie di atti e documenti – art. 21 del regolamento

Per la richiesta telematica di copie di atti e documenti relativi al procedimento è disponibile, sul punto di accesso e sul portale dei servizi telematici, un servizio sincrono attraverso il quale individuare i documenti di cui richiedere copia e, in seguito al perfezionamento del pagamento, inoltrare la richiesta effettiva della copia stessa.

Il soggetto che ne ha diritto può richiedere:

copia semplice in formato digitale;

copia semplice per l'avvocato non costituito in formato digitale;

copia autentica in formato digitale;

copia esecutiva in formato digitale;

copia semplice in formato cartaceo;

copia autentica in formato cartaceo;

copia esecutiva in formato cartaceo.

I dati relativi alla richiesta sono inoltrati all'ufficio giudiziario attraverso l'invocazione di un apposito web service; al richiedente è restituito l'identificativo univoco della richiesta inoltrata. Tale identificativo univoco è associato all'intero flusso di gestione della richiesta e di rilascio della copia.

Nel caso in cui la copia non possa essere rilasciata il sistema, in maniera automatica, comunica al richiedente l'impossibilità di evadere la richiesta.

Art. 23

Rilascio delle copie di atti e documenti – art. 21 del regolamento

Il rilascio della copia informatica di atti e documenti viene eseguito secondo le specifiche di cui all'articolo 16 del regolamento e dell'art. 23-bis del CAD; la copia è inviata al richiedente in allegato ad un messaggio di posta elettronica certificata, secondo il formato riportato nell'Allegato 9.

Nel caso di copia di documenti contenenti dati sensibili o nel caso di copia di documenti che eccedono il massimo consentito dalla posta elettronica certificata, il messaggio di cui al comma precedente contiene l'avviso di disponibilità della copia, secondo il formato riportato nell'Allegato 9; il prelievo avviene secondo le specifiche di cui all'articolo 18, commi 2, 3 e 4.

CAPO IV – CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Art. 24

Requisiti di sicurezza – art. 26 del regolamento

L'architettura dei servizi di consultazione aderisce al modello MVC (Model View Controller) e prevede il disaccoppiamento del front-end, localizzato sul punto di accesso o sul portale dei servizi telematici, dal back-end, localizzato sul gestore dei servizi telematici, incaricato di esporre i servizi sottoforma di web service (http/SOAP).

Il portale dei servizi telematici espone, attraverso un apposito servizio proxy, i web service forniti dal gestore dei servizi telematici, a beneficio dei punti di accesso e di applicazioni esterne.

I punti di accesso realizzano autonomamente la parte di front-end, che deve essere localizzata all'interno della intranet del PdA stesso e non deve essere accessibile direttamente dall'esterno.

I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne.

Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.
Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del portale dei servizi telematici.
L'accesso ai servizi di consultazione avviene su canale sicuro (protocollo SSL) previa identificazione informatica su di un punto di accesso o sul portale dei servizi telematici, secondo le specifiche di cui all'articolo 6; a seguito di tale identificazione, il punto di accesso o il portale dei servizi telematici attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice fiscale del soggetto che effettua l'accesso (nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy trasmette la richiesta al web service del gestore dei servizi telematici.
In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal regolamento.
In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche dell'Agenzia per l'Italia Digitale; in questo caso, il Direttore Generale S.I.A., valutata la soluzione proposta e opportunamente descritta nel piano della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.
Il punto di accesso può consentire l'accesso a soggetti delegati da un utente registrato (soggetto delegante), con le stesse modalità di cui ai commi 7, 8 e 9, purchè il soggetto delegante abbia predisposto un atto di delega, sottoscritto con firma digitale, che il punto di accesso conserva per cinque anni unitamente alla tracciatura di ogni accesso effettuato su delega; le informazioni e gli atti di cui sopra sono forniti su richiesta al Ministero della giustizia.
Fuori dai casi previsti ai commi 1 e 10, l'architettura dei servizi di consultazione prevede in via residuale che il punto di accesso o il portale dei servizi telematici effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che rende disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati identificativi del soggetto vengono inseriti nell'header HTTP della richiesta.
I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
L'elenco dei punti di accesso autorizzati è pubblicato nell'area pubblica del portale dei servizi telematici e nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
Il punto di accesso si dota di un piano della sicurezza, depositato al re-sponsabile per i sistemi informativi automatizzati unitamente all'istanza di iscrizione all'elenco pubblico dei punti di accesso, che prevede la trattazione, esaustiva e dettagliata, dei seguenti argomenti:
struttura logistica e operativa dell'organizzazione;
ripartizione e definizione delle responsabilità del personale addetto;
descrizione dei dispositivi installati;
descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);
descrizione delle procedure di registrazione delle utenze;
descrizione relativa all'implementazione dei meccanismi di identificazione informatica;
qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;
procedura di gestione delle copie di sicurezza dei dati;
procedura di gestione dei disastri;
analisi dei rischi e contromisure previste;
descrizione dell'eventuale processo di delega di cui al comma 10 nonché delle modalità di conservazione dell'elenco dei soggetti delegati e delle eventuali revoche delle deleghe;
descrizione della modalità di verifica dell'effettiva funzionalità e adeguatezza del sistema di sicurezza del punto di accesso.
Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi in-formativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.
Il punto di accesso abilita i propri iscritti unicamente a usufruire dei servizi esplicitamente autorizzati dal responsabile per i sistemi informativi automatizzati e riportati nel catalogo dei servizi telematici.

Il punto di accesso si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della giustizia.
Il punto di accesso fornisce al Ministero della giustizia, su richiesta, i dati di censimento sul ReGIndE di cui articolo 8 comma 1 per i casi di iscrizione dei professionisti non iscritti in albi di cui articolo 9 comma 1.
Il punto di accesso verifica l'effettiva funzionalità e adeguatezza del sistema di sicurezza almeno una volta l'anno e provvede ad inviare l'esito delle stesse, unitamente ad eventuali variazioni nei contenuti del piano, all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.dog@giustiziacert.it.

Art. 25

Registrazione dei soggetti abilitati esterni e degli utenti privati – art. 28 del regolamento

L'utente accede ai servizi di consultazione previa registrazione presso un punto di accesso autorizzato o presso il portale dei servizi telematici.
Il punto di accesso o il portale dei servizi telematici effettuano la registrazione del soggetto abilitato esterno o dell'utente privato, prelevando il codice fiscale dal token crittografico dell'utente; attraverso un'apposita maschera web, l'utente (senza poter modificare il codice fiscale) completa i propri dati, inserendo almeno le seguenti informazioni:
nome e cognome
luogo e data di nascita
residenza
domicilio
ruolo
consiglio dell'ordine o ente di appartenenza.
I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per cinque anni.
Gli esperti e gli ausiliari del giudice, non iscritti ad alcun albo professionale o per i quali il proprio ordine non abbia provveduto all'invio dell'albo, presentano, all'atto della registrazione, copia elettronica in formato PDF dell'incarico di nomina da parte del giudice; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
Qualora il professionista sia iscritto ad un albo dei consulenti tecnici, istituito presso un tribunale (ai sensi del Capo II, sezione 1, delle disposizioni di attuazione del codice di procedura civile), al PdA viene presentata copia elettronica in formato PDF del provvedimento di iscrizione all'albo stesso da parte del comitato; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
Il punto di accesso è tenuto a conservare i documenti informatici di cui ai commi precedenti, e a renderli disponibili, su richiesta, al Ministero della giustizia.
I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all'allegato 11.

CAPO V – PAGAMENTI TELEMATICI

Art. 26

Requisiti relativi al processo di pagamento telematico – art. 30 del regolamento

Al fine di comunicare in via telematica all'ufficio giudiziario l'avvenuto pagamento delle spese, dei diritti e del contributo unificato, la ricevuta di versamento è inserita come allegato della busta telematica nel caso di inoltro via PEC, oppure è associata alla richiesta telematica nel caso di istanza gestita tramite un flusso sincrono.
Il servizio di pagamento in modalità telematica è messo a disposizione dei soggetti abilitati nell'ambito delle funzionalità del punto di accesso e del portale dei servizi telematici, con lo scopo di permettere il pagamento attraverso strumenti telematici e di ottenere la ricevuta di pagamento attraverso il medesimo canale telematico; l'accesso ai servizi di pagamento avviene previa identificazione informatica di cui all'articolo 6.
Le regole per l'esecuzione del pagamento, le modalità di interconnessione tra i sistemi nonchè le modalità di rendicontazione e riconciliazione dei pagamenti rispettano le Linee Guida emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal decreto legge del 30 ottobre 2012, n. 179.

Il portale dei servizi telematici si avvale dell'infrastruttura e della piattaforma tecnologica messa a disposizione dall'Agenzia per l'Italia Digitale, attraverso il Sistema Pubblico di Connettività, (Nodo dei Pagamenti-SPC) allo scopo di garantire l'interconnessione e l'interoperabilità tra le Pubbliche Amministrazioni e i Prestatori di Servizi di Pagamento;
Il portale dei servizi telematici espone ai punti di accesso servizi web per l'esecuzione dei pagamenti telematici utilizzando le funzionalità messe a disposizione dal Nodo dei Pagamenti-SPC. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del portale dei servizi telematici.
I punti di accesso possono mettere a disposizione dei propri utenti il servizio di pagamento telematico, definendo opportuni accordi con uno o più prestatori di servizi di pagamento, nel rispetto di quanto indicato al comma 3.
Nei casi di cui al precedente comma, il punto di accesso è garante nei confronti del Ministero della Giustizia del rispetto delle Linee Guida di cui al comma 3, relativamente alle modalità di riversamento verso la banca tesoriera e alla rendicontazione; il punto di accesso rispetta quanto indicato nelle Linee Guida relativamente al flusso di rendicontazione nei confronti del Ministero della Giustizia.
Il processo di pagamento consente all'utente di scegliere tra diverse modalità di pagamento messe a sua disposizione da una molteplicità di prestatori di servizi di pagamento che aderiscono all'infrastruttura del Nodo dei pagamenti-SPC.
La ricevuta di pagamento restituita all'utente a fronte del pagamento effettuato in via telematica costituisce prova del trasferimento dell'importo versato sul conto corrente intestato alla Tesoreria dello Stato
Per il recupero delle somme erroneamente versate si procede secondo le modalità previste dalla legge.
(*torna all'indice per argomenti*)

Art. 27

Oggetti informatici interessati nel pagamento telematico – art. 30 del regolamento

La Richiesta di Pagamento Telematico (RPT), relativa al versamento di una o più spettanze legate ad un medesimo servizio, è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
definisce gli elementi necessari a caratterizzare i pagamenti, in particolare qualifica il versamento attraverso un identificativo univoco di cui al successivo comma 5;
contiene i dati identificativi del soggetto che esegue il pagamento, contiene una parte riservata (Dati Specifici Riscossione) per inserire informazioni elaborabili automaticamente dai sistemi della Giustizia;
viene predisposta dal soggetto che procede al pagamento ed inviata dal portale dei servizi telematici al Nodo dei Pagamenti-SPC;
La Ricevuta Telematica (RT) è restituita al soggetto che ha eseguito il pagamento a fronte di ogni singola RPT: essa è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
definisce gli elementi necessari a qualificare il pagamento, tra cui l'esito del pagamento stesso e, in caso positivo, l'identificativo univoco del pagamento assegnato dal sistema del prestatore dei servizi di pagamento (Psp);
trasferisce inalterate le stesse informazioni ricevute in ingresso (RPT) relative alla parte riservata (Dati Specifici Riscossione) a disposizione della PA
Il soggetto che emette la Ricevuta Telematica (RT) di cui al comma 2, la sottoscrive- ai sensi dell'art 30, comma 5 del regolamento- con firma digitale o firma elettronica qualificata in formato CAdES; a tal fine possono essere utilizzati certificati emessi da una autorità di certificazione allo scopo messa a disposizione dell'Agenzia per l'Italia Digitale.
Al fine di qualificare in maniera univoca il pagamento all'interno del dominio giustizia, è definito l'identificativo univoco di pagamento (IUV)) secondo i formati previsti dalle Linee Guida emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal decreto legge del 30 ottobre 2012, n. 179.
Lo IUV (identificato con il nome CRS nell'ambito Giustizia) è generato esclusivamente dal portale dei servizi telematici attraverso l'invocazione di un web service di cui all'art 26, comma 5 e ha il seguente formato: <check digits> <identificatore univoco>, dove:
<check digit> costituisce il codice numerico di controllo (2 posizioni);
<identificatore univoco> è rappresentato da 33 posizioni alfanumeriche così strutturate: <codice PdA richiedente><codice Sistema Gestore><codice univoco operazione>; la sezione <codice PdA richiedente> (4 caratteri alfanumerici) assicura flessibilità nella emissione del CRS; la sezione <codice Sistema Gestore> (4 caratteri alfanumerici) rappresenta il sistema a cui è destinata la ricevuta; la sezione

<codice univoco operazione> (25 caratteri alfanumerici) contiene un codice 'non ambiguo' all'interno del dominio entro il quale viene generato.
Lo IUV viene inserito nella struttura RPT (elemento identificativoUnivocoVersamento) e viene restituito invariato al punto di accesso o al portale dei servizi telematici all'interno della RT (elemento identificativoUnivocoVersamento).
Al momento dell'accettazione della ricevuta di pagamento, il sistema informatico dell'ufficio giudiziario controlla, attraverso l'identificativo univoco, che la ricevuta telematica non sia stato già utilizzata per altri servizi di pagamento e, in caso di esito positivo del controllo, la ricevuta viene marcata al fine di non permetterne il riutilizzo.

Art. 28
Riscontro del pagamento telematico – art. 30 del regolamento

Allo scopo di permettere all'Amministrazione di verificare e riscontrare le ricevute generate a seguito di pagamento telematico, nell'ambito del dominio giustizia è configurato un sottosistema per la memorizzazione e gestione delle Ricevute Telematiche di cui all'articolo 27; il sottosistema è denominato Repository Ricevute Telematiche (RRT) ed è accessibile a tutte le applicazioni e ai sistemi del dominio Giustizia interessate dai pagamenti telematici.
Il punto di accesso o il portale dei servizi telematici provvede a registrare la RT nel sistema RRT contestualmente al rilascio della stessa al soggetto abilitato esterno richiedente; la registrazione si conclude con esito positivo solo se lo IUV presente nella RT è stato generato dal portale dei servizi telematici
Per la registrazione della RT nel al sistema RRT, il portale dei servizi telematici espone un apposito web service il cui WSDL è pubblicato nell'area pubblica del portale dei servizi telematici.
Il sistema RRT permette la gestione delle RT e dei relativi identificativi univoci di pagamento secondo le modalità indicate nell'articolo 27.
Le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1 sono messe a disposizione, sulla base di specifica convenzione da sottoscriversi con il Direttore Generale S.I.A., degli enti e delle agenzie pubbliche per l'adempimento dei propri compiti di verifica, controllo e contrasto all'evasione ed elusione.
I soggetti abilitati che hanno effettuato i versamenti in via telematica possono consultare sul portale dei servizi telematici, previa identificazione informatica di cui all'articolo 6, le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1.

Art. 29
Diritto di copia – art. 31 del regolamento

Il sistema informatico del Ministero della giustizia comunica all'interessato l'importo da versare per i diritti di copia; tale importo è calcolato, sulla base delle vigenti disposizioni normative e regolamentari, in base alle indicazioni fornite dall'interessato al momento dell'individuazione dei documenti di cui richiedere copia. L'informazione è messa a disposizione dell'interessato attraverso il servizio di richiesta copie attivo sul punto di accesso e sul portale dei servizi telematici; unitamente all'importo dei diritti ed oneri viene comunicato all'interessato anche l'identificativo univoco associato associato al flusso di gestione della richiesta e rilascio della copia.
La richiesta di copia è soddisfatta solo dopo che è pervenuta la ricevuta telematica di pagamento di cui all'articolo 27, comma 2.

CAPO VI – DISPOSIZIONI FINALI E TRANSITORIE
Art. 30
Gestione del transitorio – art. 35 del regolamento

Al momento dell'attivazione, sul ReGIndE di cui all'articolo 7, dell'indirizzo di posta elettronica certificata del soggetto abilitato esterno, il portale dei servizi telematici invia un messaggio di PEC al medesimo soggetto comunicando l'avvenuta attivazione. La comunicazione riporta espressa avvertenza che il soggetto abilitato esterno dovrà usare per le successive trasmissioni unicamente la casella PEC.
A decorrere dalla comunicazione di cui al comma 1, il soggetto abilitato esterno utilizza unicamente il sistema di trasmissione della posta elettronica certificata, così come disciplinato nel presente provvedimento.
A decorrere dalla comunicazione di cui al comma 1, il gestore dei servizi telematici:
Invia comunicazioni e notificazioni solamente alla casella di PEC ivi indicata;

Consente la ricezione di atti solo tramite PEC, rifiutando automatica-mente il deposito tramite altro canale.
Le pubbliche amministrazioni comunicano il proprio indirizzo di posta elettronica certificata ai sensi dell'articolo 9-bis del presente provvedimento entro il novantesimo giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana; le pubbliche amministrazioni possono comunicare detto indirizzo anche successivamente alla scadenza di detto termine; l'indirizzo sarà reso consultabile dagli uffici giudiziari a partire dal 91° giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana.

Art. 31
Efficacia

Fatto salvo quanto indicato dall'articolo 30 comma 4, il presente provvedimento acquista efficacia decorsi 15 giorni dalla sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana e sostituisce l'analogo provvedimento del 18 luglio 2011.

Allegati
(Omissis)

Allegato 6
Formato dei messaggi relativi al deposito della busta telematica [70]

Si riportano nel seguito le specifiche relative al formato dei messaggi di posta elettronica certificata interessati dal flusso di deposito.

Deposito dell'atto Mittente	Indirizzo di posta elettronica certificata di un soggetto abilitato esterno registrato nel ReGIndE. Depositante dell'atto.
Destinatario	Indirizzo di posta elettronica certificata dell'ufficio giudiziario interessato.
Oggetto	**Sintassi: DEPOSITO [oggetto_deposito] Dove: [oggetto_deposito] = eventuale testo libero (ignorato dal sistema) Esempio: DEPOSITO Ricorso A vs. B**
Corpo	Eventuale testo libero (ignorato dal sistema)
Allegati	[qualsiasi nome].enc: busta telematica (corrisponde a "Atto.enc"), come da specifiche; il sistema accetta un solo file con estensione .enc, ed elabora solo quello; nel caso in cui vi siano più file .enc, il sistema elabora unicamente il primo

(ritorna all'indice cronologico)

[70] Si riporta l'allegato 6 poiché lo stesso disciplina il formato con il quale deve essere indicato l'oggetto del messaggio PEC attraverso il quale avviene il deposito telematico dell'atto da parte dell'abilitato esterno (avvocati ed ausiliari del giudice) e la cui inosservanza determina il mancato superamento dei controlli automatici.

D.P.C.M. 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 (*GU n. 117 del 21-5-2013*)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale e, in particolare, gli articoli 20, comma 3, 24 comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;

Visto il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante Codice in materia di protezione dei dati personali;

Visto il decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici, pubblicato nella Gazzetta Ufficiale 6 giugno 2009, n. 129;

Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, recante «Misure urgenti per la crescita del Paese», convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, con cui è stato soppresso DigitPA, le cui funzioni sono state attribuite all'Agenzia per l'Italia digitale;

Visto il decreto del Presidente della Repubblica in data 29 novembre 2011, con il quale il Presidente Filippo Patroni Griffi è stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei Ministri del 4 dicembre 2011, con il quale al predetto Ministro senza portafoglio è stato conferito l'incarico per la pubblica amministrazione e la semplificazione;

Visto il decreto del Presidente del Consiglio dei Ministri 13 dicembre 2011 recante delega di funzioni del Presidente del Consiglio dei Ministri al Ministro senza portafoglio, Presidente Filippo Patroni Griffi, in materia di pubblica amministrazione e semplificazione, tra cui, in raccordo con il Ministro delegato per l'innovazione tecnologica e lo sviluppo della società dell'informazione, prof. Francesco Profumo, le funzioni in materia di disciplina delle innovazioni connesse all'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni e nei relativi sistemi informatici e di telecomunicazione, nonché di adeguamento, per amministrazioni ed enti pubblici, della normativa vigente relativa all'organizzazione e alle procedure in ragione dell'uso delle predette tecnologie;

Rilevata la necessità di sostituire il citato decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009, in considerazione delle modifiche apportate alla disciplina delle firme elettroniche contenuta nel Codice dell'amministrazione dal decreto legislativo 30 dicembre 2010, n. 235;

Acquisito il parere tecnico di DigitPA di cui al decreto legislativo 1° dicembre 2009, n. 177 e successive modificazioni;

Sentito il Garante per la protezione dei dati personali;

Sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 nella seduta del 19 gennaio 2012;

Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con decreto legislativo 23 novembre 2000, n. 427;

Di concerto con il Ministro dell'istruzione, dell'università e della ricerca;

Decreta:

Titolo I
DISPOSIZIONI GENERALI

Art. 1
Definizioni

1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute nell'art. 1 del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni. Si intende, inoltre, per:

a) Codice: il Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

b) chiavi: la coppia di chiavi asimmetriche come definite all'art. 1, comma 1, lettere h) e i), del Codice;

c) Agenzia: l'Agenzia per l'Italia Digitale, di cui gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83;

d) compromissione della chiave privata: la sopravvenuta assenza di affidabilità nelle caratteristiche di sicurezza della chiave crittografica privata;
e) dati per la creazione della firma elettronica qualificata o digitale: l'insieme dei codici personali e delle altre quantità di sicurezza, quali le chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica qualificata o una firma digitale;
f) evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
g) funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;
h) impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;
i) marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;
l) registro dei certificati: la combinazione di uno o più archivi informatici, tenuto dal certificatore, contenente tutti i certificati emessi;
m) riferimento temporale: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
n) dispositivi sicuri per la generazione della firma elettronica qualificata: mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 12;
o) dispositivi sicuri per la generazione della firma digitale: mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 13;
p) HSM: insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche;
q) firma remota: particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;
r) firma automatica: particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo;
s) certificato di attributo: certificato elettronico contenente le qualifiche di cui all'art. 28, comma 3, lettera a) del Codice, possedute da un soggetto;
t) soluzioni di firma elettronica avanzata: soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis) del Codice.

Art. 2
Ambito di applicazione

1. Il presente decreto stabilisce, ai sensi degli articoli 20, 24, comma 4, 27, 28, 29, 32, 33, 35, comma 2, e 36, le regole tecniche per la generazione, apposizione e verifica della firma elettronica avanzata, qualificata e digitale, per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati.
2. Le disposizioni di cui al Titolo II si applicano ai certificatori che rilasciano al pubblico certificati qualificati in conformità al Codice.
3. Ai certificatori accreditati o che intendono accreditarsi ai sensi del Codice, si applicano, oltre a quanto previsto dal comma 2, anche le disposizioni di cui al Titolo III.
4. I certificatori accreditati rendono disponibile ai propri titolari un sistema di validazione temporale conforme alle disposizioni di cui al Titolo IV.
5. Le disposizioni di cui al Titolo V si applicano ai soggetti che intendono realizzare soluzioni di firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis) del Codice. Non si applicano a soluzioni di firma elettronica qualificata e digitale.
6. Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione europea e dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata nella Gazzetta Ufficiale dell'Unione europea, Serie L, n. 13 del 19 gennaio 2000, è consentito di circolare liberamente nel mercato interno.

Art. 3
Disposizioni generali

1. La firma elettronica qualificata è generata esclusivamente con i dispositivi di cui all'art. 1, comma 1, lettere n) e p).

2. La firma digitale è generata con i dispositivi di cui all'art. 1, comma 1, lettere o) e p).
3. Le presenti regole tecniche definiscono le caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale ai fini e per gli effetti di cui all'art. 20, comma 1-bis, e 21, comma 2, del Codice.
4. La firma remota di cui all'art. 1, comma 1, lettera q), è generata su un HSM custodito e gestito, sotto la responsabilità, dal certificatore accreditato ovvero dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi. Il certificatore deve essere in grado, dato un certificato qualificato, di individuare agevolmente il dispositivo afferente la corrispondente chiave privata.
5. Nel caso in cui il dispositivo di cui al comma 4 non sia custodito dal certificatore, egli deve: a) indicare al soggetto che custodisce il dispositivo le procedure operative, gestionali e le misure di sicurezza fisica e logica che tale soggetto è obbligato ad applicare; b) effettuare verifiche periodiche sulla corretta applicazione delle indicazioni di cui alla lettera a), che il soggetto che custodisce il dispositivo ha l'obbligo di consentire ed agevolare; c) redigere i verbali dell'attività di verifica di cui alla lettera b) che potranno essere richiesti in copia dall'Agenzia ai fini dell'attività di cui all'art. 31 del Codice; d) comunicare all'Agenzia il luogo in cui i medesimi dispositivi sono custoditi; e) effettuare ulteriori verifiche su richiesta dell'Agenzia consentendo di partecipare anche ad incaricati dello stesso ente; f) assicurare che il soggetto che custodisce il dispositivo si impegni a consentire le verifiche di cui alle lettere b) ed e).
6. Nel caso in cui il certificatore venga a conoscenza dell'inosservanza di quanto previsto al comma 5, procede alla revoca dei certificati afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.
7. La firma remota di cui all'art. 1, comma 1, lettera q), è realizzata con misure tecniche ed organizzative, esplicitamente approvate, per le rispettive competenze, dall'Agenzia, nell'ambito delle attività di cui agli articoli 29 e 31 del Codice, e da OCSI, per quanto concerne la sicurezza del dispositivo ai sensi dell'art. 35 del Codice, tali da garantire al titolare il controllo esclusivo della chiave privata.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Titolo II

FIRME ELETTRONICHE QUALIFICATE E DIGITALI

Art. 4

Norme tecniche di riferimento

1. Le regole tecniche relative ai dispositivi sicuri per la generazione delle firme di cui all'art. 35 del Codice sono conformi alle norme generalmente riconosciute a livello internazionale.
2. Gli algoritmi di generazione e verifica della firma elettronica qualificata e della firma digitale, le caratteristiche delle chiavi utilizzate, le funzioni di hash, i formati e le caratteristiche dei certificati qualificati e dei certificati di attributo, i formati e le caratteristiche della firma elettronica qualificata e della firma digitale, delle marche temporali, le caratteristiche delle applicazioni di verifica di cui all'art. 14, il formato dell'elenco di cui all'art. 43 del presente decreto, le modalità con cui rendere disponibili le informazioni sullo stato dei certificati, sono definiti, anche ai fini del riconoscimento e della verifica del documento informatico, con provvedimenti dell'Agenzia e pubblicati sul sito internet dello stesso ente. Nelle more dell'emanazione di tali provvedimenti continua ad applicarsi la deliberazione del Centro nazionale per l'informatica nella pubblica amministrazione n. 45 del 21 maggio 2009 e successive modificazioni.
3. Il documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21, comma 2, del Codice, se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Art. 5

Caratteristiche generali delle chiavi

1. Una coppia di chiavi per la creazione e la verifica della firma elettronica qualificata o della firma digitale può essere attribuita ad un solo titolare.
2. Se il soggetto appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del Codice, deve utilizzare una coppia di chiavi destinata a tale

scopo, diversa da tutte le altre in suo possesso. L'utilizzo di tale procedura deve essere indicato esplicitamente nel certificato qualificato.
3. Se la procedura automatica di cui al comma 2 fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.
4. Ai fini del presente decreto, le chiavi afferenti i certificati qualificati ed i correlati servizi, si distinguono secondo le seguenti tipologie: a) chiavi di sottoscrizione, destinate alla generazione e verifica della firma elettronica qualificata o della firma digitale apposta o associata ai documenti; b) chiavi di certificazione, utilizzabili per la generazione e verifica delle firme apposte o associate ai certificati qualificati, per la sottoscrizione delle informazioni sullo stato di validità dei certificati, per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale; c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali; d) chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati; e) chiavi destinate alla sottoscrizione del separato certificato di attributo.
5. Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste per ciascuna tipologia dal comma 4, salvo che, con riferimento esclusivo alle chiavi di cui al medesimo comma 4, lettera b), l'Agenzia non ne autorizzi l'utilizzo per altri scopi.
6. Le caratteristiche quantitative e qualitative delle chiavi sono tali da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche, in conformità con quanto indicato nei provvedimenti di cui all'art. 4, comma 2.
7. L'uso delle chiavi di cui al comma 4, lettera d), e il profilo del certificato alle stesse associato sono definiti con il provvedimento di cui all'art. 4, comma 2. A tali chiavi dovrà essere associato un certificato sottoscritto con le stesse chiavi di certificazione con cui sono sottoscritti i certificati di cui si forniscono informazioni sullo stato di validità.

Art. 6
Generazione delle chiavi

1. La generazione della coppia di chiavi è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e un adeguato livello di sicurezza della coppia generata, nonché la segretezza della chiave privata.
2. Il sistema di generazione della coppia di chiavi comunque assicura:
a) la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
b) l'utilizzo di algoritmi che consentano l'equiprobabilità di generazione di tutte le coppie possibili;
c) l'autenticazione informatica del soggetto che attiva la procedura di generazione.

Art. 7
Modalità di generazione delle chiavi

1. Le chiavi di cui all'art. 5, comma 4, lettere b) e d) possono essere generate esclusivamente in presenza del responsabile del servizio.
2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.
3. La generazione delle chiavi di sottoscrizione effettuata autonomamente dal titolare, avviene all'interno del dispositivo sicuro per la generazione delle firme, che è rilasciato o indicato dal certificatore, con modalità atte ad impedire che la medesima chiave possa essere associata a più certificati.
4. Il certificatore è tenuto ad assicurarsi che il dispositivo sicuro per la generazione della firma elettronica qualificata, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 35 del Codice e agli articoli 11 e 12 del presente decreto e a fornire all'Agenzia gli elementi necessari ai fini delle verifiche e dei controlli di cui all'art. 31 del Codice.
5. Il certificatore è tenuto ad assicurarsi che il dispositivo sicuro per la generazione della firma digitale, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 35 del Codice e agli articoli 11 e 13 del presente decreto e a fornire all'Agenzia gli elementi necessari ai fini delle verifiche e dei controlli di cui all'art. 31 del Codice.
6. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo sicuro per la generazione delle firme fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art. 8
Conservazione delle chiavi e dei dati per la creazione della firma elettronica qualificata o digitale

1. Fatto salvo quanto disposto ai commi 2, 3 e 4, è vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate, purché ciò avvenga con modalità tali da non ridurre il livello di sicurezza e di riservatezza delle chiavi stesse.
3. Per la firma remota, è consentita l'esportazione sicura delle chiavi private di cui all'art. 5, comma 4, lettera a) presenti su HSM al di fuori del dispositivo stesso, esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento del dispositivo in uso, purché protette con algoritmi crittografici ritenuti adeguati ai fini della certificazione e purché le operazioni di esportazione e importazione delle chiavi siano effettuate mediante funzionalità di sicurezza certificate implementate dai dispositivi sicuri di firma. La conservazione delle chiavi esportate deve avvenire nell'ambiente operativo del dispositivo sicuro di firma, sottoposta a opportune misure di sicurezza di tipo fisico e procedurale che debbono essere descritte, in forma di obiettivi o ipotesi per l'ambiente, nel relativo traguardo di sicurezza.
4. Per la firma remota, è consentita la replicazione in sicurezza delle chiavi private di cui all'art. 5, comma 4, lettera a) presenti su HSM, al fine di realizzare una configurazione ad alta affidabilità del dispositivo sicuro di firma, a condizione che tale configurazione rientri tra quelle sottoposte a certificazione ai sensi degli articoli 12 o 13. L'operazione di replicazione deve prevedere la protezione delle chiavi con algoritmi crittografici ritenuti adeguati ai fini della certificazione ed essere effettuata mediante funzionalità di sicurezza certificate implementate dal dispositivo sicuro di firma. Le chiavi replicate debbono essere conservate all'interno di dispositivi certificati con le stesse caratteristiche di sicurezza e controllati dal dispositivo certificato di origine, collocati nello stesso ambiente operativo o in altro ambiente con equivalente livello di sicurezza. Solo uno dei dispositivi fisici in questa configurazione deve essere abilitato ad effettuare le operazioni di firma.
5. Il titolare della coppia di chiavi: a) assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal certificatore al fine di adempiere agli obblighi di cui all'art. 32, comma 1, del Codice; b) conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore; c) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale inutilizzabili o di cui abbia perduto il possesso o il controllo esclusivo; d) salvo quanto previsto dai commi 3 e 4, mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma elettronica qualificata o digitale; e) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale qualora abbia il ragionevole dubbio che essi possano essere usati da altri.

Art. 9

Generazione delle chiavi di sottoscrizione al di fuori del dispositivo di firma

1. Il certificatore, se la certificazione del dispositivo di firma lo consente, può utilizzare un sistema diverso da quello destinato all'uso della chiave privata per la generazione delle chiavi di sottoscrizione.
2. Il certificatore descrive dettagliatamente il sistema di cui al comma 1 nel piano della sicurezza, di cui all'art. 35.

Art. 10

Sicurezza del sistema di generazione delle chiavi diverso dal dispositivo di firma

1. Se la generazione delle chiavi di sottoscrizione avviene su un sistema di cui all'art. 9, il sistema di generazione assicura: a) l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura; b) il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui verrà utilizzata.
2. Il sistema di generazione è isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto.
3. L'accesso al sistema è controllato e ciascun utente è preventivamente identificato per l'accesso fisico e autenticato per l'accesso logico. Ogni sessione di lavoro è registrata nel giornale di controllo.
4. Il sistema è dotato di strumenti di controllo della propria configurazione che consentono di verificare l'autenticità e l'integrità del software installato e l'assenza di programmi non previsti dalla procedura e di dati residuali provenienti dalla generazione di coppie di chiavi precedenti che possano inficiare l'equiprobabilità della generazione di quelle successive.

Art. 11

Dispositivi sicuri e procedure per la generazione delle firme elettroniche qualificate e delle firme digitali

1. La generazione delle firme elettroniche qualificate e delle firme digitali avviene all'interno di un dispositivo sicuro per la generazione delle firme, in maniera tale che non sia possibile l'intercettazione della chiave privata utilizzata.
2. Il dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale deve poter essere attivato esclusivamente dal titolare mediante sistemi di autenticazione ritenuti adeguati, secondo le rispettive competenze, dall'OCSI e dall'Agenzia, prima di procedere alla generazione della firma.
3. L'Agenzia, nell'ambito dell'attività di cui agli articoli 29 e 31 del Codice, valuta l'adeguatezza tecnologica dei sistemi di autenticazione per quanto concerne l'interazione fra il titolare e il dispositivo sicuro per la generazione della firma, tenuto conto del traguardo di sicurezza di cui al DPCM 30 ottobre 2003 e del contesto di utilizzo.
4. La personalizzazione del dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale garantisce almeno: a) l'acquisizione da parte del certificatore dei dati identificativi del dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale utilizzato e la loro associazione al titolare; b) la registrazione nel dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale del certificato qualificato, relativo alle chiavi di sottoscrizione del titolare.
5. La personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali può prevedere, per l'utilizzo nelle procedure di firma, la registrazione, nel dispositivo medesimo, del certificato elettronico relativo alla chiave pubblica del certificatore la cui corrispondente privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare.
6. La personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali è registrata nel giornale di controllo di cui all'art. 36.
7. Il certificatore adotta, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate e digitali, procedure atte ad identificare il titolare del dispositivo medesimo e dei certificati in esso contenuti.
8. I certificatori che rilasciano certificati qualificati forniscono almeno un sistema che consenta la generazione delle firme elettroniche qualificate e digitali.

Art. 12
Ulteriori requisiti per i dispositivi sicuri per la generazione della firma elettronica qualificata

1. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma elettronica qualificata, anche remota o automatica, prevista dall'art. 35 del Codice è effettuata secondo criteri non inferiori a quelli previsti: a) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai profili di protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni; b) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai profili di protezione o traguardi di sicurezza giudicati adeguati ai sensi dell'art. 35, commi 5 e 6 del Codice e successive modificazioni.

Art. 13
Ulteriori requisiti per i dispositivi sicuri per la generazione della firma digitale

1. Salvo quanto disposto al comma 2, la certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma digitale è effettuata ai sensi dell'art. 12.
2. L'organismo di certificazione della sicurezza informatica può individuare ulteriori modalità di verifica della conformità ai requisiti di sicurezza dei dispositivi sicuri per la creazione di una firma digitale remota ai sensi dell'art. 35, commi 1 e 2 del Codice.
3. I certificati qualificati afferenti chiavi private custodite nei dispositivi di cui al comma 2, non devono contenere l'estensione qcStatements id-etsi-qcs-QcSSCD.

Art. 14
Verifica delle firme elettroniche qualificate e digitali

1. I certificatori che rilasciano certificati qualificati forniscono ovvero indicano almeno un sistema che consenta di effettuare la verifica delle firme elettroniche qualificate e delle firme digitali, conforme a quanto stabilito con i provvedimenti di cui all'art. 4, comma 2.
2. Il sistema di verifica delle firme elettroniche qualificate e digitali deve quantomeno: a) presentare, almeno sinteticamente, lo stato di aggiornamento delle informazioni di validità dei certificati di certificazione presenti nell'elenco pubblico; b) visualizzare le informazioni presenti nel certificato qualificato, in attuazione di quanto stabilito nell'art. 28, comma 3, del Codice, nonché le estensioni obbligatorie nel certificato qualificato (qcStatements), indicate nei provvedimenti di cui all'art. 4, comma

2; c) consentire l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori; d) in caso di firme multiple, visualizzare l'eventuale dipendenza tra queste; e) visualizzare chiaramente l'esito della verifica dello stato dei certificati qualificati e di eventuali certificati di attributo secondo le modalità indicate nei provvedimenti di cui all'art. 4, comma 2; f) evidenziare l'eventuale modifica del documento informatico dopo la sottoscrizione dello stesso; g) consentire di salvare il risultato dell'operazione di verifica su un documento informatico h) rendere evidente la circostanza di cui all'art. 19, comma 7.
3. L'Agenzia, ai sensi dell'art. 31 del Codice, accerta la conformità dei sistemi di verifica di cui al comma 1 alle norme del Codice e alle presenti regole tecniche.
4. L'Agenzia, al fine di fornire garanzie di attendibilità nelle operazioni di verifica e di rendere effettivamente interoperabili le firme elettroniche qualificate e le firme digitali, anche in base all'evoluzione delle normative europee ed all'evoluzione degli standard tecnici, può elaborare Linee Guida utili per la verifica della firma elettronica qualificata e della firma digitale apposte a documenti informatici cui i certificatori accreditati hanno l'obbligo di attenersi.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 15
Informazioni riguardanti i certificatori

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi del Codice forniscono all'Agenzia le seguenti informazioni e documenti a loro relativi: a) dati anagrafici ovvero denominazione o ragione sociale; b) residenza ovvero sede legale; c) sedi operative; d) rappresentante legale; e) certificati delle chiavi di certificazione; f) piano per la sicurezza di cui all'art. 35; g) manuale operativo di cui all'art. 40; h) relazione sulla struttura organizzativa; i) copia di una polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi.
2. L'Agenzia rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), e), g) al fine di rendere pubbliche le informazioni che individuano il certificatore qualificato. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.

Art. 16
Comunicazione tra certificatore e l'Agenzia

1. I certificatori che rilasciano al pubblico certificati qualificati comunicano all'Agenzia la casella di posta elettronica certificata da utilizzare per realizzare un sistema di comunicazione attraverso il quale scambiare le informazioni previste dal presente decreto.
2. L'Agenzia rende disponibile sul proprio sito internet l'indirizzo della propria casella di posta elettronica certificata.

Art. 17
Generazione e uso delle chiavi del certificatore

1. La generazione delle chiavi di certificazione avviene in modo conforme a quanto previsto dalle presenti regole tecniche.
2. Per ciascuna chiave di certificazione il certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.
3. I valori contenuti nei singoli campi del certificato delle chiavi di certificazione sono codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.
4. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma utilizzati per le chiavi di cui all'art. 5, comma 4, lettere b), c) e d), è effettuata secondo criteri non inferiori a quelli previsti: a) dal livello EAL 4+ della norma ISO/IEC 15408 in conformità ai profili di protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni; b) dal livello di certificazione e in conformità ai profili di protezione o traguardi di sicurezza giudicati adeguati dagli organismi di cui all'art. 11, comma 1, lettera b) della Direttiva europea 1999/93/EU.
5. La certificazione di sicurezza di cui al comma 4 può inoltre essere effettuata secondo i criteri previsti dal livello di valutazione E3 e robustezza HIGH dell'ITSEC, o superiori, con un traguardo di sicurezza giudicato adeguato dall'Agenzia nell'ambito dell'attività di cui agli articoli 29 e 31 del Codice.

Art. 18
Generazione dei certificati qualificati

1. Fermo restando quanto previsto dall'art. 32 del Codice, all'atto dell'emissione del certificato qualificato, il certificatore: a) accerta l'autenticità della richiesta; b) nel caso di chiavi generate dallo stesso certificatore, assicura la consegna al legittimo titolare ovvero, nel caso di chiavi non generate dallo stesso certificatore, verifica il possesso della chiave privata da parte del titolare e il corretto funzionamento della coppia di chiavi.
2. Il certificato qualificato è generato con un sistema conforme a quanto previsto dall'art. 33.
3. Il termine del periodo di validità del certificato qualificato precede di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità.
4. L'emissione dei certificati qualificati è registrata nel giornale di controllo specificando il riferimento temporale relativo alla registrazione.

Art. 19
Informazioni contenute nei certificati

1. Fatto salvo quanto previsto dall'art. 28 del Codice, i certificati qualificati contengono almeno le seguenti ulteriori informazioni: a) Codice identificativo del titolare presso il certificatore; b) tipologia della coppia di chiavi in base all'uso cui sono destinate.
2. Le informazioni personali contenute nel certificato qualificato ai sensi di quanto previsto nell'art. 28 del Codice sono utilizzabili unicamente per identificare il titolare della firma elettronica qualificata o della firma digitale, per verificare la firma del documento informatico, nonché per indicare eventuali qualifiche specifiche del titolare.
3. I valori contenuti nei singoli campi del certificato qualificato sono codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.
4. Le informazioni e le qualifiche di cui all'art. 28, comma 3, lettera a) del Codice, codificate secondo le modalità indicate dai provvedimenti di cui all'art. 4, comma 2, del presente decreto, sono inserite dal certificatore su richiesta del titolare: a) nel certificato qualificato senza l'indicazione dell'organizzazione di appartenenza. A tal fine, il titolare del certificato fornisce al certificatore una dichiarazione sostitutiva ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; b) ovvero, nel certificato di attributo o nel certificato qualificato con l'indicazione dell'organizzazione di appartenenza. A tal fine, il titolare del certificato richiede all'organizzazione di appartenenza una autorizzazione all'emissione del certificato, qualificato o di attributo che consegna al certificatore. L'organizzazione, che ha l'obbligo di fornire tale autorizzazione, assume l'impegno di richiedere al certificatore la revoca del certificato qualificato qualora venga a conoscenza della variazione delle informazioni o delle qualifiche contenute nello stesso. Il titolare, nel richiedere l'autorizzazione, ha l'obbligo di comunicare all'organizzazione di appartenenza il certificatore cui intende rivolgersi.
5. Il certificatore, salvo quanto disposto al comma 6, determina il periodo di validità dei certificati qualificati anche in funzione della robustezza crittografica delle chiavi impiegate.
6. L'Agenzia, ai sensi dell'art. 4, comma 2, determina il periodo massimo di validità del certificato qualificato in funzione degli algoritmi e delle caratteristiche delle chiavi.
7. Il certificato qualificato può contenere l'indicazione che l'utilizzo della chiave privata per la generazione della firma è subordinato alla verifica da parte del certificatore della validità del certificato qualificato e dell'eventuale certificato di attributo. All'attuazione del presente comma si provvede con le modalità stabilite dai provvedimenti di cui all'art. 4, comma 2.

Art. 20
Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'art. 36 del Codice, il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali.
2. Il certificatore conserva le richieste di revoca e sospensione per lo stesso periodo previsto all'art. 32, comma 3, lettera j) del Codice.

Art. 21
Codice di emergenza

1. Per ciascun certificato qualificato emesso il certificatore fornisce al titolare almeno un Codice riservato, da utilizzare per richiedere la sospensione del certificato nei casi di emergenza indicati nel manuale operativo di cui all'art. 40 e comunicati al titolare.
2. La richiesta di cui al comma 1 è successivamente confermata utilizzando una delle modalità previste dal certificatore.

3. Il certificatore adotta specifiche misure di sicurezza per assicurare la segretezza del Codice di emergenza.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 22
Revoca dei certificati qualificati relativi a chiavi di sottoscrizione

1. La revoca del certificato qualificato relativo a chiavi di sottoscrizione viene effettuata dal certificatore mediante l'inserimento del suo Codice identificativo in una delle liste di certificati revocati e sospesi (CRL).
2. Se la revoca avviene a causa della possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione dell'aggiornamento della lista di revoca.
3. La revoca dei certificati è annotata nel giornale di controllo con la specificazione della data e dell'ora della pubblicazione della CRL.
4. Il certificatore comunica tempestivamente l'avvenuta revoca al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta revocato.

Art. 23
Revoca di un certificato qualificato su iniziativa del certificatore

1. Salvo i casi di motivata urgenza, il certificatore che intende revocare un certificato qualificato ne dà preventiva comunicazione al titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

Art. 24
Revoca del certificato qualificato su richiesta del titolare

1. La richiesta di revoca è inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua decorrenza.
2. Le modalità di inoltro della richiesta sono indicate dal certificatore nel manuale operativo di cui all'art. 40.
3. Il certificatore verifica l'autenticità della richiesta e procede alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal comma 2.
4. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 25
Revoca su richiesta del terzo interessato

1. La richiesta di revoca da parte del terzo interessato da cui derivano i poteri di firma del titolare è inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua decorrenza.
2. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca di cui al comma 1 è inoltrata non appena il terzo venga a conoscenza della variazione di stato.
3. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 26
Sospensione dei certificati qualificati

1. La sospensione del certificato qualificato è effettuata dal certificatore mediante l'inserimento del suo Codice identificativo in una delle liste dei certificati revocati e sospesi (CRL).
2. Il certificatore comunica tempestivamente l'avvenuta sospensione al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.
3. Il certificatore indica nel manuale operativo, ai sensi dell'art. 40, comma 3, lettera l), la durata massima del periodo di sospensione e le azioni intraprese al termine dello stesso in assenza di diverse indicazioni da parte del soggetto che ha richiesto la sospensione.
4. In caso di revoca di un certificato qualificato sospeso, la data della stessa decorre dalla data di inizio del periodo di sospensione.
5. La sospensione e la cessazione della stessa sono annotate nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

6. La cessazione dello stato di sospensione del certificato, che sarà considerato come mai sospeso, è tempestivamente comunicata al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato ha cambiato stato.

Art. 27
Sospensione del certificato qualificato su iniziativa del certificatore

1. Salvo casi d'urgenza che il certificatore è tenuto a motivare contestualmente alla comunicazione conseguente alla sospensione di cui al comma 2, il certificatore che intende sospendere un certificato qualificato ne dà preventiva comunicazione al titolare e all'eventuale terzo interessato specificando i motivi della sospensione e la sua durata.
2. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore procede tempestivamente alla pubblicazione della sospensione.

Art. 28
Sospensione del certificato qualificato su richiesta del titolare

1. La richiesta di sospensione del certificato qualificato, con la specificazione della sua durata, è inoltrata al certificatore, secondo le modalità indicate nel manuale operativo approvato dall'Agenzia.
2. Il certificatore verifica l'autenticità della richiesta e procede alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal precedente comma 1.

Art. 29
Sospensione su richiesta del terzo interessato

1. La richiesta di sospensione del certificato qualificato da parte del terzo interessato, da cui derivano i poteri di firma del titolare, è inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua durata.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 30
Sostituzione delle chiavi di certificazione

1. La procedura di sostituzione delle chiavi, generate dal certificatore in conformità all'art. 17, assicura il rispetto del termine di cui all'art. 18, comma 3.
2. I certificati generati a seguito della sostituzione delle chiavi di certificazione sono inviati all'Agenzia.

Art. 31
Revoca dei certificati relativi a chiavi di certificazione

1. La revoca del certificato relativo ad una coppia di chiavi di certificazione è consentita solo nei seguenti casi: a) compromissione della chiave privata; b) malfunzionamento irrecuperabile del dispositivo sicuro per la generazione delle firme; c) cessazione dell'attività.
2. La revoca è comunicata entro ventiquattro ore all'Agenzia e resa nota a tutti i titolari di certificati qualificati sottoscritti con la chiave privata la cui corrispondente chiave pubblica è contenuta nel certificato revocato.
3. La revoca di certificati di cui al comma 1, pubblicati dall'Agenzia nell'elenco pubblico dei certificatori di cui all'art. 43, è resa nota attraverso il medesimo elenco.

Art. 32
Requisiti di sicurezza dei sistemi operativi

1. I sistemi operativi dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati qualificati e la gestione del registro dei certificati qualificati, devono essere stati oggetto di opportune personalizzazioni atte a innalzarne il livello di sicurezza (hardening) a cura del certificatore.
2. Ai sensi dell'art. 31 del Codice, l'Agenzia verifica l'idoneità delle personalizzazioni di cui al comma 1 e indica al certificatore eventuali azioni correttive.
3. Il comma 1 non si applica al sistema operativo dei dispositivi di firma.

Art. 33
Sistema di generazione dei certificati qualificati

1. La generazione dei certificati qualificati avviene su un sistema utilizzato esclusivamente per la generazione di certificati, situato in locali adeguatamente protetti.
2. L'entrata e l'uscita dai locali protetti è registrata sul giornale di controllo.
3. L'accesso ai sistemi di elaborazione è consentito, limitatamente alle funzioni assegnate, esclusivamente al personale autorizzato, identificato attraverso un'opportuna procedura di riconoscimento da parte del sistema al momento di apertura di ciascuna sessione.
4. L'inizio e la fine di ciascuna sessione sono registrati sul giornale di controllo.

Art. 34
Accesso del pubblico ai certificati

1. Le liste dei certificati revocati e sospesi sono rese pubbliche.
2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico nonché comunicati a terzi, al fine di verificare le firme digitali, esclusivamente nei casi consentiti dal titolare del certificato e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.
3. Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi li consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità delle firme elettroniche qualificate e digitali.
4. Chiunque ha diritto di conoscere se a proprio nome sia stato rilasciato un certificato qualificato. Le modalità per ottenere l'informazione di cui al primo periodo sono definite con il provvedimento di cui all'art. 42, comma 10, del presente decreto.

Art. 35
Piano per la sicurezza

1. Il certificatore definisce un piano per la sicurezza nel quale sono contenuti almeno i seguenti elementi: a) struttura generale, modalità operativa e struttura logistica; b) descrizione dell'infrastruttura di sicurezza fisica rilevante ai fini dell'attività di certificatore; c) allocazione dei servizi e degli uffici negli immobili rilevanti ai fini dell'attività di certificatore; d) descrizione delle funzioni del personale e sua allocazione ai fini dell'attività di certificatore; e) attribuzione delle responsabilità; f) algoritmi crittografici o altri sistemi utilizzati; g) descrizione delle procedure utilizzate nell'attività di certificatore; h) descrizione dei dispositivi installati; i) descrizione dei flussi di dati; l) procedura di gestione delle copie di sicurezza dei dati; m) procedura di continuità operativa del servizio di pubblicazione delle liste di revoca e sospensione; n) analisi dei rischi; o) descrizione delle contromisure; p) descrizione delle verifiche e delle ispezioni; q) descrizione delle misure adottate ai sensi degli articoli 32, comma 1, e 47, comma 2; r) procedura di gestione dei disastri; s) descrizione della procedura di cui all'art. 8, comma 3, ponendo in rilievo le modalità di conservazione e protezione dei supporti contenenti le chiavi esportate; t) misure di sicurezza per la protezione dei dispositivi di firma remota, ivi comprese le modalità di custodia; u) limitatamente a quanto previsto all'art. 11, comma 3, modalità con cui è assicurato il controllo esclusivo delle chiavi private custodite sui dispositivi di firma remota; v) le misure procedurali e tecniche applicate per la distruzione dei dispositivi HSM e delle chiavi che contengono in caso di guasto del dispositivo HSM che non consente l'applicazione delle funzionalità di sicurezza certificate implementate dai dispositivi medesimi.
2. Quanto previsto dalle lettere t) e u) del comma 1 può essere oggetto di dichiarazioni separate da parte del certificatore, ad integrazione del piano per la sicurezza.
3. L'Agenzia, a seguito dell'analisi di quanto dichiarato alle lettere t) e u) del comma 1, può imporre al certificatore di inserire nei certificati qualificati afferenti la firma remota limitazioni d'uso e di valore.
4. Il piano per la sicurezza, sottoscritto dal legale rappresentante del certificatore, ovvero dal responsabile della sicurezza da questo delegato, è consegnato all'Agenzia in busta sigillata o cifrato, al fine di garantirne la riservatezza, in base alle indicazioni fornite dall'Agenzia.
5. Il piano per la sicurezza si attiene alle misure di sicurezza previste dal Titolo V della Parte I del decreto legislativo 30 giugno 2003, n. 196.

Art. 36
Giornale di controllo

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il certificatore, allorché si verificano le condizioni previste dal presente decreto.

2. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.
3. A ciascuna registrazione è apposto un riferimento temporale.
4. Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.
5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo sono conservate per un periodo pari a venti anni, salvo quanto previsto dall'art. 11 del decreto legislativo n. 196 del 2003.

Art. 37
Sistema di qualità del certificatore

1. Entro un anno dall'avvio dell'attività di certificazione, il certificatore dichiara la conformità del proprio sistema di qualità alle norme ISO 9000, successive modifiche o a norme equivalenti.
2. Il manuale della qualità è depositato presso l'Agenzia e reso disponibile presso il certificatore.

Art. 38
Organizzazione del personale addetto al servizio di certificazione

1. Fatto salvo quanto previsto al comma 3, l'organizzazione del certificatore prevede almeno le seguenti figure professionali: a) responsabile della sicurezza; b) responsabile del servizio di certificazione e validazione temporale; c) responsabile della conduzione tecnica dei sistemi; d) responsabile dei servizi tecnici e logistici; e) responsabile delle verifiche e delle ispezioni (auditing).
2. Non è possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1.
3. Ferma restando la responsabilità del certificatore, l'organizzazione dello stesso può prevedere che alcune delle suddette responsabilità siano affidate ad altre organizzazioni. In questo caso il responsabile della sicurezza o altro dipendente appositamente designato gestisce i rapporti con tali figure professionali.
4. In nessun caso quanto previsto al comma 3 si applica per le figure professionali di cui al comma 1, lettere a) ed e).

Art. 39
Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'art. 38 deve aver maturato una esperienza professionale nelle tecnologie informatiche e delle telecomunicazioni almeno quinquennale.
2. Per ogni aggiornamento apportato al sistema di certificazione è previsto un apposito addestramento.

Art. 40
Manuale operativo

1. Il manuale operativo definisce le procedure applicate dal certificatore che rilascia certificati qualificati nello svolgimento della sua attività.
2. Il manuale operativo è depositato presso l'Agenzia e pubblicato a cura del certificatore in modo da essere consultabile per via telematica.
3. Il manuale contiene almeno le seguenti informazioni: a) dati identificativi del certificatore; b) dati identificativi della versione del manuale operativo; c) responsabile del manuale operativo; d) definizione degli obblighi del certificatore, del titolare e dei richiedenti le informazioni per la verifica delle firme; e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi; f) indirizzo del sito web del certificatore ove sono pubblicate le tariffe; g) modalità di identificazione e registrazione degli utenti; h) modalità di generazione delle chiavi per la creazione e la verifica della firma; i) modalità di emissione dei certificati; l) modalità di inoltro delle richieste e della gestione di sospensione e revoca dei certificati; m) modalità di sostituzione delle chiavi; n) modalità di gestione del registro dei certificati; o) modalità di accesso al registro dei certificati; p) modalità per l'apposizione e la definizione del riferimento temporale; q) modalità di protezione dei dati personali; r) modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 14, comma 1; s) modalità operative per la generazione della firma elettronica qualificata e della firma digitale.

Art. 41
Riferimenti temporali opponibili ai terzi

1. I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del Codice.

2. I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del Codice.
3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo.
4. Costituiscono inoltre validazione temporale: a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272; b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione; c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del Codice; d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il decreto del Presidente della Repubblica 12 gennaio 2007, n. 18.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Titolo III
CERTIFICATORI ACCREDITATI

Art. 42

Obblighi per i certificatori accreditati

1. Il certificatore accreditato genera un certificato per ciascuna delle chiavi di firma utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori, lo pubblica nel proprio registro dei certificati e lo rende accessibile per via telematica al fine di verificare la validità delle chiavi utilizzate dall'Agenzia. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.
2. Il certificatore accreditato garantisce l'interoperabilità del prodotto di verifica di cui all'art. 14 del presente decreto con i documenti informatici sottoscritti mediante firme elettroniche qualificate e digitali ad opera dell'Agenzia, nell'ambito delle attività di cui all'art. 31 del Codice.
3. Il certificatore accreditato mantiene copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione di cui all'art. 43, comma 1, lettera e) del presente decreto, che rende accessibile per via telematica per la specifica finalità della verifica delle firme elettroniche qualificate e digitali.
4. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 29, comma 1 del Codice, svolgono la propria attività in conformità con quanto previsto dai provvedimenti emanati dall'Agenzia ai sensi dell'art. 4, comma 2.
Fino all'emanazione di tali provvedimenti continua ad applicarsi la deliberazione CNIPA 21 maggio 2009, n. 45, recante regole per il riconoscimento e la verifica del documento informatico e successive modificazioni.
5. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 29, comma 1, del Codice assicurano la valorizzazione dell'estensione qcStatements id-etsi-qcs-QcSSCD esclusivamente nei certificati qualificati la cui corrispondente chiave privata sia custodita nei dispositivi di cui all'art. 12.
6. I sistemi di generazione e verifica delle firme elettroniche qualificate e delle firme digitali, forniti o indicati dal certificatore accreditato ai sensi degli articoli 11, comma 8 e 14, comma 1, non devono consentire a quest'ultimo di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.
7. Al fine dell'attività di cui all'art. 31 del Codice, il certificatore deve consegnare all'Agenzia un esemplare dei dispositivi di firma elettronica qualificata e di firma digitale forniti ai titolari. Il primo periodo non si applica in relazione ai dispositivi di firma HSM.
8. Al fine dell'attività di cui all'art. 31 del Codice, il certificatore deve consegnare all'Agenzia copia delle applicazioni di generazione e verifica delle firme elettroniche qualificate o delle firme digitali fornite ai titolari per uso personale.
9. Al fine del mantenimento dell'accreditamento di cui all'art. 29 del Codice, il certificatore è obbligato a partecipare alle sessioni di test di interoperabilità indicate dall'Agenzia.
10. I certificatori rendono disponibile all'Agenzia un servizio che consenta, ai fini dell'art. 34, comma 4, di conoscere se, per un determinato codice fiscale, sia stato emesso un certificato qualificato e, in caso affermativo, la sua scadenza. L'Agenzia, sentite le associazioni di categoria e il Garante per la protezione

dei dati personali, indica in un proprio provvedimento le caratteristiche del servizio, le modalità e i vincoli per la sua fruizione.

Art. 43
Elenco pubblico dei certificatori accreditati

1. L'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia ai sensi dell'art. 29, comma 6, del Codice, e del decreto legislativo 1 dicembre 2009, n. 177, contiene per ogni certificatore accreditato almeno le seguenti informazioni: a) denominazione; b) sede legale; c) indirizzo della sede legale; d) indirizzi internet ove il certificatore pubblica in lingua italiana e lingua inglese informazioni inerenti all'attività svolta;
e) lista dei certificati delle chiavi di certificazione; f) indirizzo di posta elettronica; g) data di accreditamento volontario; h) eventuale data di cessazione; i) eventuale certificatore sostitutivo.
2. L'elenco pubblico è sottoscritto e reso disponibile per via telematica dall'Agenzia al fine di verificare le firme elettroniche qualificate e digitali e diffondere i dati dei certificatori accreditati. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge. L'Agenzia stabilisce il formato dell'elenco pubblico attraverso propria deliberazione.
3. L'elenco pubblico è sottoscritto elettronicamente dal Presidente dell'Agenzia o dai soggetti da lui designati.
4. L'Agenzia pubblica sul proprio sito istituzionale i manuali operativi di cui all'art. 40, sottoscritti ai sensi del comma 3.
5. Nella Gazzetta Ufficiale della Repubblica italiana è dato avviso: a) dell'indicazione dei soggetti preposti alla sottoscrizione dell'elenco pubblico di cui al comma 3; b) del valore dei codici identificativi del certificato relativo alle chiavi utilizzate per la sottoscrizione dell'elenco pubblico, generati attraverso gli algoritmi di cui all'art. 4; c) con almeno sessanta giorni di preavviso rispetto alla scadenza del certificato, della sostituzione delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico; d) della revoca dei certificati utilizzati per la sottoscrizione dell'elenco pubblico sopravvenuta per ragioni di sicurezza.

Art. 44
Rappresentazione del documento informatico

1. Il certificatore indica nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per evitare le conseguenze previste dall'art. 4, comma 3.

Art. 45
Limitazioni d'uso

1. Il certificatore, su richiesta del titolare, del terzo interessato o dell'Agenzia, è tenuto a inserire nel certificato qualificato eventuali limitazioni d'uso.
2. La modalità di rappresentazione dei limiti d'uso e di valore di cui all'art. 28, comma 3, del Codice è definita dall'Agenzia con uno dei provvedimenti di cui all'art. 4, comma 2.
3. Il certificatore è tenuto ad indicare, in lingua italiana e lingua inglese, la limitazione d'uso dei certificati utilizzati per la verifica delle firme di cui all'art. 35, comma 3, del Codice.

Art. 46
Verifica delle marche temporali

1. I certificatori accreditati forniscono ovvero indicano almeno un sistema, conforme al successivo comma 2, che consenta di effettuare la verifica delle marche temporali.
2. L'Agenzia con i provvedimenti di cui all'art. 4, comma 2, stabilisce le regole di interoperabilità per la verifica della marca temporale, anche associata al documento informatico cui si riferisce.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Titolo IV
REGOLE PER LA VALIDAZIONE TEMPORALE MEDIANTE MARCA TEMPORALE

Art. 47
Validazione temporale con marca temporale

1. Una evidenza informatica è sottoposta a validazione temporale mediante generazione e applicazione di una marca temporale alla relativa impronta.

2. Le marche temporali sono generate da un apposito sistema di validazione temporale, sottoposto ad opportune personalizzazioni atte a innalzarne il livello di sicurezza, in grado di: a) garantire l'esattezza del riferimento temporale conformemente a quanto richiesto dal presente decreto; b) generare la struttura dei dati temporali secondo quanto specificato negli articoli 48 e 51; c) sottoscrivere elettronicamente la struttura di dati di cui alla lettera b).
3. L'evidenza informatica da sottoporre a validazione temporale può essere costituita da un insieme di impronte.

Art. 48
Informazioni contenute nella marca temporale

1. Una marca temporale contiene almeno le seguenti informazioni: a) identificativo dell'emittente; b) numero di serie della marca temporale; c) algoritmo di sottoscrizione della marca temporale; d) certificato relativo alla chiave utilizzata per la verifica della marca temporale; e) riferimento temporale della generazione della marca temporale; f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale; g) valore dell'impronta dell'evidenza informatica.
2. La marca temporale può inoltre contenere un Codice identificativo dell'oggetto a cui appartiene l'impronta di cui al comma 1, lettera g).

Art. 49
Chiavi di marcatura temporale

1. Dal certificato relativo alla coppia di chiavi utilizzate per la validazione temporale deve essere possibile individuare il sistema di validazione temporale.
2. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite ed un nuovo certificato è emesso, in relazione alla robustezza delle chiavi crittografiche utilizzate, dopo non più di tre mesi di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il certificato corrispondente alla chiave precedentemente in uso. Detto periodo è indicato nel manuale operativo e, previa valutazione, ritenuto congruente dall'Agenzia.
3. Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale sono utilizzate chiavi di certificazione appositamente generate.
4. Le chiavi di certificazione e di marcatura temporale possono essere generate esclusivamente in presenza dei responsabili dei rispettivi servizi.

Art. 50
Gestione dei certificati e delle chiavi

1. Alle chiavi di certificazione utilizzate, ai sensi dell'art. 49, comma 3, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.
2. I certificati relativi ad una coppia di chiavi di marcatura temporale, oltre ad essere conformi a quanto stabilito ai sensi dell'art. 4, comma 2, contengono l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 51
Precisione dei sistemi di validazione temporale

1. Il riferimento temporale assegnato ad una marca temporale coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.
2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC).

Art. 52
Sicurezza dei sistemi di validazione temporale

1. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento del sistema di validazione temporale in modo da renderlo incompatibile con i requisiti previsti dal presente decreto, ed in particolare con quello di cui all'art. 51, comma 1, è annotato sul giornale di controllo e causa il blocco del sistema medesimo.

2. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.
3. I sistemi operativi dei sistemi di elaborazione utilizzati nelle attività di validazione temporale devono essere stati oggetto di opportune personalizzazioni atte a innalzarne il livello di sicurezza (hardening).
4. Ai sensi dell'art. 31 del Codice, l'Agenzia verifica l'idoneità delle personalizzazioni, di cui al comma 3, e indica al certificatore eventuali azioni correttive.

Art. 53
Registrazione delle marche generate

1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.
2. La marca temporale è valida per il periodo di conservazione, stabilito o concordato con il certificatore, di cui al comma 1.

Art. 54
Richiesta di marca temporale

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'invio della richiesta di marca temporale.
2. La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale.
3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'art. 4, comma 2.
4. La generazione delle marche temporali garantisce un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

Titolo V
FIRMA ELETTRONICA AVANZATA

Art. 55
Disposizioni generali

1. La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.
2. I soggetti che erogano o realizzano soluzioni di firma elettronica avanzata si distinguono in: a) coloro che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti di cui alla lettera b); b) coloro che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore dei soggetti di cui alla lettera a).

Art. 56
Caratteristiche delle soluzioni di firma elettronica avanzata

1. Le soluzioni di firma elettronica avanzata garantiscono: a) l'identificazione del firmatario del documento; b) la connessione univoca della firma al firmatario; c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima; d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma; e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto; f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a); g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati; h) la connessione univoca della firma al documento sottoscritto.
2. La firma elettronica avanzata generata in violazione di quanto disposto da una o più disposizioni di cui alle lettere a), b), c), d), e), g), h) del comma 1, non soddisfa i requisiti previsti dagli articoli 20, comma 1-bis, e 21, comma 2, del Codice.

Art. 57
Obblighi a carico dei soggetti che erogano soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a) devono: a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso

del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente; b) conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità; c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo; d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet; e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1; f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto; g) pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet; h) assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.
2. Al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti di cui all'art. 55, comma 2, lettera a), si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila.
3. Le modalità scelte per ottemperare a quanto disposto al comma 2 devono essere rese note ai soggetti interessati, pubblicandole anche sul proprio sito internet.
4. Il comma 2 del presente articolo non si applica alle persone giuridiche pubbliche che erogano soluzioni di firma elettronica avanzata per conto di pubbliche amministrazioni.
5. Nell'ambito delle pubbliche amministrazioni e in quello sanitario limitatamente alla categoria di utenti rappresentata dai cittadini fruitori di prestazioni sanitarie, la dichiarazione di accettazione delle condizioni del servizio prevista al comma 1, lettera a) può essere fornita oralmente dall'utente al funzionario pubblico o all'esercente la professione sanitaria, il quale la raccoglie in un documento informatico che sottoscrive con firma elettronica qualificata o firma digitale.
6. I commi 1 e 2 non si applicano alle soluzioni di cui all'art. 61, commi 1 e 2, alle quali si applicano le norme vigenti in materia.

Art. 58

Soggetti che realizzano soluzioni di firma elettronica avanzata a favore di terzi

1. I soggetti di cui all'art. 55, comma 2, lettera b) che offrono una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, devono essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative, alla normaISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia.
2. I soggetti di cui all'art. 55, comma 2, lettera b) che offrono soluzioni di firma elettronica avanzata alle pubbliche amministrazioni, ovvero le società che li controllano, devono essere in possesso della certificazione di conformità del proprio sistema di qualità alla norma ISO 9001 e successive modifiche o a norme equivalenti.
3. I commi 1 e 2 non si applicano alle persone giuridiche private partecipate, in tutto o in parte, dalla pubblica amministrazione qualora realizzino per la stessa soluzioni di firma elettronica avanzata.
4. I commi 1 e 2 del presente articolo non si applicano alle persone giuridiche pubbliche che rendono disponibili soluzioni di firma elettronica avanzata a pubbliche amministrazioni.
5. I soggetti di cui all'art. 55, comma 2, lettera b), al fine di dare evidenza del grado di conformità della soluzione di firma elettronica avanzata a quanto previsto dalle presenti regole tecniche, possono far certificare la propria soluzione secondo la norma ISO/IEC 15408, livello EAL 1 o superiore, da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia.

Art. 59

Affidabilità delle soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a), al fine di dare evidenza del grado di conformità alla norma ISO/IEC 27001 del proprio sistema di gestione per la sicurezza delle informazioni a supporto della soluzione di firma elettronica avanzata proposta, possono richiederne la certificazione ad una terza parte indipendente autorizzata allo scopo secondo le norme vigenti in materia.
2. I soggetti di cui all'art. 55, comma 2, lettera a), al fine di dare evidenza del grado di conformità della soluzione di firma elettronica avanzata a quanto previsto dalle presenti regole tecniche, su base volontaria, possono far certificare la propria soluzione secondo la norma ISO/IEC 15408, livello EAL 1 o superiore da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia.

Art. 60
Limiti d'uso della firma elettronica avanzata

1. La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a).

Art. 61
Soluzioni di firma elettronica avanzata

1. L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del Codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005 recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata» sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche.
2. L'utilizzo della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi, del documento d'identità dei pubblici dipendenti (Mod. ATe), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del codice.
3. I formati della firma di cui al comma 2 sono gli stessi previsti ai sensi dell'art. 4, comma 2.
4. Le applicazioni di verifica della firma generata ai sensi del comma 2 devono accertare che il certificato digitale utilizzato nel processo di verifica corrisponda ad uno degli strumenti di cui al medesimo comma.
5. I certificatori accreditati che emettono certificati per gli strumenti di cui al comma 2 rendono disponibili strumenti di verifica della firma.
6. Fermo restando quanto disposto dall'art. 55, comma 1, al fine di favorire la realizzazione di soluzioni di firma elettronica avanzata, l'Agenzia elabora Linee guida sulla base delle quali realizzare soluzioni di firma elettronica avanzata conformi alle presenti regole tecniche.

Titolo VI
DISPOSIZIONI FINALI

Art. 62
Valore delle firme elettroniche qualificate e digitali nel tempo

1. Le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Art. 63
Disposizioni finali e transitorie

1. Il presente decreto sostituisce il decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante «Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.», pubblicato nella Gazzetta Ufficiale 6 giugno 2009, n. 129.
2. I certificatori accreditati ai sensi dell'art. 29 del Codice aggiornano la documentazione prevista per lo svolgimento di tale attività entro centoventi giorni dall'entrata in vigore del presente decreto.
3. Eventuali difformità nella generazione delle firme digitali, delle firme elettroniche qualificate, dei certificati qualificati e delle marche temporali, alle regole tecnologiche di cui al Titolo II, che non ne mettano a rischio la sicurezza, non ne inficiano la validità. L'Agenzia valuta tali difformità e rende note le proprie decisioni sul proprio sito internet.
Il presente decreto sarà inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

D.P.C.M. 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (14A02098) ***(GU n.59 del 12-3-2014 - Suppl. Ordinario n. 20)***

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante «Codice dell'amministrazione digitale» e, in particolare, gli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice;

Visto il decreto del Presidente del Consiglio dei ministri 31 ottobre 2000, e successive modificazioni, recante «Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428»;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;

Visto il decreto «Codice in materia di protezione dei dati personali»;

Visto il decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni, recante «Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137»;

Visto il decreto legislativo 1° dicembre 2009, n. 177, recante «Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'art. 24 della legge 18 giugno 2009, n. 69»;

Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese», con cui è stato soppresso DigitPA e le funzioni sono state attribuite all'Agenzia per l'Italia digitale;

Vista la deliberazione CNIPA n. 11/2004 del 19 febbraio 2004, recante «Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445»;

Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2013, recante «Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71», pubblicato nella Gazzetta Ufficiale 21 maggio 2013, n. 117;

Visto il decreto del Presidente della Repubblica in data 28 aprile 2013, con il quale l'onorevole avvocato Gianpiero D'Alia è stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei ministri del 28 aprile 2013, con il quale al predetto Ministro senza portafoglio è stato conferito l'incarico per la pubblica amministrazione e la semplificazione;

Visto il decreto del Presidente del Consiglio dei ministri 27 maggio 2013 recante delega di funzioni del Presidente del Consiglio dei ministri al Ministro senza portafoglio, onorevole avvocato Gianpiero D'Alia, in materia di pubblica amministrazione e semplificazione;

Acquisito il parere tecnico dell'Agenzia per l'Italia digitale;

Sentito il Garante per la protezione dei dati personali;

Sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 nella seduta del 24 luglio 2013; Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con decreto legislativo 23 novembre 2000, n. 427;

di concerto con il Ministro dei beni e delle attività culturali e del turismo per la parte relativa alla conservazione dei documenti informatici delle pubbliche amministrazioni;

Decreta:

Art. 1

Definizioni

1. Ai fini del presente decreto si applicano le definizioni del glossario di cui all'allegato 1 che ne costituisce parte integrante.

2. Le specifiche tecniche relative alle regole tecniche di cui al presente decreto sono indicate nell'allegato n. 2 relativo ai formati, nell'allegato n. 3 relativo agli standard tecnici di riferimento per la formazione, la gestione e la conservazione dei documenti informatici, nell'allegato n. 4 relativo alle specifiche tecniche del pacchetto di archiviazione e nell'allegato n. 5 relativo ai metadati. Le specifiche tecniche di cui al presente comma sono aggiornate con delibera dell'Agenzia per l'Italia digitale, previo parere del Garante per la protezione dei dati personali, e pubblicate sul proprio sito istituzionale.

Art. 2
Ambito di applicazione

1. Il presente decreto, adottato ai sensi dell'art. 71 del Codice, stabilisce le regole tecniche previste dall'art. 20, commi 3 e 5-bis, dall'art. 23-ter, comma 4, dall'art. 43, commi 1 e 3, dall'art. 44 e dall'art. 44-bis del Codice.

2. Le disposizioni del presente decreto si applicano ai soggetti di cui all'art. 2, commi 2 e 3, del Codice, nonché ai soggetti esterni a cui è eventualmente affidata la gestione o la conservazione dei documenti informatici.

3. Ai sensi dell'art. 2, comma 5, del Codice, le presenti regole tecniche si applicano nel rispetto della disciplina rilevante in materia di tutela dei dati personali e, in particolare, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Art. 3
Sistema di conservazione

1. In attuazione di quanto previsto dall'art. 44, comma 1, del Codice, il sistema di conservazione assicura, dalla presa in carico dal produttore di cui all'art. 6 fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati di cui all'allegato 5 al presente decreto;

b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati di cui all'allegato 5 al presente decreto, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

2. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

3. Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

4. Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono riportati negli allegati 2 e 3 al presente decreto.

Art. 4
Oggetti della conservazione

1. Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;

b) pacchetti di archiviazione;

c) pacchetti di distribuzione.

2. Ai fini dell'interoperabilità tra i sistemi di conservazione, i soggetti che svolgono attività di conservazione dei documenti informatici adottano le specifiche della struttura dati contenute nell'allegato 4, almeno per la gestione dei pacchetti di archiviazione.

Art. 5
Modelli organizzativi della conservazione

1. Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente.

2. Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta:

a) all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare;

b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

3. Le pubbliche amministrazioni realizzano i processi di conservazione all'interno della propria struttura organizzativa o affidandoli a conservatori accreditati, pubblici o privati, di cui all'art. 44-bis, comma 1, del Codice, fatte salve le competenze del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.

Art. 6
Ruoli e responsabilità

1. Nel sistema di conservazione si individuano almeno i seguenti ruoli:

a) produttore;

b) utente;

c) responsabile della conservazione.

2. I ruoli di produttore e utente sono svolti da persone fisiche o giuridiche interne o esterne al sistema di conservazione, secondo i modelli organizzativi definiti all'art. 5.

3. Il responsabile della gestione documentale o il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi assicura la trasmissione del contenuto del pacchetto di versamento, da lui prodotto, al sistema di conservazione secondo le modalità operative definite nel manuale di conservazione.

4. L'utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste all'art. 10.

5. Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato ai sensi dell'art. 5.

6. Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato.

7. La conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all'art. 5, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.

8. Il soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali.

9. Resta ferma la competenza del Ministero dei beni e delle attività culturali e del turismo in materia di tutela dei sistemi di conservazione degli archivi pubblici o degli archivi privati che rivestono interesse storico particolarmente importante.

Art. 7
Responsabile della conservazione

1. Il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice, oltre che con il responsabile della gestione documentale ovvero con il coordinatore della gestione documentale ove nominato, per quanto attiene alle pubbliche amministrazioni. In particolare il responsabile della conservazione:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma
digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove

necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

2. Ai sensi dell'art. 44, comma 1-ter, del Codice, il responsabile della conservazione può chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, comma 1, del Codice, distinti dai conservatori o dai conservatori accreditati. Le pubbliche amministrazioni possono chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati, a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-bis, comma 1, del Codice, distinti dai conservatori accreditati

3. Nelle pubbliche amministrazioni, il ruolo del responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato.

4. Nelle pubbliche amministrazioni, il ruolo di responsabile della conservazione può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Art. 8
Manuale di conservazione

1. Il manuale di conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

2. Il manuale di conservazione è un documento informatico che riporta, almeno:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;

b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;

c) la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;

e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;

f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;

h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;

i) la descrizione delle procedure per la produzione di duplicati o copie;

j) i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;

k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;

l) le normative in vigore nei luoghi dove sono conservati i documenti.

Art. 9
Processo di conservazione

1. Il processo di conservazione prevede:

a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;

b) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato all'art. 11;

c) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;

d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente
un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;

e) l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 e secondo le modalità riportate nel manuale della conservazione;

g) la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

h) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;

i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento
informatico;

j) la produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;

k) lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore;

l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

2. Fatto salvo quanto previsto dal decreto legislativo 22 gennaio 2004, n. 42, in ordine alla tutela, da parte del Ministero dei beni e delle attività culturali e del turismo, sugli archivi e sui singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico, i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle stabilite dal presente decreto.

Art. 10
Modalità di esibizione

1. Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva secondo le modalità descritte nel manuale di conservazione.

Art. 11
Formati degli oggetti destinati alla conservazione

1. I documenti informatici destinati alla conservazione utilizzano i formati previsti nell'allegato 2 al presente decreto.

Art. 12
Sicurezza del sistema di conservazione

1. Nelle pubbliche amministrazioni, il responsabile della conservazione, di concerto con il responsabile della sicurezza e, nel caso delle pubbliche amministrazioni centrali, anche con il responsabile dell'ufficio

di cui all'art. 17 del Codice, provvede a predisporre, nell'ambito del piano generale della sicurezza, il piano della sicurezza del sistema di conservazione, nel rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del medesimo decreto, nonché in coerenza con quanto previsto dagli articoli 50-bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. Le suddette misure sono descritte nel manuale di conservazione di cui all'art. 8.

2. I soggetti privati appartenenti ad organizzazioni che già adottano particolari regole di settore per la sicurezza dei sistemi informativi adeguano il sistema di conservazione a tali regole. Gli altri soggetti possono adottare quale modello di riferimento le regole di sicurezza indicate dagli articoli 50-bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. I sistemi di conservazione rispettano le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Art. 13
Accreditamento

1. L'Agenzia per l'Italia digitale definisce, con propri provvedimenti, le modalità per l'accreditamento e la vigilanza sui soggetti di cui all'art. 44-bis del Codice i quali adottano le presenti regole tecniche di cui al presente decreto per la gestione e la documentazione del sistema di conservazione, nonché per l'espletamento del processo di conservazione.

Art. 14
Disposizioni finali

1. Il presente decreto entra in vigore il trentesimo giorno successivo alla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

2. I sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del presente decreto secondo un piano dettagliato allegato al manuale di conservazione. Fino al completamento di tale processo per tali sistemi possono essere applicate le previgenti regole tecniche. Decorso tale termine si applicano in ogni caso le regole tecniche di cui al presente decreto.

3. Fino al completamento del processo di cui al comma 2, restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti.

4. La deliberazione CNIPA n. 11/2004 cessa di avere efficacia nei termini previsti dai comma 2 e 3. Il presente decreto è inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Decreto del Ministro della Giustizia 10 marzo 2014, n. 55 - Regolamento recante la determinazione dei parametri per la liquidazione dei compensi per la professione forense, ai sensi dell'articolo 13, comma 6, della legge 31 dicembre 2012, n. 247 (ESTRATTO).

Art. 4

Parametri generali per la determinazione dei compensi in sede giudiziale

1. Ai fini della liquidazione del compenso si tiene conto delle caratteristiche, dell'urgenza e del pregio dell'attività prestata, dell'importanza, della natura, della difficoltà e del valore dell'affare, delle condizioni soggettive del cliente, dei risultati conseguiti, del numero e della complessità delle questioni giuridiche e di fatto trattate. In ordine alla difficoltà dell'affare si tiene particolare conto dei contrasti giurisprudenziali, e della quantità e del contenuto della corrispondenza che risulta essere stato necessario intrattenere con il cliente e con altri soggetti. Il giudice tiene conto dei valori medi di cui alle tabelle allegate, che, in applicazione dei parametri generali, possono essere aumentati di regola sino all'80 per cento, ovvero possono essere diminuiti in ogni caso non oltre il 50 per cento. Per la fase istruttoria l'aumento è di regola fino al 100 per cento e la ((diminuzione in ogni caso non oltre il 70 per cento.

1-bis. Il compenso determinato tenuto conto dei parametri generali di cui al comma 1 è di regola ulteriormente aumentato del 30 per cento quando gli atti depositati con modalità telematiche sono redatti con tecniche informatiche idonee ad agevolarne la consultazione o la fruizione e, in particolare, quando esse consentono la ricerca testuale all'interno dell'atto e dei documenti allegati, nonché la navigazione all'interno dell'atto[71].

2. (Omissis).

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

[71] Comma aggiunto dal DM 8 marzo 2018 n. 37.

Decreto Legge 24 giugno 2014, n. 90, coordinato con la legge di conversione 11 agosto 2014, n. 114 Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari (ESTRATTO).

(ritorna all'indice cronologico)

(torna all'indice per argomenti)

Art. 44.
Obbligatorietà del deposito telematico degli atti processuali.

1. Le disposizioni di cui ai commi 1, 2 e 3 dell'art. 16-*bis* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, si applicano esclusivamente ai procedimenti iniziati innanzi al tribunale ordinario dal 30 giugno 2014. Per i procedimenti di cui al periodo precedente iniziati prima del 30 giugno 2014, le predette disposizioni si applicano a decorrere dal 31 dicembre 2014; fino a quest'ultima data, nei casi previsti dai commi 1, 2 e 3 dell'art. 16 –*bis* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, gli atti processuali ed i documenti possono essere depositati con modalità telematiche e in tal caso il deposito si perfeziona esclusivamente con tali modalità.
2. All'art. 16-*bis* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:
(omissis).

Art. 45.
Modifiche al codice di procedura civile in materia di contenuto e di sottoscrizione del processo verbale e di comunicazione della sentenza.

1. Al codice di procedura civile sono apportate le seguenti modificazioni:
a) all'art. 126, il secondo comma è sostituito dal seguente:
«Il processo verbale è sottoscritto dal cancelliere. Se vi sono altri intervenuti, il cancelliere, quando la legge non dispone altrimenti, dà loro lettura del processo verbale.»;
b) all'art. 133, secondo comma, le parole: «il dispositivo» sono sostituite dalle seguenti: «il testo integrale della sentenza» ed è aggiunto, in fine, il seguente periodo: «La comunicazione non è idonea a far decorrere i termini per le impugnazioni di cui all'art. 325» ;
c) all'art. 207, secondo comma, le parole: «che le sottoscrive» sono soppresse.
1-bis . Alle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie, di cui al regio decreto 18 dicembre 1941, n. 1368, sono apportate le seguenti modificazioni:
a) all'art. 111, secondo comma, è aggiunto, in fine, il seguente periodo: «Quando le comparse sono depositate con modalità telematiche, il presente comma non si applica»;
b) all'art. 137, primo comma, è aggiunto, in fine, il seguente periodo: «Quando il ricorso o il controricorso sono depositati con modalità telematiche, il presente comma non si applica».

Art. 45-bis.
Disposizioni in materia di contenuto degli atti di parte e di comunicazioni e notificazioni con modalità telematiche.

1. All'art. 125, primo comma, del codice di procedura civile, il secondo periodo è sostituito dal seguente: «Il difensore deve altresì indicare il proprio numero di fax».
2. Al decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:
a) all'art. 16-ter :
1) al comma 1, le parole: «dall'art. 16 del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2» sono sostituite dalle seguenti: «dall'art. 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni,
dalla legge 28 gennaio 2009, n. 2»;
2) dopo il comma 1, è aggiunto il seguente:
«1-bis. Le disposizioni del comma 1 si applicano anche alla giustizia amministrativa»;
b) dopo l'art. 16-sexies è inserito il seguente:
«art. 16-septies…(omissis)».

3. All’art. 136 del codice del processo amministrativo, di cui all’allegato 1 al decreto legislativo 2 luglio 2010, n. 104, e successive modificazioni, il comma 1 è sostituito dal seguente:
(omissis)
4. All’art. 13, comma 3-bis , del testo unico delle disposizioni legislative e regolamentari in materia di spese di giustizia, di cui al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni, le parole:
«Ove il difensore non indichi il proprio indirizzo di posta elettronica certificata e il proprio numero di fax ai sensi degli articoli 125, primo comma, del codice di procedura civile» sono sostituite dalle seguenti: «Ove il difensore non indichi il proprio numero di fax ai sensi dell’art. 125, primo comma, del codice di procedura civile».

Art. 46.
Modifiche alla legge 21 gennaio 1994, n. 53.

1. Alla legge 21 gennaio 1994, n. 53, sono apportate le seguenti modificazioni:
(omissis)[72]
2. All’art. 16-*quater* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, dopo il comma 3, è aggiunto, in fine, il seguente: «3-*bis*. Le disposizioni dei commi 2 e 3 non si applicano alla giustizia amministrativa.».

Art. 48.
Vendita delle cose mobili pignorate con modalità telematiche.

1. All’art. 530 del codice di procedura civile, il sesto comma è sostituito dal seguente:
«Il giudice dell’esecuzione stabilisce che il versamento della cauzione, la presentazione delle offerte, lo svolgimento della gara tra gli offerenti, ai sensi dell’art. 532, nonché il pagamento del prezzo, siano effettuati con modalità telematiche, salvo che le stesse siano pregiudizievoli per gli interessi dei creditori o per il sollecito svolgimento della procedura.».
2. Le disposizioni del comma 1 si applicano alle vendite disposte a decorrere dal trentesimo giorno successivo alla entrata in vigore della legge di conversione del presente decreto.

Art. 51
Razionalizzazione degli uffici di cancelleria e notificazioni per via telematica.

1. All'art. 162, primo comma, della legge 23 ottobre 1960, n. 1196, é aggiunto, in fine, il seguente periodo: «Le cancellerie delle corti di appello e dei tribunali ordinari sono aperte al pubblico almeno quattro ore nei giorni feriali, secondo l'orario stabilito dai rispettivi presidenti, sentiti i capi delle cancellerie interessate.».
2. All'art. 16-bis del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, al comma 7 sono apportate le seguenti modificazioni:
a) le parole: «di cui ai commi da 1 a 4» sono sostituite dalle seguenti: «con modalità telematiche»;
b) sono aggiunti, in fine, i seguenti periodi: «Il deposito é tempestivamente eseguito quando la ricevuta di avvenuta consegna è generata entro la fine del giorno di scadenza e si applicano le disposizioni di cui all'art. 155, quarto e quinto comma, del codice di procedura civile. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nelle specifiche tecniche del responsabile per i sistemi informativi automatizzati del ministero della giustizia, il deposito degli atti o dei documenti può essere eseguito mediante gli invii di più messaggi di posta elettronica certificata. Il deposito è tempestivo quando è eseguito entro la fine del giorno di scadenza»[73].

Art. 52.
Poteri di autentica dei difensori e degli ausiliari del giudice.

1. Al decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:
a) all’art. 16-*bis* dopo il comma 9 è aggiunto, infine, il seguente:

[72] Cfr: legge 53/1994 come modificata da questo comma.
[73] Cfr. art. 16bis d.l. 179/12 come modificato da questo articolo.

«9 -*bis* . (*omissis*) »;[74]
b) dopo l'art. 16 -*quinquies* è inserito il seguente:
«Art. 16-sexies (Domicilio digitale). *omissis*».
2. Al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, sono apportate le seguenti modificazioni:
a) all'art. 40, dopo il comma 1-*ter* sono aggiunti i seguenti:
«1-*quater*. Il diritto di copia senza certificazione di conformità non è dovuto quando la copia è estratta dal fascicolo informatico dai soggetti abilitati ad accedervi.
1-*quinquies*. Il diritto di copia autentica non è dovuto nei casi previsti dall'art. 16 -*bis* , comma 9-*bis*, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.»;
b) all'art. 268, dopo il comma 1 è aggiunto il seguente:
«1-*bis*. Il diritto di copia autentica non è dovuto nei casi previsti dall'art. 16 -*bis* , comma 9 -*bis* , del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.»;
c) all'art. 269, il comma 1-*bis* è sostituito dal seguente:
«1-*bis*. Il diritto di copia senza certificazione di conformità non è dovuto quando la copia è estratta dal fascicolo informatico dai soggetti abilitati ad accedervi.».

(ritorna all'indice cronologico)

(torna all'indice per argomenti)

[74] Cfr.: art. 16bis d.l. 179/2012 come modificato da quest'articolo.

Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

(ritorna all'indice cronologico)

(torna all'indice per argomenti)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,
visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,
vista la proposta della Commissione europea,
previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,
visto il parere del Comitato economico e sociale europea,
deliberando secondo la procedura legislativa ordinaria,
considerando quanto segue:

(1) Instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.

(2) Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

(3) La direttiva 1999/93/CE del Parlamento europeo e del Consiglio trattava le firme elettroniche senza fornire un quadro transfrontaliero e transettoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego. Il presente regolamento rafforza ed estende l'acquis di tale direttiva.

(4) La comunicazione della Commissione del 26 agosto 2010, dal titolo «Agenda digitale europea» ha individuato nella frammentazione del mercato digitale, nella mancanza di interoperabilità e nell'aumento della criminalità cibernetica i grandi ostacoli al circolo virtuoso dell'economia digitale. Nella relazione 2010 sulla cittadinanza dell'UE, intitolata «Eliminare gli ostacoli all'esercizio dei diritti dei cittadini dell'Unione», la Commissione ha ulteriormente sottolineato la necessità di risolvere i principali problemi che impediscono ai cittadini dell'Unione di godere dei vantaggi di un mercato unico digitale e di servizi digitali transfrontalieri.

(5) Nelle conclusioni del 4 febbraio 2011 e del 23 ottobre 2011 il Consiglio europeo ha invitato la Commissione a creare un mercato unico digitale entro il 2015, a fare rapidi progressi in settori essenziali dell'economia digitale e a promuovere un mercato unico digitale pienamente integrato favorendo l'impiego transfrontaliero dei servizi online, con particolare riguardo all'agevolazione dell'identificazione e dell'autenticazione elettronica sicura.

(6) Nelle conclusioni del 27 maggio 2011, il Consiglio ha invitato la Commissione a contribuire al mercato unico digitale creando le condizioni adatte per il riconoscimento reciproco transfrontaliero di funzioni essenziali quali l'identificazione elettronica, i documenti elettronici, le firme elettroniche e i servizi elettronici di recapito, nonché per l'interoperabilità dei servizi di eGovernment in tutta l'Unione europea.

(7) Nella risoluzione del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico, il Parlamento europeo ha sottolineato l'importanza della sicurezza dei servizi elettronici, in particolare delle firme elettroniche, e della necessità di creare un'infrastruttura pubblica essenziale a livello paneuropeo ed ha invitato la Commissione ad allestire un Portale europeo delle autorità di convalida per garantire l'interoperabilità transfrontaliera delle firme elettroniche e per aumentare la sicurezza delle transazioni effettuate utilizzando Internet.

(8) La direttiva 2006/123/CE del Parlamento europeo e del Consiglio, dispone che gli Stati membri creino «sportelli unici» per garantire che tutte le procedure e formalità relative all'accesso a un'attività di servizi ed al suo svolgimento possano essere facilmente espletate a distanza ed elettronicamente attraverso lo sportello unico corrispondente e con le autorità competenti. Numerosi servizi online accessibili presso gli sportelli unici richiedono l'identificazione, l'autenticazione e la firma elettroniche.

(9) In molti casi i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri. Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno. Disporre di mezzi di identificazione elettronica

riconosciuti reciprocamente permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche.

(10) La direttiva 2011/24/UE del Parlamento europeo e del Consiglio istituisce una rete di autorità nazionali responsabili dell'assistenza sanitaria online. Per migliorare la sicurezza e la continuità dell'assistenza sanitaria transfrontaliera, tale rete deve elaborare orientamenti sull'accesso transfrontaliero ai dati e ai servizi elettronici, anche sostenendo «misure comuni di identificazione e autenticazione per agevolare la trasferibilità dei dati nell'assistenza sanitaria transfrontaliera». Il riconoscimento reciproco dell'identificazione e dell'autenticazione elettronica è un fattore essenziale per realizzare l'assistenza sanitaria transfrontaliera per i cittadini europei. Quando i cittadini viaggiano per ottenere assistenza medica, la loro cartella clinica deve essere accessibile nel paese in cui si sottopongono alle cure. Ciò richiede un quadro di identificazione elettronica solido, sicuro e affidabile.

(11) Il presente regolamento dovrebbe essere applicato nel pieno rispetto dei principi relativi alla protezione dei dati personali ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio. A tale riguardo, per quanto concerne il principio del riconoscimento reciproco stabilito dal presente regolamento, l'autenticazione in un servizio online dovrebbe riguardare esclusivamente il trattamento di dati di identificazione che siano adeguati, pertinenti e non eccedenti per garantire l'accesso a detto servizio online. Inoltre, gli obblighi previsti dalla direttiva 95/46/CE in materia di riservatezza e sicurezza dei trattamenti dovrebbero essere rispettati dai prestatori di servizi fiduciari e dagli organismi di vigilanza.

(12) Un obiettivo del presente regolamento è l'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici. Il presente regolamento non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri. Lo scopo del presente regolamento è garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

(13) È opportuno che gli Stati membri rimangano liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, e che possano decidere dell'eventuale partecipazione del settore privato nell'offerta di tali mezzi. È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione. Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici.

(14) Occorre che il presente regolamento fissi talune condizioni in merito all'obbligo di riconoscimento dei mezzi di identificazione elettronica e alle modalità di notifica dei regimi di identificazione elettronica. È opportuno che tali condizioni aiutino gli Stati membri a costruire la necessaria fiducia nei rispettivi regimi di identificazione elettronica e a riconoscere reciprocamente i mezzi di identificazione elettronica che fanno parte dei regimi notificati. È opportuno che il principio del riconoscimento reciproco si applichi ove il regime di identificazione elettronica dello Stato membro notificante soddisfi le condizioni di notifica e la notifica sia stata pubblicata nella *Gazzetta ufficiale dell'Unione europea*. Tuttavia, il principio del riconoscimento reciproco dovrebbe riguardare esclusivamente l'autenticazione nei servizi online. È opportuno che l'accesso a tali servizi online e la loro fornitura finale al richiedente siano strettamente collegati al diritto a usufruire di tali servizi alle condizioni fissate nel diritto nazionale.

(15) L'obbligo di riconoscere i mezzi di identificazione elettronica dovrebbe riferirsi esclusivamente ai mezzi il cui livello di garanzia dell'identità corrisponde a un livello pari o superiore a quello richiesto per il servizio online in questione. Inoltre, tale obbligo dovrebbe applicarsi solo qualora l'organismo del settore pubblico in questione utilizzi il livello di garanzia «significativo» o «elevato» in relazione all'accesso a tale servizio online. È opportuno che gli Stati membri mantengano la libertà, conformemente al diritto comunitario, di riconoscere mezzi di identificazione elettronica aventi livelli di garanzia dell'identità inferiori.

(16) I livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata. Il livello di garanzia dipende dal grado di sicurezza fornito dai mezzi di identificazione elettronica riguardo all'identità pretesa o dichiarata di una persona tenendo conto dei procedimenti (ad esempio, controllo e verifica dell'identità, e autenticazione), delle attività di gestione (ad esempio,

l'entità che rilascia i mezzi di identificazione elettronica e la procedura di rilascio di tali mezzi) e dei controlli tecnici messi in atto. Come risultato dei progetti pilota su larga scala finanziati dall'Unione, della normazione e di attività a livello internazionale, esistono varie definizioni e descrizioni tecniche dei livelli di garanzia. In particolare, il progetto pilota su larga scala STORK e la norma ISO 29115 fanno riferimento, tra l'altro, ai livelli 2, 3 e 4, che dovrebbero essere tenuti nella massima considerazione all'atto di stabilire le norme, le procedure e i requisiti tecnici minimi per i livelli di garanzia basso, significativo ed elevato ai sensi del presente regolamento, assicurando al contempo l'applicazione coerente del presente regolamento in particolare per quanto riguarda il livello di garanzia elevato in relazione al controllo dell'identità ai fini del rilascio di certificati qualificati. I requisiti stabiliti dovrebbero essere neutrali dal punto di vista tecnologico. Dovrebbe essere possibile soddisfare i requisiti di sicurezza necessari attraverso tecnologie differenti.

(17) È opportuno che gli Stati membri incoraggino il settore privato a impiegare volontariamente mezzi di identificazione elettronica nell'ambito di un regime notificato a fini di identificazione ove necessario per servizi online o transazioni elettroniche. La facoltà di ricorrere a tali mezzi di identificazione elettronica consentirebbe al settore privato di avvalersi dell'identificazione e autenticazione elettroniche già ampiamente impiegate in molti Stati membri almeno per i servizi pubblici e di agevolare alle imprese e ai cittadini l'accesso transfrontaliero ai loro servizi online. Per facilitare l'impiego transfrontaliero di tali mezzi di identificazione elettronica da parte del settore privato, è opportuno che la possibilità di autenticazione offerta da uno Stato membro sia disponibile alle parti del settore privato facenti affidamento sulla certificazione stabilite al di fuori del territorio di detto Stato membro alle stesse condizioni applicate alle parti del settore privato facenti affidamento sulla certificazione stabilite nel suddetto Stato membro. Di conseguenza, per quanto riguarda le parti del settore privato facenti affidamento sulla certificazione, lo Stato membro notificante può definire termini di accesso ai mezzi di autenticazione. Detti termini di accesso possono indicare se i mezzi di autenticazione relativi al regime notificato sono attualmente disponibili alle parti del settore privato facenti affidamento sulla certificazione.

(18) Il presente regolamento dovrebbe prevedere la responsabilità dello Stato membro notificante, della parte che rilascia i mezzi di identificazione elettronica e della parte che gestisce la procedura di autenticazione per mancato rispetto degli obblighi pertinenti a norma del presente regolamento. Tuttavia, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali in materia di responsabilità. Pertanto esso non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni o alle pertinenti norme procedurali applicabili, incluso l'onere della prova.

(19) La sicurezza dei regimi di identificazione elettronica è fondamentale per un affidabile riconoscimento reciproco transfrontaliero dei mezzi di identificazione elettronica. In tale contesto, gli Stati membri dovrebbero cooperare in materia di sicurezza e interoperabilità dei regimi di identificazione elettronica a livello dell'Unione. Ogniqualvolta i regimi di identificazione elettronica richiedano alle parti che fanno affidamento sulla certificazione di utilizzare hardware o software specifici a livello nazionale, l'interoperabilità transfrontaliera richiede che tali Stati membri non impongano tali requisiti e le spese relative alle parti facenti affidamento sulla certificazione stabilite al di fuori del loro territorio. In tal caso si dovrebbero esaminare ed elaborare soluzioni appropriate nell'ambito del quadro di interoperabilità. Tuttavia, sono inevitabili i requisiti tecnici derivanti dalle specifiche inerenti ai mezzi di identificazione elettronica nazionali e suscettibili di avere ripercussioni per i detentori di tali mezzi elettronici (ad esempio, le smart card).

(20) È opportuno che la cooperazione degli Stati membri agevoli l'interoperabilità tecnica dei regimi di identificazione elettronica notificati, al fine di promuovere un elevato livello di fiducia e sicurezza, in funzione del grado di rischio. È opportuno che lo scambio di informazioni e la condivisione delle migliori prassi fra Stati membri, finalizzati al riconoscimento reciproco dei regimi, facilitino tale cooperazione.

(21) È anche opportuno che il presente regolamento istituisca un quadro giuridico generale per l'impiego dei servizi fiduciari. Tuttavia, non è opportuno che istituisca un obbligo generale di farne uso o che installi un punto di accesso per tutti i servizi fiduciari esistenti. In particolare, non è auspicabile che il regolamento copra la prestazione di servizi fiduciari usati esclusivamente nell'ambito di sistemi chiusi da un insieme definito di partecipanti che non hanno ripercussioni su terzi. Ad esempio, i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal presente regolamento. Solo i servizi fiduciari prestati al pubblico aventi ripercussioni su terzi dovrebbero soddisfare i requisiti previsti dal presente regolamento. Non è neanche auspicabile che il presente regolamento copra aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici

nei casi in cui la normativa nazionale o unionale stabilisca obblighi quanto alla forma. Inoltre, non dovrebbe avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali.

(22) Al fine di contribuire al loro impiego transfrontaliero generale, è opportuno che sia possibile utilizzare i servizi fiduciari come prove in procedimenti giudiziali in tutti gli Stati membri. Spetta al diritto nazionale definire gli effetti giuridici dei servizi fiduciari, salvo che il presente regolamento provveda altrimenti.

(23) Nella misura in cui il presente regolamento disponga l'obbligo di riconoscere un servizio fiduciario, tale servizio fiduciario può essere rifiutato solo qualora il destinatario dell'obbligo non sia in grado di leggerlo o verificarlo per motivi tecnici che sfuggono al suo immediato controllo. Tuttavia, tale obbligo non dovrebbe di per se stesso esigere che un organismo pubblico ottenga l'hardware e il software necessari per la leggibilità tecnica di tutti i servizi fiduciari esistenti.

(24) Gli Stati membri possono mantenere o introdurre disposizioni nazionali, conformemente al diritto dell'Unione, in materia di servizi fiduciari, nella misura in cui detti servizi non siano pienamente armonizzati dal presente regolamento. Tuttavia, i servizi fiduciari conformi al presente regolamento dovrebbero godere della libera circolazione nel mercato interno.

(25) È opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quali servizi fiduciari qualificati.

(26) In considerazione del ritmo dei mutamenti tecnologici, occorre che il presente regolamento adotti un approccio aperto all'innovazione.

(27) È opportuno che il presente regolamento sia neutrale sotto il profilo tecnologico. È auspicabile che gli effetti giuridici prodotti dal presente regolamento siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti.

(28) Al fine di migliorare in particolare la fiducia delle piccole e medie imprese (PMI) e dei consumatori nel mercato interno e di promuovere l'impiego dei servizi e prodotti fiduciari, è opportuno introdurre le nozioni di servizi fiduciari qualificati e di prestatori di servizi fiduciari qualificati, per precisare i requisiti e gli obblighi che garantiscano un elevato livello di sicurezza di tutti i servizi e prodotti fiduciari qualificati impiegati o prestati.

(29) In linea con gli obblighi assunti a norma della Convenzione delle Nazioni Unite per i diritti delle persone con disabilità, approvata con decisione 2010/48/CE del Consiglio, in particolare l'articolo 9 della Convenzione, le persone con disabilità dovrebbero poter utilizzare servizi fiduciari e prodotti destinati al consumatore finale impiegati nella prestazione di tali servizi alle stesse condizioni degli altri consumatori. Ove fattibile, pertanto, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi dovrebbero essere resi accessibili alle persone con disabilità. La valutazione di fattibilità dovrebbe includere considerazioni tecniche ed economiche.

(30) Gli Stati membri dovrebbero designare uno o più organismi di vigilanza per lo svolgimento delle attività di vigilanza previste dal presente regolamento. Gli Stati membri dovrebbero altresì avere facoltà di decidere, di comune accordo con un altro Stato membro, di designare un organismo di vigilanza nel territorio di tale altro Stato membro.

(31) Gli organismi di vigilanza dovrebbero cooperare con le autorità di protezione dei dati, ad esempio informandole in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali. In particolare, è opportuno che la trasmissione di informazioni copra gli incidenti di sicurezza e le violazioni dei dati personali.

(32) È opportuno che tutti i prestatori di servizi fiduciari adottino buone prassi di sicurezza in funzione dei rischi connessi con le loro attività, in modo da migliorare la fiducia degli utilizzatori nel mercato unico.

(33) È opportuno che le disposizioni sull'uso degli pseudonimi nei certificati non impediscano agli Stati membri di chiedere l'identificazione delle persone in base alla normativa unionale o nazionale.

(34) È opportuno che tutti gli Stati membri si adeguino a requisiti essenziali comuni di vigilanza per garantire un livello paragonabile di sicurezza dei servizi fiduciari qualificati. Per facilitare l'applicazione coerente di tali requisiti in tutta l'Unione occorre che gli Stati membri adottino procedure paragonabili e scambino informazioni sulle loro attività di vigilanza e sulle migliori prassi del settore.

(35) Tutti i prestatori di servizi fiduciari dovrebbero essere soggetti ai requisiti del presente regolamento, in particolare a quelli in materia di sicurezza e responsabilità, al fine di garantire la dovuta diligenza, la trasparenza e l'attendibilità delle loro operazioni e servizi. Tuttavia, tenendo conto del tipo di

servizi fornito dai prestatori di servizi fiduciari, per quanto riguarda tali requisiti è opportuno distinguere tra servizi fiduciari qualificati e non qualificati.

(36) L'istituzione di un regime di vigilanza per tutti i prestatori di servizi fiduciari dovrebbe assicurare parità di condizioni per la sicurezza e l'attendibilità delle loro operazioni e servizi, contribuendo in tal modo alla tutela degli utenti e al funzionamento del mercato interno. I prestatori di servizi fiduciari non qualificati dovrebbero essere soggetti ad attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. Pertanto l'organismo di sorveglianza non dovrebbe avere un obbligo generale di vigilanza sui prestatori di servizi non qualificati. L'organismo di sorveglianza dovrebbe adottare misure solo quando viene informato (ad esempio, dallo stesso prestatore di servizi fiduciari non qualificati, da un altro organismo di sorveglianza, mediante la notifica di un utente o di un partner commerciale o in base a sue indagine proprie) che un prestatore di servizi fiduciari non qualificato non soddisfa i requisiti del presente regolamento.

(37) Il presente regolamento dovrebbe prevedere la responsabilità di tutti i prestatori di servizi fiduciari. In particolare, stabilisce il regime di responsabilità in base al quale tutti i prestatori di servizi fiduciari dovrebbero essere responsabili dei danni provocati a persone fisiche o giuridiche a causa del mancato rispetto degli obblighi previsti dal presente regolamento. Al fine di agevolare la valutazione del rischio finanziario che i prestatori di servizi fiduciari possano dover sostenere o che debbano coprire con polizze assicurative, il presente regolamento autorizza i prestatori di servizi fiduciari a stabilire limiti, a talune condizioni, all'uso dei servizi da essi prestati e non essere pertanto responsabili dei danni derivanti dall'uso dei servizi oltre i suddetti limiti. I clienti dovrebbero essere debitamente e anticipatamente informati di tali limiti. Tali limiti dovrebbero essere riconoscibili per i terzi, ad esempio inserendo informazioni sui limiti nei termini e nelle condizioni del servizio prestato o attraverso altri mezzi riconoscibili. Allo scopo di dare effetto a tali principi, il presente regolamento dovrebbe essere applicato conformemente alle norme nazionali sulla responsabilità. Pertanto, il presente regolamento non pregiudica tali norme nazionali in ordine, ad esempio, alla definizione dei danni, del dolo, della negligenza o alle pertinenti norme procedurali applicabili.

(38) La notifica delle violazioni di sicurezza e delle valutazioni di rischio per la sicurezza è essenziale per fornire informazioni adeguate alle parti interessate in caso di violazione di sicurezza o perdita di integrità.

(39) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di notifica delle violazioni di cui al presente regolamento, è opportuno imporre l'obbligo agli organismi di vigilanza di fornire informazioni riassuntive alla Commissione e all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

(40) Per consentire alla Commissione e agli Stati membri di valutare l'efficacia del meccanismo di vigilanza perfezionato di cui al presente regolamento, è opportuno chiedere agli organismi di vigilanza di riferire sulle loro attività. Ciò servirebbe ad agevolare lo scambio di buone prassi fra organismi di vigilanza e consentirebbe di verificare l'applicazione coerente ed efficiente dei requisiti essenziali di vigilanza in tutti gli Stati membri.

(41) Per garantire che i servizi fiduciari qualificati siano sostenibili e duraturi e migliorare la fiducia degli utilizzatori nella continuità di detti servizi, è opportuno che gli organismi di vigilanza verifichino l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nel caso in cui prestatori di servizi fiduciari qualificati cessino le loro attività.

(42) Per facilitare la vigilanza sui prestatori di servizi fiduciari qualificati, ad esempio allorché un prestatore offre i suoi servizi sul territorio di uno Stato membro in cui non è soggetto a vigilanza o qualora i computer di un prestatore siano situati nel territorio di uno Stato membro diverso da quello in cui il prestatore è stabilito, è opportuno istituire un sistema di assistenza mutua fra gli organismi di vigilanza negli Stati membri.

(43) Al fine di assicurare la conformità dei prestatori di servizi fiduciari qualificati e dei servizi da essi prestati ai requisiti stabiliti dal presente regolamento, un organismo di valutazione della conformità dovrebbe effettuare una valutazione della conformità; i prestatori di servizi fiduciari qualificati dovrebbero trasmettere all'organismo di vigilanza le relazioni di valutazione di conformità risultanti. Ogniqualvolta l'organismo di vigilanza richieda a un prestatore di servizi fiduciari qualificato di presentare una relazione di valutazione di conformità ad hoc, l'organismo di vigilanza dovrebbe rispettare in particolare i principi di buona amministrazione, compreso l'obbligo di fornire le motivazioni delle sue decisioni, nonché il principio di proporzionalità. Pertanto, l'organismo di vigilanza dovrebbe debitamente giustificare la propria decisione di imporre una valutazione di conformità ad hoc.

(44) Il presente regolamento mira a garantire un quadro coerente affinché i servizi fiduciari siano dotati di

un livello elevato di sicurezza e certezza giuridica. A tale riguardo, nel trattare la valutazione di conformità di prodotti e servizi, la Commissione dovrebbe, ove opportuno, cercare sinergie con i pertinenti regimi europei e internazionali vigenti, quali il regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio che sancisce gli obblighi in materia di accreditamento degli organismi di valutazione della conformità e vigilanza del mercato di prodotti.

(45) Per consentire un processo di avviamento efficiente, che conduca all'inclusione dei prestatori di servizi fiduciari qualificati e dei servizi fiduciari qualificati da essi offerti negli elenchi di fiducia, è opportuno incoraggiare interazioni preliminari fra gli aspiranti prestatori di servizi fiduciari qualificati e l'organismo di vigilanza competente, in vista di facilitare l'esercizio della dovuta diligenza nell'offerta di servizi fiduciari qualificati.

(46) Gli elenchi di fiducia sono elementi essenziali nel costruire la fiducia fra operatori di mercato perché indicano la condizione qualificata del prestatore di servizi al momento della vigilanza.

(47) La fiducia nei servizi online e la loro agevolezza sono essenziali perché gli utilizzatori possano beneficiare a pieno dei servizi elettronici e avvalersi consapevolmente di essi. A tale scopo si dovrebbe creare un marchio di fiducia UE per individuare i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati. Tale marchio di fiducia UE per i servizi fiduciari qualificati distinguerebbe chiaramente i servizi fiduciari qualificati da altri servizi fiduciari, contribuendo così alla trasparenza sul mercato. L'utilizzo di un marchio di fiducia UE da parte dei prestatori di servizi fiduciari qualificati dovrebbe essere volontario e non dovrebbe implicare requisiti aggiuntivi diversi da quelli previsti dal presente regolamento.

(48) Sebbene sia necessario un elevato livello di sicurezza per garantire il riconoscimento reciproco delle firme elettroniche, in casi specifici come nel contesto della decisione 2009/767/CE della Commissione, è opportuno che siano accettate anche firme elettroniche con una garanzia di sicurezza più debole.

(49) Il presente regolamento dovrebbe stabilire il principio secondo il quale alla firma elettronica non dovrebbero essere negati gli effetti giuridici per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal presente regolamento secondo cui una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa.

(50) Poiché attualmente le autorità competenti negli Stati membri utilizzano formati diversi di firme elettroniche avanzate per firmare elettronicamente i loro documenti, occorre garantire che almeno alcuni formati di firma elettronica possano essere supportati tecnicamente dagli Stati membri allorché ricevono documenti firmati elettronicamente. Analogamente, allorché le autorità competenti negli Stati membri fanno uso di sigilli elettronici, occorre garantire che supportino almeno alcuni formati di sigillo elettronico avanzato.

(51) È opportuno che il firmatario possa affidare a terzi i dispositivi per la creazione di una firma elettronica qualificata, purché siano rispettati appropriati meccanismi e procedure per garantire che il firmatario mantenga il controllo esclusivo sull'uso dei suoi dati di creazione di firma elettronica e l'uso del dispositivo soddisfi i requisiti della firma elettronica qualificata.

(52) Visti i suoi molteplici vantaggi economici, sarà ulteriormente sviluppata la creazione di firme elettroniche a distanza, qualora l'ambiente di creazione di firma elettronica sia gestito da un prestatore di servizi fiduciari a nome del firmatario. Tuttavia, per garantire che alle firme elettroniche sia attribuito lo stesso riconoscimento giuridico delle firme elettroniche create con un ambiente interamente gestito dall'utente, i prestatori che offrono servizi di firma elettronica a distanza dovrebbero applicare procedure di sicurezza di gestione e amministrative specifiche e utilizzare sistemi e prodotti affidabili, che in particolare comprendano canali di comunicazione elettronici sicuri per garantire l'affidabilità dell'ambiente di creazione di firma elettronica e assicurare che sia utilizzato sotto il controllo esclusivo del firmatario. Nel caso di una firma elettronica qualificata creata mediante un dispositivo di creazione di firma elettronica a distanza, dovrebbero applicarsi i requisiti applicabili ai prestatori di servizi fiduciari qualificati, stabiliti dal presente regolamento.

(53) La sospensione dei certificati qualificati è una prassi operativa abituale dei prestatori di servizi fiduciari in una serie di Stati membri, che è diversa dalla revoca e comporta la perdita di validità temporanea di un certificato. La certezza del diritto richiede che la situazione di sospensione di un certificato sia sempre indicata chiaramente. A tale scopo i prestatori di servizi fiduciari dovrebbero avere la responsabilità di indicare chiaramente la situazione del certificato e, in caso di sospensione, il periodo di tempo esatto durante il quale il certificato è sospeso. È opportuno che il presente regolamento non imponga ai prestatori di servizi fiduciari o agli Stati membri l'utilizzo della

sospensione, ma preveda norme di trasparenza nei casi in cui tale prassi è disponibile.

(54) L'interoperabilità transfrontaliera e il riconoscimento dei certificati qualificati è una condizione essenziale per il riconoscimento transfrontaliero delle firme elettroniche qualificate. Pertanto, i certificati qualificati non dovrebbero essere soggetti a requisiti obbligatori oltre ai requisiti di cui al presente regolamento. Tuttavia, a livello nazionale, dovrebbe essere consentita l'inclusione di attributi specifici, quali identificatori unici, nei certificati qualificati, purché tali attributi specifici non ostacolino l'interoperabilità transfrontaliera e il riconoscimento dei certificati e delle firme elettroniche qualificati.

(55) La certificazione della sicurezza delle tecnologie d'informazione basata su norme internazionali, come l'ISO 15408 e i metodi di valutazione e le disposizioni di riconoscimento reciproco connessi, è uno strumento importante per verificare la sicurezza dei dispositivi per la creazione di una firma elettronica qualificata e dovrebbe essere promossa. Soluzioni e servizi innovativi, quali la firma in cloud e la firma mobile, tuttavia, si basano su soluzioni tecniche e organizzative per dispositivi per la creazione di una firma elettronica qualificata per i quali possono non essere ancora disponibili norme di sicurezza o per i quali può essere in corso la prima certificazione della sicurezza delle tecnologie d'informazione. Il livello di sicurezza di tali dispositivi per la creazione di una firma elettronica qualificata potrebbe essere valutato utilizzando procedure alternative solo se tali norme di sicurezza non sono disponibili o se la prima certificazione della sicurezza delle tecnologie d'informazione è in corso. Tali processi dovrebbero essere comparabili alle norme per la certificazione della sicurezza delle tecnologie d'informazione sempre che i livelli di sicurezza siano equivalenti. Tali processi potrebbero essere agevolati da una revisione tra pari.

(56) Il presente regolamento dovrebbe stabilire i requisiti relativi a dispositivi per la creazione di una firma elettronica qualificata al fine di assicurare la funzionalità delle firme elettroniche avanzate. Il presente regolamento non dovrebbe contemplare la globalità dell'ambiente del sistema in cui tali dispositivi operano. Pertanto, l'ambito di applicazione della certificazione dei dispositivi per la creazione di una firma qualificata dovrebbe essere limitato all'hardware e al software di sistema utilizzato per gestire e proteggere i dati per la creazione di una firma elettronica creati, memorizzati o trattati nel dispositivo di creazione di una firma. Come specificato nelle norme pertinenti, l'ambito di applicazione dell'obbligo di certificazione dovrebbe escludere le applicazioni relative alla creazione di una firma.

(57) Per garantire la certezza giuridica della validità della firma, è essenziale specificare i componenti di una firma elettronica qualificata, che dovrebbero essere valutati dalla parte facente affidamento sulla certificazione che effettua la convalida. Inoltre, è opportuno che attraverso la specificazione degli obblighi dei prestatori di servizi fiduciari qualificati che possono offrire un servizio di convalida qualificata a parti facenti affidamento sulla certificazione che non vogliono o non possono effettuare esse stesse la convalida di firme elettroniche qualificate siano stimolati gli investimenti del settore privato e pubblico in tali servizi. È opportuno che entrambi gli elementi rendano la convalida delle firme elettroniche qualificate semplice e agevole per tutte le parti a livello dell'Unione.

(58) Qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.

(59) È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.

(60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di sigilli elettronici dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di sigillo elettronico, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.

(61) È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.

(62) Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa

gli obblighi previsti nel presente regolamento.

(63)I documenti elettronici sono importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.

(64)Nel trattare i formati delle firme e dei sigilli elettronici avanzati, la Commissione dovrebbe basarsi sulle prassi, sulle norme e sulla legislazione esistente, in particolare la decisione 2011/130/UE della Commissione.

(65)Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server.

(66)È essenziale prevedere un quadro giuridico per agevolare il riconoscimento transfrontaliero tra gli ordinamenti giuridici nazionali esistenti relativi ai servizi elettronici di recapito certificato. Tale quadro potrebbe aprire inoltre per i prestatori di servizi fiduciari dell'Unione nuove opportunità di mercato per l'offerta di nuovi servizi elettronici di recapito certificati paneuropei.

(67)I servizi di autenticazione dei siti web prevedono un mezzo tramite il quale il visitatore di un sito può accertarsi che dietro a quel sito web vi è un'entità reale e legittima. Tali servizi contribuiscono a diffondere sicurezza e fiducia nelle transazioni commerciali on line, in quanto gli utenti si fideranno di un sito web che è stato autenticato. La fornitura e l'uso di servizi di autenticazione dei siti web sono interamente volontari. Tuttavia, affinché l'autenticazione dei siti web divenga un mezzo per rafforzare la fiducia, fornire un'esperienza migliore all'utente e promuovere la crescita nel mercato interno, è opportuno che il presente regolamento stabilisca obblighi minimi in materia di sicurezza e responsabilità per i prestatori e i loro servizi. A tal fine, si è tenuto conto dei risultati delle iniziative industriali esistenti, ad esempio, il Forum Autorità di certificazione/Browser (CA/B Forum). Inoltre, il presente regolamento non dovrebbe impedire l'uso di altri mezzi o metodi di autenticazione di un sito web non rientranti nel presente regolamento e non dovrebbe vietare ai prestatori di servizi di autenticazione dei siti web di paesi terzi di prestare i propri servizi ai clienti dell'Unione. Tuttavia, i servizi di autenticazione dei siti web di un prestatore di un paese terzo dovrebbero essere riconosciuti come qualificati ai sensi del presente regolamento solo se è stato concluso un accordo internazionale tra l'Unione e il paese di stabilimento di detto prestatore.

(68)La nozione di «persone giuridiche» secondo le disposizioni del trattato sul funzionamento dell'Unione europea (TFUE) in materia di stabilimento lascia agli operatori la libertà di scegliere la forma giuridica che ritengono opportuna per svolgere la loro attività. Di conseguenza, per «persone giuridiche» ai sensi del TFUE si intendono tutte le entità costituite conformemente al diritto di uno Stato membro o da esso disciplinate, a prescindere dalla loro forma giuridica.

(69)Le istituzioni, gli organi, gli uffici e le agenzie dell'Unione sono incoraggiate a riconoscere l'identificazione elettronica e i servizi fiduciari contemplati dal presente regolamento ai fini dell'amministrazione cooperativa facendo tesoro, in particolare, delle buone prassi esistenti e dei risultati dei progetti in corso nei settori contemplati dal presente regolamento.

(70)Al fine di completare determinati aspetti tecnici dettagliati del presente regolamento in modo flessibile e veloce, dovrebbe essere delegato alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE riguardo ai criteri che devono soddisfare gli organismi responsabili della certificazione dei dispositivi per la creazione di una firma elettronica qualificata. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.

(71)Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione, in particolare per specificare i numeri di riferimento delle norme il cui impiego conferisce una presunzione di adempimento di determinati requisiti stabiliti nel presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio.

(72)In sede di elaborazione degli atti delegati o di esecuzione, la Commissione dovrebbe tenere debito conto delle norme e delle specifiche tecniche elaborate da organizzazioni e organismi di normalizzazione europei e internazionali, in particolare il Comitato europeo di normalizzazione (CEN), l'Istituto europeo delle norme di telecomunicazione (ETSI), l'Organizzazione internazionale per la standardizzazione (ISO) e l'Unione internazionale delle telecomunicazioni (UIT), al fine di

assicurare un livello elevato di sicurezza e interoperabilità dell'identificazione elettronica e dei servizi fiduciari.

(73) Per motivi di certezza del diritto e di chiarezza è opportuno abrogare la direttiva 1999/93/CE.

(74) Per garantire la certezza giuridica per operatori di mercato che già fanno uso di certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE, è necessario prevedere un idoneo periodo transitorio. Analogamente, dovrebbero essere stabilite misure transitorie per i dispositivi per la creazione di una firma sicura, la cui conformità sia stata determinata ai sensi della direttiva 1999/93/CE, nonché per i prestatori di servizi di certificazione che rilasciano certificati qualificati entro il 1º luglio 2016. Infine, è altresì necessario dotare la Commissione dei mezzi per adottare atti di esecuzione e atti delegati prima di tale data.

(75) Le date di applicazione stabilite nel presente regolamento non pregiudicano gli obblighi esistenti già contratti dagli Stati membri in base al diritto dell'Unione, in particolare della direttiva 2006/123/CE.

(76) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della portata dell'azione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(77) Il garante europeo della protezione dei dati è stato consultato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio e ha espresso un parere il 27 settembre 2012,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:

a) fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,

b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e

c) istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati diautenticazione di siti web.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

3. Il presente regolamento non pregiudica il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;

2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;

3) «dati di identificazione personale», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;

4) «regime di identificazione elettronica», un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;

5) «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;

6)«parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;
7)«organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;
8)«organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio;
9) «firmatario», una persona fisica che crea una firma elettronica;
10)«firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;
11) «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;
12)«firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;
13)«dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;
14)«certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;
15)«certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;
16)«servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:
a)creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
b) creazione, verifica e convalida di certificati di autenticazione di siti web; o
c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;
17)«servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;
18)«organismo di valutazione della conformità», un organismo ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;
19)«prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;
20)«prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;
21)«prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;
22)«dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;
23)«dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;
24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;
25)«sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;
26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;
27)«sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;
28)«dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;
29)«certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;
30)«certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;
31)«dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;
33) «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;
34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;
35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;
36) «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;
37) «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;
38) «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;
39) «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;
40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;
41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

Articolo 4

Principio del mercato interno

1. Non sono imposte restrizioni alla prestazione di servizi fiduciari nel territorio di uno Stato membro da parte di un prestatore di servizi fiduciari stabilito in un altro Stato membro per motivi che rientrano negli ambiti di applicazione del presente regolamento.
2. I prodotti e i servizi fiduciari conformi al presente regolamento godono della libera circolazione nel mercato interno.

Articolo 5

Trattamento e protezione dei dati

1. Il trattamento dei dati a carattere personale è effettuato a norma della direttiva 95/46/CE.
2. Fatti salvi gli effetti giuridici che il diritto nazionale attribuisce agli pseudonimi, gli Stati membri non vietano l'uso di pseudonimi nelle transazioni elettroniche.

CAPO II
IDENTIFICAZIONE ELETTRONICA

Articolo 6

Riconoscimento reciproco

1. Ove il diritto o la prassi amministrativa nazionale richiedano l'impiego di un'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro, i mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti nel primo Stato membro ai fini dell'autenticazione transfrontaliera di tale servizio online, purché soddisfino le seguenti condizioni:
a) i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9;
b) il livello di garanzia dei mezzi di identificazione elettronica corrisponde a un livello di garanzia pari o superiore al livello di garanzia richiesto dall'organismo del settore pubblico competente per accedere al servizio online in questione nel primo Stato membro, sempre che il livello di garanzia di tali mezzi di identificazione elettronica corrisponda al livello di garanzia significativo o elevato;
c) l'organismo del settore pubblico competente usa il livello di garanzia significativo o elevato in relazione all'accesso a tale servizio online.

Tale riconoscimento ha luogo non oltre 12 mesi dalla data in cui la Commissione pubblica l'elenco i di cui alla lettera a), primo comma.
2. Un mezzo di identificazione elettronica rilasciato nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9 e che corrisponde al livello di garanzia basso può essere riconosciuto dagli organismi del settore pubblico ai fini dell'autenticazione transfrontaliera del servizio prestato online da tali organismi.

Articolo 7

Ammissibilità alla notifica dei regimi di identificazione elettronica

Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:

a) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica sono rilasciati:
   i) dallo Stato membro notificante;
   ii) su incarico dello Stato membro notificante; o
   iii) a titolo indipendente dallo Stato membro notificante e sono riconosciuti da tale Stato membro;

b) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico e che richiede l'identificazione elettronica nello Stato membro notificante;

c) il regime di identificazione elettronica e i mezzi di identificazione elettronica rilasciati conformemente alle sue disposizioni soddisfano i requisiti di almeno uno dei livelli di garanzia stabiliti nell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

d) lo Stato membro notificante garantisce che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure relative al pertinente livello di garanzia definito nell'atto di esecuzione di cui all'articolo 8, paragrafo 3, alla persona fisica o giuridica di cui all'articolo 3, punto 1, al momento in cui è rilasciata l'identificazione elettronica nell'ambito di detto regime;

e) la parte che rilascia i mezzi di identificazione elettronica nell'ambito di detto regime assicura che i mezzi di identificazione elettronica siano attribuiti alla persona di cui alla lettera d) del presente articolo conformemente alle specifiche, norme e procedure tecniche relative al pertinente livello di garanzia definito nnell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

f) lo Stato membro notificante garantisce la disponibilità dell'autenticazione online, per consentire alle parti facenti affidamento sulla certificazione stabilite nel territorio di un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica.

   Per le parti facenti affidamento sulla certificazione diverse dagli organismi del settore pubblico, lo Stato membro notificante può definire i termini di accesso a tale autenticazione. Quando l'autenticazione transfrontaliera è effettuata in relazione a un servizio online prestato da un organismo del settore pubblico, essa è fornita a titolo gratuito.

   Gli Stati membri non impongono alcun requisito tecnico specifico sproporzionato alle parti facenti affidamento sulla certificazione che intendono effettuare tale autenticazione, qualora tali requisiti impediscano o ostacolino notevolmente l'interoperabilità dei regimi di identificazione elettronica notificati;

g) almeno sei mesi prima della notifica di cui all'articolo 9, paragrafo 1, lo Stato membro notificante fornisce agli altri Stati membri, ai fini dell'obbligo previsto dall'articolo 12, paragrafo 5, una descrizione di detto regime conformemente alle modalità procedurali stabilite dagli atti di esecuzione di cui all'articolo 12, paragrafo 7;

h) il regime di identificazione elettronica soddisfa i requisiti definiti nell'atto di esecuzione di cui all'articolo 12, paragrafo 8.

Articolo 8

Livelli di garanzia dei regimi di identificazione elettronica

1. Un regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1, specifica livelli di garanzia basso, significativo e/o elevato per i mezzi di identificazione elettronica rilasciati nell'ambito di detto regime.

2. I livelli di garanzia basso, significativo e elevato soddisfano rispettivamente i seguenti criteri:

a) il livello di garanzia basso si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza limitato riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre il rischio di uso abusivo o alterazione dell'identità;

b) il livello di garanzia significativo si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza significativo riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre significativamente il rischio di uso abusivo o alterazione dell'identità;

c) il livello di garanzia elevato si riferisce a un mezzo di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza più elevato dei mezzi di identificazione elettronica aventi un livello di

garanzia significativo ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità.

3. Entro il 18 settembre 2015, tenendo conto delle norme internazionali pertinenti e fatto salvo il paragrafo 2, la Commissione, mediante atti di esecuzione, definisce le specifiche, norme e procedure tecniche minime in riferimento alle quali sono specificati i livelli di garanzia basso, significativo e elevato dei mezzi di identificazione elettronica ai fini del paragrafo 1.

Le suddette specifiche, norme e procedure tecniche minime sono fissate facendo riferimento all'affidabilità e alla qualità dei seguenti elementi:

a) della procedura di controllo e verifica dell'identità delle persone fisiche o giuridiche che chiedono il rilascio dei mezzi di identificazione elettronica;

b) della procedura di rilascio dei mezzi di identificazione elettronica richiesti;

c) del meccanismo di autenticazione mediante il quale la persona fisica o giuridica usa i mezzi di identificazione elettronica per confermare la propria identità a una parte facente affidamento sulla certificazione;

d) dell'entità che rilascia i mezzi di identificazione elettronica;

e) di qualsiasi altro organismo implicato nella domanda di rilascio dei mezzi di identificazione elettronica; e

f) delle specifiche tecniche e di sicurezza dei mezzi di identificazione elettronica rilasciati.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 9

Notifica

1. Lo Stato membro notificante rende note alla Commissione le informazioni seguenti e, senza indugio, qualsiasi loro successiva modifica:

a) una descrizione del regime di identificazione elettronica, con indicazione dei suoi livelli di garanzia e della o delle entità che rilasciano i mezzi di identificazione elettronica nell'ambito del regime;

b) il regime di vigilanza e il regime di informazioni sulla responsabilità applicabili per quanto riguarda:

   i) la parte che rilascia i mezzi di identificazione elettronica; e

   ii) la parte che gestisce la procedura di autenticazione;

c) l'autorità o le autorità responsabili del regime di identificazione elettronica;

d) informazioni sull'entità o sulle entità che gestiscono la registrazione dei dati unici di identificazione personale;

e) una descrizione di come sono soddisfatti i requisiti definiti negli atti di esecuzione di cui all'articolo 12, paragrafo 8;

f) una descrizione dell'autenticazione di cui all'articolo 7, lettera f);

g) disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

2. Un anno dopo la data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco dei regimi di identificazione elettronica notificati ai sensi del paragrafo 1 del presente articolo e le informazioni fondamentali al riguardo.

3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco di cui al paragrafo 2 entro due mesi dalla data di ricezione di tale notifica.

4. Uno Stato membro può presentare alla Commissione una richiesta di eliminazione del regime di identificazione elettronica da esso notificato dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricezione della richiesta dello Stato membro.

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche a norma del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 10

Violazione della sicurezza

1. In caso di violazione o parziale compromissione del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, o dell'autenticazione di cui all'articolo 7, lettera f), con limitazione dell'affidabilità dell'autenticazione transfrontaliera di tale regime, lo Stato membro notificante senza indugio sospende o revoca tale autenticazione transfrontaliera o le sue parti compromesse e ne informa gli altri Stati membri e la Commissione.

2. Una volta posto rimedio alla violazione o alla compromissione di cui al paragrafo 1, lo Stato membro notificante ristabilisce l'autenticazione transfrontaliera e informa senza indugio gli altri Stati membri e la Commissione.
3. Qualora non sia posto rimedio alla violazione o alla compromissione di cui al paragrafo 1 entro tre mesi dalla sospensione o dalla revoca, lo Stato membro notificante notifica agli altri Stati membri e alla Commissione il ritiro del regime di identificazione elettronica.
La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 9, paragrafo 2, nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 11

Responsabilità

1. Lo Stato membro notificante è responsabile per i danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dei suoi obblighi di cui all'articolo 7, lettere d) e f), in una transazione transfrontaliera.
2. La parte che rilascia i mezzi di identificazione elettronica è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dell'obbligo di cui all'articolo 7, lettera e), in una transazione transfrontaliera.
3. La parte che gestisce la procedura di autenticazione è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica per non avere garantito la corretta gestione dell'autenticazione di cui all'articolo 7, lettera f), in una transazione transfrontaliera.
4. I paragrafi 1, 2 e 3 si applicano conformemente alle norme nazionali in materia di responsabilità.
5. I paragrafi 1, 2 e 3 lasciano impregiudicata la responsabilità conformemente al diritto nazionale delle parti di una transazione in cui sono utilizzati mezzi di identificazione elettronica che rientrano nel regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1.

Articolo 12

Cooperazione e interoperabilità

1. I regimi nazionali di identificazione elettronica notificati a norma dell'articolo 9, paragrafo 1, sono interoperabili.
2. È istituito un quadro di interoperabilità ai fini del paragrafo 1.
3. Il quadro di interoperabilità risponde ai seguenti criteri:
a) mira a essere neutrale dal punto di vista tecnologico e non comporta discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro;
b) segue, ove possibile, le norme europee e internazionali;
c) facilita l'applicazione del principio della tutela della vita privata fin dalla progettazione (privacy by design); e
d) garantisce che i dati personali siano trattati a norma della direttiva 95/46/CE.
4. Il quadro di interoperabilità è composto da:
a) un riferimento ai requisiti tecnici minimi connessi ai livelli di garanzia di cui all'articolo 8;
b) una mappatura dei livelli di garanzia nazionali dei regimi di identificazione elettronica notificati in base ai livelli di garanzia di cui all'articolo 8;
c) un riferimento ai requisiti tecnici minimi di interoperabilità;
d) un riferimento a un insieme minimo di dati di identificazione personale che rappresentano un'unica persona fisica o giuridica, disponibile nell'ambito dei regimi di identificazione elettronica;
e) norme di procedura;
f) disposizioni per la risoluzione delle controversie; e
g) norme di sicurezza operativa comuni.
5. Gli Stati membri cooperano per quanto riguarda:
a) l'interoperabilità dei regimi di identificazione elettronica notificati ai sensi dell'articolo 9, paragrafo 1, e dei regimi di identificazione elettronica che gli Stati membri intendono notificare; e
b) la sicurezza dei regimi di identificazione elettronica.
6. La cooperazione fra gli Stati membri riguarda:
a) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i regimi di identificazione elettronica e, in particolare, i requisiti tecnici connessi all'interoperabilità e ai livelli di garanzia;
b) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i metodi di lavoro con i livelli di garanzia dei regimi di identificazione elettronica di cui all'articolo 8;
c) la valutazione tra pari dei regimi di identificazione elettronica che rientrano nel presente regolamento; e
d) l'esame degli sviluppi pertinenti nel settore dell'identificazione elettronica.

7. Entro il 18 marzo 2015, la Commissione, mediante atti di esecuzione, fissa le modalità procedurali necessarie per facilitare la collaborazione fra gli Stati membri di cui ai paragrafi 5 e 6, al fine di promuovere un elevato livello di fiducia e di sicurezza, commisurato al grado di rischio esistente.
8. Entro il 18 settembre 2015, al fine di garantire condizioni uniformi di esecuzione del requisito di cui al paragrafo 1, la Commissione, fatti salvi i criteri di cui al paragrafo 3 e tenendo conto dei risultati della cooperazione fra gli Stati membri, adotta atti di esecuzione sul quadro di interoperabilità quale definito al paragrafo 4.
9. Gli atti di esecuzione di cui a paragrafi 7 e 8 sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

CAPO III
SERVIZI FIDUCIARI
SEZIONE 1
Disposizioni generali
Articolo 13
Responsabilità e onere della prova

1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.
L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.
Si presume il dolo o la negligenza di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.
2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle limitazioni d'uso dei servizi da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati.
3. I paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità.

Articolo 14
Relazioni internazionali

1. I servizi fiduciari prestati da prestatori di servizi fiduciari stabiliti in un paese terzo sono riconosciuti giuridicamente equivalenti ai servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione qualora i servizi fiduciari aventi origine nel paese terzo siano riconosciuti a norma di un accordo concluso fra l'Unione e il paese terzo in questione o un'organizzazione internazionale a norma dell'articolo 218 TFUE.
2. Gli accordi di cui al paragrafo 1 garantiscono, in particolare, che:
a) i requisiti che si applicano ai prestatori di servizi fiduciari qualificati stabiliti nell'Unione e ai servizi fiduciari qualificati che prestano siano soddisfatti dai prestatori di servizi fiduciari nel paese terzo o presso le organizzazioni internazionali con cui è concluso l'accordo, nonché dai servizi fiduciari da essi prestati;
b) i servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione sono riconosciuti come giuridicamente equivalenti ai servizi fiduciari prestati da prestatori di servizi fiduciari nel paese terzo o presso l'organizzazione internazionale con cui è concluso l'accordo.

Articolo 15
Accessibilità per le persone con disabilità

Ove possibile, i servizi fiduciari prestati e i prodotti destinati all'utilizzatore finale impiegati per la prestazione di detti servizi sono resi accessibili alle persone con disabilità.

Articolo 16
Sanzioni

Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive.

SEZIONE 2
Vigilanza
Articolo 17
Organismo di vigilanza

1. Gli Stati membri designano un organismo di vigilanza stabilito nel loro territorio o, di comune accordo con un altro Stato membro, un organismo di vigilanza stabilito in tale altro Stato membro. Tale organismo è responsabile di compiti di vigilanza nello Stato membro designante.
Agli organismi di vigilanza sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dei rispettivi organismi di vigilanza designati.

3. Il ruolo dell'organismo di vigilanza è il seguente:

a) vigilare sui prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante per assicurarsi, mediante attività di vigilanza ex ante e ex post, che essi e i servizi fiduciari qualificati da essi prestati rispondano ai requisiti di cui al presente regolamento;

b) adottare misure, ove necessario, in relazione a prestatori di servizi fiduciari non qualificati stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora sia informato che tali prestatori di servizi fiduciari non qualificati o i servizi fiduciari da essi prestati presumibilmente non soddisfano i requisiti stabiliti dal presente regolamento.

4. Ai fini del paragrafo 3 e fatte salve le limitazioni ivi previste, l'organismo di vigilanza ha, in particolare, i compiti seguenti:

a) cooperare con altri organismi di vigilanza e assisterli a norma dell'articolo 18;

b) analizzare le relazioni di valutazione della conformità di cui all'articolo 20, paragrafo 1, e all'articolo 21, paragrafo 1;

c) informare gli altri organismi di vigilanza e il pubblico in merito a violazioni della sicurezza o perdita di integrità a norma dell'articolo 19, paragrafo 2;

d) riferire alla Commissione in merito alle sue principali attività a norma del paragrafo 6 del presente articolo;

e) svolgere verifiche o chiedere a un organismo di valutazione della conformità di effettuare una valutazione di conformità dei prestatori di servizi fiduciari qualificati a norma dell'articolo 20, paragrafo 2;

f) cooperare con le autorità di protezione, in particolare informandole senza indugio dei dati in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali;

g) concedere la qualifica ai prestatori di servizi fiduciari e ai servizi da essi prestati e ritirare tale qualifica a norma degli articoli 20 e 21;

h) informare l'organismo responsabile dell'elenco nazionale di fiducia di cui all'articolo 22, paragrafo 3, in merito alle proprie decisioni di concedere o ritirare la qualifica, salvo se tale organismo è anche l'organismo di vigilanza;

i) verificare l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nei casi in cui il prestatore di servizi fiduciari qualificati cessa le sue attività, inclusi i modi in cui le informazioni sono mantenute accessibili a norma dell'articolo 24, paragrafo 2, lettera h);

j) imporre ai prestatori di servizi fiduciari di rimediare a qualsiasi mancato adempimento dei requisiti di cui al presente regolamento.

5. Gli Stati membri possono imporre che l'organismo di vigilanza istituisca, mantenga e aggiorni un'infrastruttura fiduciaria secondo le condizioni di cui al diritto nazionale.

6. Entro il 31 marzo di ogni anno, ogni organismo di vigilanza presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile insieme a una sintesi delle notifiche di violazione ricevute da prestatori di servizi fiduciari a norma dell'articolo 19, paragrafo 2.

7. La Commissione mette a disposizione degli Stati membri la relazione annuale di cui al paragrafo 6.

8. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui al paragrafo 6. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 18

Assistenza reciproca

1. Gli organismi di vigilanza collaborano fra loro al fine di scambiarsi buone prassi.

Un organismo di vigilanza, previa ricezione di una richiesta giustificata da parte di un altro organismo di vigilanza, fornisce a quest'ultimo assistenza perché possano svolgere le attività di organismi di vigilanza in modo coerente. L'assistenza reciproca può coprire, in particolare, le richieste di informazioni e le misure di vigilanza, quali richieste di svolgere ispezioni in connessione con le relazioni di valutazione della conformità di cui agli articoli 20 e 21.

2. L'organismo di vigilanza cui è presentata una richiesta di assistenza può rifiutare tale richiesta per uno dei seguenti motivi:

a) l'organismo di vigilanza non è competente a fornire l'assistenza richiesta;

b) l'assistenza richiesta non è proporzionata alle attività di vigilanza dell'organismo di vigilanza svolte a norma dell'articolo 17;

c) fornire l'assistenza richiesta sarebbe incompatibile con il presente regolamento.

3. Ove appropriato, gli Stati membri possono autorizzare i rispettivi organismi di vigilanza a svolgere indagini congiunte con la partecipazione di membri del personale di organismi di vigilanza di altri Stati membri. Le disposizioni e le procedure per tali indagini congiunte sono convenute e stabilite dagli Stati membri interessati conformemente al rispettivo diritto nazionale.

Articolo 19

Requisiti di sicurezza relativi ai prestatori di servizi fiduciari

1. I prestatori di servizi fiduciari qualificati e non qualificati adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali misure assicurano un livello di sicurezza commisurato al grado di rischio esistente. In particolare, sono adottate misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti.
2. Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, i prestatori di servizi fiduciari qualificati e non qualificati notificano all'organismo di vigilanza e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.
Qualora sia probabile che la violazione della sicurezza o la perdita di integrità abbia effetti negativi su una persona fisica o giuridica a cui è stato prestato il servizio fiduciario, il prestatore di servizi fiduciari notifica senza indugio anche alla persona fisica o giuridica la violazione di sicurezza o la perdita di integrità.
Ove appropriato, in particolare qualora la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza notificato ne informa gli organismi di vigilanza negli altri Stati membri interessati e l'ENISA.
L'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico.
3. L'organismo di vigilanza trasmette all'ENISA, una volta all'anno, una sintesi delle notifiche di violazione di sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari.
4. La Commissione può, mediante atti di esecuzione:
a) specificare ulteriormente le misure di cui al paragrafo 1; e
b) definire i formati e le procedure, comprese le scadenze, applicabili ai fini del paragrafo 2.
Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 3

Servizi fiduciari qualificati

Articolo 20

Vigilanza dei prestatori di servizi fiduciari qualificati

1. I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è di confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati soddisfano i requisiti di cui al presente regolamento. I prestatori di servizi fiduciari qualificati presentano la pertinente relazione di valutazione di conformità all'organismo di vigilanza entro il termine di tre giorni lavorativi dalla sua ricezione.
2. Fatto salvo il paragrafo 1, l'organismo di vigilanza può, in qualsiasi momento, condurre una verifica o chiedere a un organismo di valutazione della conformità di eseguire una valutazione di conformità dei prestatori di servizi fiduciari qualificati, a spese di tali prestatori di servizi fiduciari, per confermare che essi e i servizi fiduciari qualificati da essi prestati rispondono ai requisiti di cui al presente regolamento. Laddove siano state rilevate violazioni delle norme di protezione dei dati personali, l'organismo di vigilanza comunica alle autorità di protezione dei dati i risultati delle verifiche.
3. Ove l'organismo di vigilanza imponga al prestatore di servizi fiduciari qualificato di rimediare agli eventuali mancati adempimenti dei requisiti di cui al presente regolamento e ove il prestatore non agisca di conseguenza e, se applicabile, entro un limite di tempo stabilito dall'organismo di vigilanza, quest'ultimo, tenendo conto in particolare della dimensione, della durata e delle conseguenze di tale mancato adempimento, può ritirare la qualifica di tale prestatore o del servizio interessato da esso prestato e informare l'organismo di cui all'articolo 22, paragrafo 3, al fine di aggiornare gli elenchi di fiducia di cui all'articolo 22, paragrafo 1. L'organismo di vigilanza comunica al prestatore di servizi fiduciari qualificato la revoca della sua qualifica o della qualifica del servizio interessato.
4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento per le seguenti norme:

a)accreditamento degli organismi di valutazione della conformità e per la relazione di valutazione di conformità di cui al paragrafo 1;
b)regole in materia di audit in base alle quali gli organismi di valutazione effettueranno le loro valutazioni della conformità dei prestatori di servizi fiduciari qualificati di cui al paragrafo 1.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 21

Avviamento di un servizio fiduciario qualificato

1. Qualora i prestatori di servizi fiduciari, privi di qualifica, intendano avviare la prestazione di servizi fiduciari qualificati, trasmettono all'organismo di vigilanza una notifica della loro intenzione insieme a una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità.
2. L'organismo di vigilanza verifica se il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento e, in particolare, i requisiti per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati da essi prestati.

Se conclude che il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al primo comma, l'organismo di vigilanza concede la qualifica al prestatore di servizi fiduciari e ai servizi fiduciari da esso prestati e informa l'organismo di cui all'articolo 22, paragrafo 3, affinché aggiorni gli elenchi di fiducia di cui all'articolo 22, paragrafo 1, non oltre tre mesi dopo la notifica a norma del paragrafo 1 del presente articolo.

Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

3. I prestatori di servizi fiduciari qualificati possono iniziare a prestare il servizio fiduciario qualificato dopo che la qualifica è stata registrata negli elenchi di fiducia di cui all'articolo 22, paragrafo 1.
4. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 22

Elenchi di fiducia

1. Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia, che includono le informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono responsabili, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati.
2. Gli Stati membri istituiscono, mantengono e pubblicano, in modo sicuro, gli elenchi di fiducia di cui al paragrafo 1, firmati o sigillati elettronicamente in una forma adatta al trattamento automatizzato.
3. Gli Stati membri notificano alla Commissione, senza indugio, informazioni sull'organismo responsabile dell'istituzione, del mantenimento e della pubblicazione degli elenchi nazionali di fiducia, precisando dove gli elenchi sono pubblicati, e sui certificati utilizzati per firmare o sigillare tali elenchi di fiducia e le eventuali modifiche apportate.
4. La Commissione rende pubbliche, attraverso un canale sicuro, le informazioni di cui al paragrafo 3 in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.
5. Entro il 18 settembre 2015, la Commissione, mediante atti di esecuzione, specifica le informazioni di cui al paragrafo 1 e definisce le specifiche tecniche e i formati per gli elenchi di fiducia applicabili ai fini dei paragrafi da 1 a 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 23

Marchio di fiducia UE per i servizi fiduciari qualificati

1. Dopo la registrazione della qualifica di cui all'articolo 21, paragrafo 2, secondo comma, nell'elenco di fiducia di cui all'articolo 22, paragrafo 1, i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.
2. Quando utilizzano il marchio di fiducia UE per i servizi fiduciari qualificati di cui al paragrafo 1, i prestatori di servizi fiduciari qualificati garantiscono che sul loro sito web sia disponibile un link all'elenco di fiducia pertinente.
3. Entro il 1º luglio 2015 la Commissione, mediante atti di esecuzione, fornisce criteri specifici relativi alla forma e, in particolare, alla presentazione, alla composizione, alla dimensione e al disegno del marchio di fiducia UE per i servizi fiduciari qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 24

Requisiti per i prestatori di servizi fiduciari qualificati

1. Allorché rilascia un certificato qualificato per un servizio fiduciario, un prestatore di servizi fiduciari qualificato verifica, mediante mezzi appropriati e conformemente al diritto nazionale, l'identità e, se del caso, eventuali attributi specifici della persona fisica o giuridica a cui il certificato qualificato è rilasciato.
Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato direttamente o ricorrendo a un terzo conformemente al diritto nazionale:

a) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica; o
b) a distanza, mediante mezzi di identificazione elettronica, con cui prima del rilascio del certificato qualificato è stata garantita una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisfano i requisiti fissati all'articolo 8 riguardo ai livelli di garanzia «significativo» o «elevato»; o
c) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato a norma della lettera a) o b); o
d) mediante altri metodi di identificazione riconosciuti a livello nazionale che forniscono una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica. La garanzia equivalente è confermata da un organismo di valutazione della conformità.

2. Un prestatore di servizi fiduciari qualificato che presta servizi fiduciari qualificati:

a) informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;
b) impiega personale e, ove applicabile, subcontraenti dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che hanno ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e applica procedure amministrative e gestionali, che corrispondono a norme europee o internazionali;
c) riguardo alla responsabilità civile per danni a norma dell'articolo 13, mantiene risorse finanziarie adeguate e/o si procura un'assicurazione di responsabilità civile appropriata, conformemente al diritto nazionale;
d) prima di avviare una relazione contrattuale informa, in modo chiaro e completo, chiunque intenda utilizzare un servizio fiduciario qualificato dei termini e delle condizioni esatte per l'utilizzo di tale servizio, comprese eventuali limitazioni del suo utilizzo;
e) utilizza sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi che assicurano;
f) utilizza sistemi affidabili per memorizzare i dati a esso forniti, in modo verificabile, affinché:
   i) siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati fanno riferimento;
   ii) soltanto le persone autorizzate possano effettuare inserimenti e modifiche ai dati memorizzati;
   iii) l'autenticità dei dati sia verificabile;
g) adotta misure adeguate contro le falsificazioni e i furti di dati;
h) registra e mantiene accessibili per un congruo periodo di tempo, anche dopo la cessazione delle attività del prestatore di servizi fiduciari qualificato, tutte le informazioni pertinenti relative a dati rilasciati e ricevuti dal prestatore di servizi fiduciari qualificato, in particolare a fini di produzione di prove nell'ambito di procedimenti giudiziali e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;
i) dispone di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni verificate dall'organismo di vigilanza a norma dell'articolo 17, paragrafo 4, lettera i);
j) garantisce il trattamento lecito dei dati personali a norma della direttiva 95/46/CE;
k) se i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati, istituiscono una banca dati dei certificati aggiornata.

3. Se un prestatore di servizi fiduciari qualificato che rilascia certificati qualificati decide di revocare un certificato, registra tale revoca nella propria banca dati dei certificati e pubblica la situazione di revoca del certificato tempestivamente e, in ogni caso, entro 24 ore dal ricevimento della richiesta. La revoca diventa immediatamente effettiva all'atto della pubblicazione.

4. In considerazione del paragrafo 3, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati trasmettono alle parti facenti affidamento sulla certificazione informazioni sulla situazione di validità o revoca dei certificati qualificati da essi rilasciati. Queste informazioni sono rese disponibili almeno per ogni certificato rilasciato in qualsiasi momento e oltre il periodo di validità del certificato, in modo automatizzato, affidabile, gratuito ed efficiente.

5. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sistemi e prodotti affidabili, che soddisfano i requisiti di cui al paragrafo 2, lettere e) ed f), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati ove i sistemi e i prodotti affidabili adempiano a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 4

Firme elettroniche

Articolo 25

Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Articolo 26

Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

a) è connessa unicamente al firmatario;
b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Articolo 27

Firme elettroniche nei servizi pubblici

1. Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato di firma elettronica e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
2. Se uno Stato membro richiede una firma elettronica avanzata basata su un certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate basate su un certificato qualificato e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.
3. Gli Stati membri non richiedono, per un utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, una firma elettronica dotata di un livello di garanzia di sicurezza più elevato di quello della firma elettronica qualificata.
4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alle firme elettroniche avanzate. Si presume che i requisiti per le firme elettroniche avanzate di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 26, siano rispettati ove una firma elettronica avanzata soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.
5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento delle firme elettroniche avanzate o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 28

Certificati qualificati di firme elettroniche

1. I certificati qualificati di firme elettroniche soddisfano i requisiti di cui all'allegato I.
2. I certificati qualificati di firme elettroniche non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato I.
3. I certificati qualificati di firme elettroniche possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento delle firme elettroniche qualificate.

4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.
5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:
a)in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;
b)il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.
6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di firma elettronica. Si presume che i requisiti di cui all'allegato I siano stati rispettati ove un certificato qualificato di firma elettronica risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 29

Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata soddisfano i requisiti di cui all'allegato II.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai dispositivi per la creazione di una firma elettronica qualificata. Si presume che i requisiti di cui all'allegato II siano stati rispettati ove un dispositivo per la creazione di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 30

Certificazione dei dispositivi per la creazione di una firma elettronica qualificata

1. La conformità dei dispositivi per la creazione di una firma elettronica qualificata con i requisiti stabiliti all'allegato II è certificata da appropriati organismi pubblici o privati designati dagli Stati membri.
2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dell'organismo pubblico o privato di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.
3. La certificazione di cui al paragrafo 1 si basa su uno dei seguenti elementi:
a)un processo di valutazione di sicurezza condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici incluse nell'elenco redatto conformemente al secondo comma; o
b)un processo diverso da quello di cui alla lettera a), a condizione che utilizzi livelli di sicurezza comparabili e che l'organismo pubblico o privato di cui al paragrafo 1 notifichi tale processo alla Commissione. Detto processo può essere utilizzato solo in assenza delle norme di cui alla lettera a) ovvero quando è in corso un processo di valutazione di sicurezza di cui alla lettera a).

La Commissione adotta, mediante atti di esecuzione, un elenco di norme per la valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui alla lettera a). Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 48, paragrafo 2.
4. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 47 riguardo alla fissazione di criteri specifici che gli organismi designati di cui al paragrafo 1 del presente articolo devono soddisfare.

Articolo 31

Pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati

1. Gli Stati membri notificano alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la conclusione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica qualificata certificati dagli organismi di cui all'articolo 30, paragrafo 1. Essi notificano inoltre alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la cancellazione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica che non sono più certificati.
2. Sulla base delle informazioni pervenutele, la Commissione redige, pubblica e mantiene un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati.
3. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure applicabili ai fini del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 32

Requisiti per la convalida delle firme elettroniche qualificate

1. Il processo di convalida di una firma elettronica qualificata conferma la validità di una firma elettronica qualificata purché:

a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I;

b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma;

c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione;

d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;

e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma;

f) la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata;

g) l'integrità dei dati firmati non sia stata compromessa;

h) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma;

2. Il sistema utilizzato per convalidare la firma elettronica qualificata fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consente di rilevare eventuali questioni attinenti alla sicurezza.

3. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alla convalida delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove la convalida delle firme elettroniche qualificate risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 33

Servizio di convalida qualificato delle firme elettroniche qualificate

1. Un servizio di convalida qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che:

a) fornisce la convalida a norma dell'articolo 32, paragrafo 1; e

b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di convalida qualificato di cui al paragrafo 1. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il servizio di convalida di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 34

Servizio di conservazione qualificato delle firme elettroniche qualificate

1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 5

Sigilli elettronici

Articolo 35

Effetti giuridici dei sigilli elettronici

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

3. Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

Articolo 36

Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Articolo 37

Sigilli elettronici nei servizi pubblici

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.

4. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati. Si presume che i requisiti per i sigilli elettronici avanzati di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 36 siano rispettati ove un sigillo elettronico avanzato soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 38

Certificati qualificati di sigilli elettronici

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.

2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.

3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.

4. Qualora un certificato qualificato di un sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea dei certificati qualificati di sigilli elettronici:

a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

6. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 39

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.
3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

Articolo 40

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.

SEZIONE 6

Validazione temporale elettronica

Articolo 41

Effetti giuridici della validazione temporale elettronica

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.
2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.
3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Articolo 42

Requisiti per la validazione temporale elettronica qualificata

1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:
a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;
b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e
c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 7

Servizi elettronici di recapito certificato

Articolo 43

Effetti giuridici di un servizio elettronico di recapito certificato

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.
2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Articolo 44

Requisiti per i servizi elettronici di recapito certificato qualificati

1. I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:
a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;
b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;
c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;
d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;
e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di invio e ricezione dei dati. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

SEZIONE 8

Autenticazione dei siti web

Articolo 45

Requisiti per i certificati qualificati di autenticazione di siti web

1. I certificati qualificati di autenticazione di siti web soddisfano i requisiti di cui all'allegato IV.
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di autenticazione di siti web. Si presume che i requisiti di cui all'allegato IV siano stati rispettati ove un certificato qualificato di autenticazione di sito web risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

CAPO IV

DOCUMENTI ELETTRONICI

Articolo 46

Effetti giuridici dei documenti elettronici

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

CAPO V

DELEGA DI POTERE E DISPOSIZIONI DI ESECUZIONE

Articolo 47

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
2. Il potere di adottare gli atti delegati di cui all'articolo 30, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 17 settembre 2014.
3. La delega di potere di cui all'articolo 30, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
5. L'atto delegato adottato ai sensi dell'articolo 30, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 48

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

CAPO VI

DISPOSIZIONI FINALI

Articolo 49

Riesame

La Commissione riesamina l'applicazione del presente regolamento e presenta una relazione in proposito al Parlamento europeo e al Consiglio entro il 1º luglio 2020. La Commissione valuta in particolare se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche,

compresi l'articolo 6, l'articolo 7, lettera f), e gli articoli 34, 43, 44 e 45, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici.

La relazione di cui al primo comma è corredata, se necessario, di proposte legislative.

Ogni quattro anni dopo la relazione di cui al primo paragrafo la Commissione presenta inoltre al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nella realizzazione degli obiettivi del presente regolamento.

Articolo 50

Abrogazione

1. La direttiva 1999/93/CEE è abrogata con effetto dal 1º luglio 2016.
2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento.

Articolo 51

Disposizioni transitorie

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento.
2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE sono considerati certificati qualificati di firma elettronica a norma del presente regolamento fino alla loro scadenza.
3. Un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE presenta una relazione di valutazione della conformità all'organismo di vigilanza quanto prima e, comunque, non oltre il 1º luglio 2017. Fino alla presentazione della suddetta relazione di valutazione della conformità e fino a che l'organismo di vigilanza non ne abbia completato la valutazione, il prestatore di servizi di certificazione è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento.
4. Se un prestatore di servizi di certificazione che rilascia certificati qualificati a norma della direttiva 1999/93/CE non presenta una relazione di valutazione della conformità all'organismo di vigilanza entro i termini di cui al paragrafo 3, egli non è considerato un prestatore di servizi fiduciari qualificato a norma del presente regolamento a decorrere dal 2 luglio 2017.

Articolo 52

Entrata in vigore

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.
2. Il presente regolamento si applica a decorrere dal 1º luglio 2016, a eccezione delle seguenti disposizioni:

a) articolo 8, paragrafo 3, articolo 9, paragrafo 5, articolo 12, paragrafi da 2 a 9, articolo 17, paragrafo 8, articolo 19, paragrafo 4, articolo 20, paragrafo 4, articolo 21, paragrafo 4, articolo 22, paragrafo 5, articolo 23, paragrafo 3, articolo 24, paragrafo 5, articolo 27, paragrafi 4 e 5, articolo 28, paragrafo 6, articolo 29, paragrafo 2, articolo 30, paragrafi 3 e 4, articolo 31, paragrafo 3, articolo 32, paragrafo 3, articolo 33, paragrafo 2, articolo 34, paragrafo 2, articolo 37, paragrafi 4 e 5, articolo 38, paragrafo 6, articolo 42, paragrafo 2, articolo 44, paragrafo 2, articolo 45, paragrafo 2, articolo 47 e articolo 48, che si applicano dal 17 settembre 2014;

b) l'articolo 7, l'articolo 8, paragrafi 1 e 2, gli articoli 9, 10, 11 e l'articolo 12, paragrafo 1, si applicano a decorrere dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8;

c) l'articolo 6 si applica a decorrere da tre anni dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8.

3. Quando il regime di identificazione elettronica notificato è compreso nell'elenco pubblicato dalla Commissione ai sensi dell'articolo 9 prima della data di cui al paragrafo 2, lettera c), del presente articolo, il riconoscimento dei mezzi di identificazione elettronica in virtù di tale regime ai sensi dell'articolo 6 ha luogo non oltre 12 mesi dopo la pubblicazione di detto regime ma non prima della data di cui al paragrafo 2, lettera c), del presente articolo.
4. Nonostante il paragrafo 2, lettera c), del presente articolo, uno Stato membro può decidere che i mezzi di identificazione elettronica a norma del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, da un altro Stato membro, siano riconosciuti nel primo Stato membro a decorrere dalla data di pubblicazione degli atti di esecuzione di cui agli articoli 8, paragrafo 3, e 12, paragrafo 8. Gli Stati membri interessati ne informano la Commissione. La Commissione rende pubbliche tali informazioni.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Decreto Legge 12 settembre 2014, n. 132, coordinato con la Legge di conversione 10 novembre 2014, n. 162 - Misure urgenti di degiurisdizionalizzazione ed altri interventi per la definizione dell'arretrato in materia di processo civile (ESTRATTO).

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

(omissis)

Art. 18

Iscrizione a ruolo del processo esecutivo per espropriazione

1. Al libro terzo del codice di procedura civile sono apportate le seguenti modificazioni:

a) l'articolo 518, sesto comma, è sostituito dal seguente:

«Compiute le operazioni, l'ufficiale giudiziario consegna senza ritardo al creditore il processo verbale, il titolo esecutivo e il precetto. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi degli atti di cui al periodo precedente, entro quindici giorni dalla consegna. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il cancelliere al momento del deposito forma il fascicolo dell'esecuzione. Sino alla scadenza del termine di cui all'articolo 497 copia del processo verbale è conservata dall'ufficiale giudiziario a disposizione del debitore. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie degli atti di cui al primo periodo del presente comma sono depositate oltre il termine di quindici giorni dalla consegna al creditore.»;

b) l'articolo 543, quarto comma, è sostituito dal seguente:

«Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'originale dell'atto di citazione. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi dell'atto di citazione, del titolo esecutivo e del precetto, entro trenta giorni dalla consegna. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il cancelliere al momento del deposito forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie degli atti di cui al secondo periodo sono depositate oltre il termine di trenta giorni dalla consegna al creditore.»;

c) l'articolo 557 è sostituito dal seguente:

«Art. 557 (Deposito dell'atto di pignoramento). - Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'atto di pignoramento e la nota di trascrizione restituitagli dal conservatore dei registri immobiliari. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi del titolo esecutivo, del precetto, dell'atto di pignoramento e della nota di trascrizione entro quindici giorni dalla consegna dell'atto di pignoramento.

Nell'ipotesi di cui all'articolo 555, ultimo comma, il creditore deve depositare la nota di trascrizione appena restituitagli dal conservatore dei registri immobiliari.

Il cancelliere forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie dell'atto di pignoramento, del titolo esecutivo e del precetto sono depositate oltre il termine di quindici giorni dalla consegna al creditore.».

2. Alle disposizioni per l'attuazione del codice di procedura civile, dopo l'articolo 159 è inserito il seguente:

«Art. 159-bis (Nota d'iscrizione a ruolo del processo esecutivo per espropriazione). - La nota d'iscrizione a ruolo del processo esecutivo per espropriazione deve in ogni caso contenere l'indicazione delle parti, nonché le generalità e il codice fiscale, ove attribuito, della parte che iscrive la causa a ruolo, del difensore, della cosa o del bene oggetto di pignoramento. Il Ministro della giustizia, con proprio decreto avente natura non regolamentare, può indicare ulteriori dati da inserire nella nota di iscrizione a ruolo.».

2-bis. Alle disposizioni per l'attuazione del codice di procedura civile, dopo l'articolo 164-bis, introdotto dall'articolo 19, comma 2, lettera b), del presente decreto, è inserito il seguente:

"Art. 164-ter. - (Inefficacia del pignoramento per mancato deposito della nota di iscrizione a ruolo). - Quando il pignoramento è divenuto inefficace per mancato deposito della nota di iscrizione a ruolo nel termine stabilito, il creditore entro cinque giorni dalla scadenza del termine ne fa dichiarazione al debitore e all'eventuale terzo, mediante atto notificato. In ogni caso ogni obbligo del debitore e del terzo cessa quando la nota di iscrizione a ruolo non è stata depositata nei termini di legge.

La cancellazione della trascrizione del pignoramento si esegue quando è ordinata giudizialmente ovvero quando il creditore pignorante dichiara, nelle forme richieste dalla legge, che il pignoramento è divenuto inefficace per mancato deposito della nota di iscrizione a ruolo nel termine stabilito.".

3. Le disposizioni di cui ai commi 1, 2 e 2-bis si applicano ai procedimenti esecutivi iniziati a decorrere dal trentesimo giorno successivo all'entrata in vigore della legge di conversione del presente decreto-legge.
4. All'articolo 16-bis, comma 2, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono aggiunti, in fine, i seguenti periodi:
(omissis)[75]

Art. 19.
Misure per l'efficienza e la semplificazione del processo esecutivo

1. Al codice di procedura civile sono apportate le seguenti modificazioni:
a) all'articolo 26, il secondo comma è sostituito dal seguente: "Per l'esecuzione forzata su autoveicoli, motoveicoli e rimorchi è competente il giudice del luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede";
b) dopo l'articolo 26 è inserito il seguente:
«Art. 26-bis (Foro relativo all'espropriazione forzata di crediti). - Quando il debitore è una delle pubbliche amministrazioni indicate dall'articolo 413, quinto comma, per l'espropriazione forzata di crediti è competente, salvo quanto disposto dalle leggi speciali, il giudice del luogo dove il terzo debitore ha la residenza, il domicilio, la dimora o la sede.
Fuori dei casi di cui al primo comma, per l'espropriazione forzata di crediti è competente il giudice del luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede.»;
c) all'articolo 492 sono apportate le seguenti modificazioni:
1) il settimo comma è abrogato;
2) all'ottavo comma, le parole «negli stessi casi di cui al settimo comma e» sono soppresse;
d) dopo l'articolo 492 è inserito il seguente:
«Art. 492-bis (Ricerca con modalità telematiche dei beni da pignorare). - Su istanza del creditore procedente, il presidente del tribunale del luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede, verificato il diritto della parte istante a procedere ad esecuzione forzata, autorizza la ricerca con modalità telematiche dei beni da pignorare. L'istanza deve contenere l'indicazione dell'indirizzo di posta elettronica ordinaria ed il numero di fax del difensore nonché, ai fini dell'articolo 547, dell'indirizzo di posta elettronica certificata.
Fermo quanto previsto dalle disposizioni in materia di accesso ai dati e alle informazioni degli archivi automatizzati del Centro elaborazione dati istituito presso il Ministero dell'interno ai sensi dell'articolo 8 della legge 1° aprile 1981, n. 121, con l'autorizzazione di cui al primo comma il presidente del tribunale o un giudice da lui delegato dispone che l'ufficiale giudiziario acceda mediante collegamento telematico diretto ai dati contenuti nelle banche dati delle pubbliche amministrazioni o alle quali le stesse possono accedere e, in particolare, nell'anagrafe tributaria, compreso l'archivio dei rapporti finanziari, nel pubblico registro automobilistico e in quelle degli enti previdenziali, per l'acquisizione di tutte le informazioni rilevanti per l'individuazione di cose e crediti da sottoporre ad esecuzione, comprese quelle relative ai rapporti intrattenuti dal debitore con istituti di credito e datori di lavoro o committenti. Terminate le operazioni l'ufficiale giudiziario redige un unico processo verbale nel quale indica tutte le banche dati interrogate e le relative risultanze.
Se l'accesso ha consentito di individuare cose che si trovano in luoghi appartenenti al debitore compresi nel territorio di competenza dell'ufficiale giudiziario, quest'ultimo accede agli stessi per provvedere d'ufficio agli adempimenti di cui agli articoli 517, 518 e 520. Se i luoghi non sono compresi nel territorio di competenza di cui al periodo precedente, copia autentica del verbale è rilasciata al creditore che, entro quindici giorni dal rilascio a pena d'inefficacia della richiesta, la presenta, unitamente all'istanza per gli adempimenti di cui agli articoli 517, 518 e 520, all'ufficiale giudiziario territorialmente competente.
L'ufficiale giudiziario, quando non rinviene una cosa individuata mediante l'accesso nelle banche dati di cui al secondo comma, intima al debitore di indicare entro quindici giorni il luogo in cui si trova, avvertendolo che l'omessa o la falsa comunicazione è punita a norma dell'articolo 388, sesto comma, del codice penale.
Se l'accesso ha consentito di individuare crediti del debitore o cose di quest'ultimo che sono nella disponibilità di terzi, l'ufficiale giudiziario notifica d'ufficio, ove possibile a norma dell'articolo 149-bis o a mezzo telefax, al debitore e al terzo il verbale, che dovrà anche contenere l'indicazione del credito per cui si procede, del titolo esecutivo e del precetto, dell'indirizzo di posta elettronica certificata di cui al primo comma, del luogo in cui il creditore ha eletto domicilio o ha dichiarato di essere residente,

[75] Cfr.: art. 16bis d.l. 179/2012 come modificato da questo articolo.

dell'ingiunzione, dell'invito e dell'avvertimento al debitore di cui all'articolo 492, primo, secondo e terzo comma, nonché l'intimazione al terzo di non disporre delle cose o delle somme dovute, nei limiti di cui all'articolo 546. Il verbale di cui al presente comma è notificato al terzo per estratto, contenente esclusivamente i dati a quest'ultimo riferibili.
Quando l'accesso ha consentito di individuare più crediti del debitore o piu' cose di quest'ultimo che sono nella disponibilità di terzi l'ufficiale giudiziario sottopone ad esecuzione i beni scelti dal creditore.
Quando l'accesso ha consentito di individuare sia cose di cui al terzo comma che crediti o cose di cui al quinto comma, l'ufficiale giudiziario sottopone ad esecuzione i beni scelti dal creditore.»;
d-bis) all'articolo 503 è aggiunto, in fine, il seguente comma:
"L'incanto può essere disposto solo quando il giudice ritiene probabile che la vendita con tale modalità abbia luogo ad un prezzo superiore della metà rispetto al valore del bene, determinato a norma dell'articolo 568";
d-ter) dopo l'articolo 521 è inserito il seguente:
"Art. 521-bis. - (Pignoramento e custodia di autoveicoli, motoveicoli e rimorchi). - Il pignoramento di autoveicoli, motoveicoli e rimorchi si esegue mediante notificazione al debitore e successiva trascrizione di un atto nel quale si indicano esattamente, con gli estremi richiesti dalla legge speciale per la loro iscrizione nei pubblici registri, i beni e i diritti che si intendono sottoporre ad esecuzione, e gli si fa l'ingiunzione prevista nell'articolo 492.
Il pignoramento contiene altresì l'intimazione a consegnare entro dieci giorni i beni pignorati, nonché i titoli e i documenti relativi alla proprietà e all'uso dei medesimi, all'istituto vendite giudiziarie autorizzato ad operare nel territorio del circondario nel quale è compreso il luogo in cui il debitore ha la residenza, il domicilio, la dimora o la sede. Col pignoramento il debitore è costituito custode dei beni pignorati e di tutti gli accessori comprese le pertinenze e i frutti, senza diritto a compenso. Al momento della consegna l'istituto vendite giudiziarie assume la custodia del bene pignorato e ne dà immediata comunicazione al creditore pignorante, a mezzo posta elettronica certificata ove possibile. Decorso il termine di cui al primo comma, gli organi di polizia che accertano la circolazione dei beni pignorati procedono al ritiro della carta di circolazione nonché, ove possibile, dei titoli e dei documenti relativi alla proprietà e all'uso dei beni pignorati e consegnano il bene pignorato all'istituto vendite giudiziarie autorizzato ad operare nel territorio del circondario nel quale è compreso il luogo in cui il bene pignorato è stato rinvenuto. Si applica il terzo comma. Eseguita l'ultima notificazione, l'ufficiale giudiziario consegna senza ritardo al creditore l'atto di pignoramento perché proceda alla trascrizione nei pubblici registri.
Entro trenta giorni dalla comunicazione di cui al terzo comma, il creditore deve depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, con copie conformi del titolo esecutivo, del precetto, dell'atto di pignoramento e della nota di trascrizione. La conformità di tali copie è attestata dall'avvocato del creditore ai soli fini del presente articolo. Il cancelliere forma il fascicolo dell'esecuzione. Il pignoramento perde efficacia quando la nota di iscrizione a ruolo e le copie dell'atto di pignoramento, del titolo esecutivo e del precetto sono depositate oltre il termine di cui al quinto comma. Si applicano in quanto compatibili le disposizioni del presente capo";
e) all'articolo 543 sono apportate le seguenti modificazioni:
1) al primo comma, la parola "personalmente" è soppressa;
2) al secondo comma, il numero 4) è sostituito dal seguente:
«4) la citazione del debitore a comparire davanti al giudice competente, con l'invito al terzo a comunicare la dichiarazione di cui all'articolo 547 al creditore procedente entro dieci giorni a mezzo raccomandata ovvero a mezzo di posta elettronica certificata; con l'avvertimento al terzo che in caso di mancata comunicazione della dichiarazione, la stessa dovrà essere resa dal terzo comparendo in un'apposita udienza e che quando il terzo non compare o, sebbene comparso, non rende la dichiarazione, il credito pignorato o il possesso di cose di appartenenza del debitore, nell'ammontare o nei termini indicati dal creditore, si considereranno non contestati ai fini del procedimento in corso e dell'esecuzione fondata sul provvedimento di assegnazione»;
3) dopo il quarto comma è inserito il seguente:
«Quando procede a norma dell'articolo 492-bis, l'ufficiale giudiziario consegna senza ritardo al creditore il verbale, il titolo esecutivo ed il precetto, e si applicano le disposizioni di cui al quarto comma. Decorso il termine di cui all'articolo 501, il creditore pignorante e ognuno dei creditori intervenuti muniti di titolo esecutivo possono chiedere l'assegnazione o la vendita delle cose mobili o l'assegnazione dei crediti. Sull'istanza di cui al periodo precedente il giudice fissa l'udienza per l'audizione del creditore e del debitore e provvede a norma degli articoli 552 o 553.
Il decreto con cui viene fissata l'udienza di cui al periodo precedente è notificato a cura del creditore procedente e deve contenere l'invito e l'avvertimento al terzo di cui al numero 4) del secondo comma.»;

f) all'articolo 547, il primo comma è sostituito dal seguente:
«Con dichiarazione a mezzo raccomandata inviata al creditore procedente o trasmessa a mezzo di posta elettronica certificata, il terzo, personalmente o a mezzo di procuratore speciale o del difensore munito di procura speciale, deve specificare di quali cose o di quali somme è debitore o si trova in possesso e quando ne deve eseguire il pagamento o la consegna.»;
g) all'articolo 548, sono apportate le seguenti modificazioni:
1) il primo comma è abrogato;
2) il secondo comma è sostituito dal seguente:
«Quando all'udienza il creditore dichiara di non aver ricevuto la dichiarazione, il giudice, con ordinanza, fissa un'udienza successiva. L'ordinanza è notificata al terzo almeno dieci giorni prima della nuova udienza. Se questi non compare alla nuova udienza o, comparendo, rifiuta di fare la dichiarazione, il credito pignorato o il possesso del bene di appartenenza del debitore, nei termini indicati dal creditore, si considera non contestato ai fini del procedimento in corso e dell'esecuzione fondata sul provvedimento di assegnazione e il giudice provvede a norma degli articoli 552 o 553.»;
h) (Soppressa);
h-bis) all'articolo 569, terzo comma, il secondo periodo è sostituito dai seguenti: "Il giudice con la medesima ordinanza stabilisce le modalità con cui deve essere prestata la cauzione e fissa, al giorno successivo alla scadenza del termine, l'udienza per la deliberazione sull'offerta e per la gara tra gli offerenti di cui all'articolo 573. Il giudice provvede ai sensi dell'articolo 576 solo quando ritiene probabile che la vendita con tale modalità possa aver luogo ad un prezzo superiore della metà rispetto al valore del bene, determinato a norma dell'articolo 568";
h-ter) all'articolo 572, terzo comma, il primo periodo è sostituito dal seguente: "Se l'offerta è inferiore a tale valore il giudice non può far luogo alla vendita quando ritiene probabile che la vendita con il sistema dell'incanto possa aver luogo ad un prezzo superiore della metà rispetto al valore del bene determinato a norma dell'articolo 568";
i) l'articolo 609 è sostituito dal seguente:
«Art. 609 (Provvedimenti circa i mobili estranei all'esecuzione). – Quando nell'immobile si trovano beni mobili che non debbono essere consegnati, l'ufficiale giudiziario intima alla parte tenuta al rilascio ovvero a colui al quale gli stessi risultano appartenere di asportarli, assegnandogli il relativo termine. Dell'intimazione si dà atto a verbale ovvero, se colui che è tenuto a provvedere all'asporto non è presente, mediante atto notificato a spese della parte istante. Quando entro il termine assegnato l'asporto non è stato eseguito l'ufficiale giudiziario, su richiesta e a spese della parte istante, determina, anche a norma dell'articolo 518, primo comma, il presumibile valore di realizzo dei beni ed indica le prevedibili spese di custodia e di asporto.
Quando può ritenersi che il valore dei beni è superiore alle spese di custodia e di asporto, l'ufficiale giudiziario, a spese della parte istante, nomina un custode e lo incarica di trasportare i beni in altro luogo. Il custode è nominato a norma dell'articolo 559. In difetto di istanza e di pagamento anticipato delle spese i beni, quando non appare evidente l'utilità del tentativo di vendita di cui al quinto comma, sono considerati abbandonati e l'ufficiale giudiziario, salva diversa richiesta della parte istante, ne dispone lo smaltimento o la distruzione.
Se sono rinvenuti documenti inerenti lo svolgimento di attività imprenditoriale o professionale che non sono stati asportati a norma del primo comma, gli stessi sono conservati, per un periodo di due anni, dalla parte istante ovvero, su istanza e previa anticipazione delle spese da parte di quest'ultima, da un custode nominato dall'ufficiale giudiziario. In difetto di istanza e di pagamento anticipato delle spese si applica, in quanto compatibile, quanto previsto dal secondo comma, ultimo periodo. Allo stesso modo si procede alla scadenza del termine biennale di cui al presente comma a cura della parte istante o del custode.
Decorso il termine fissato nell'intimazione di cui al primo comma, colui al quale i beni appartengono può, prima della vendita ovvero dello smaltimento o distruzione dei beni a norma del secondo comma, ultimo periodo, chiederne la consegna al giudice dell'esecuzione per il rilascio. Il giudice provvede con decreto e, quando accoglie l'istanza, dispone la riconsegna previa corresponsione delle spese e compensi per la custodia e per l'asporto.
Il custode provvede alla vendita senza incanto nelle forme previste per la vendita dei beni mobili pignorati, secondo le modalità disposte dal giudice dell'esecuzione per il rilascio. Si applicano, in quanto compatibili, gli articoli 530 e seguenti del codice di procedura civile. La somma ricavata è impiegata per il pagamento delle spese e dei compensi per la custodia, per l'asporto e per la vendita, liquidate dal giudice dell'esecuzione per il rilascio. Salvo che i beni appartengano ad un soggetto diverso da colui che è tenuto al rilascio, l'eventuale eccedenza è utilizzata per il pagamento delle spese di esecuzione liquidate a norma dell'articolo 611.

In caso di infruttuosità della vendita nei termini fissati dal giudice dell'esecuzione, si procede a norma del secondo comma, ultimo periodo.
Se le cose sono pignorate o sequestrate, l'ufficiale giudiziario dà immediatamente notizia dell'avvenuto rilascio al creditore su istanza del quale fu eseguito il pignoramento o il sequestro, e al giudice dell'esecuzione per l'eventuale sostituzione del custode.».
2. Alle disposizioni per l'attuazione al codice di procedura civile, di cui al regio decreto 18 dicembre 1941, n. 1368, sono apportate le seguenti modificazioni:
a) dopo l'articolo 155 sono inseriti i seguenti:
«Art. 155-bis (Archivio dei rapporti finanziari). - Per archivio dei rapporti finanziari di cui all'articolo 492-bis, secondo comma, del codice si intende la sezione di cui all'articolo 7, sesto comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605.
Art. 155-ter (Partecipazione del creditore alla ricerca dei beni da pignorare con modalità telematiche). - La partecipazione del creditore alla ricerca dei beni da pignorare di cui all'articolo 492-bis del codice ha luogo a norma dell'articolo 165 di queste disposizioni.
Nei casi di cui all'articolo 492-bis, sesto e settimo comma, l'ufficiale giudiziario, terminate le operazioni di ricerca dei beni con modalità telematiche, comunica al creditore le banche dati interrogate e le informazioni dalle stesse risultanti a mezzo telefax o posta elettronica anche non certificata, dandone atto a verbale. Il creditore entro dieci giorni dalla comunicazione indica all'ufficiale giudiziario i beni da sottoporre ad esecuzione; in mancanza la richiesta di pignoramento perde efficacia.
Art. 155-quater (Modalità di accesso alle banche dati). - Con decreto del Ministro della giustizia, di concerto con il Ministro dell'interno e con il Ministro dell'economia e delle finanze e sentito il Garante per la protezione dei dati personali, sono individuati i casi, i limiti e le modalità di esercizio della facoltà di accesso alle banche dati di cui al secondo comma dell'articolo 492-bis del codice, nonché le modalità di trattamento e conservazione dei dati e le cautele a tutela della riservatezza dei debitori. Con il medesimo decreto sono individuate le ulteriori banche dati delle pubbliche amministrazioni o alle quali le stesse possono accedere, che l'ufficiale giudiziario può interrogare tramite collegamento telematico diretto o mediante richiesta al titolare dei dati.
Il Ministro della giustizia può procedere al trattamento dei dati acquisiti senza provvedere all'informativa di cui all'articolo 13 del decreto legislativo 30 giugno 2003, n. 196.
È istituito, presso ogni ufficio notifiche, esecuzioni e protesti, il registro cronologico denominato "Modello ricerca beni", conforme al modello adottato con il decreto del Ministro della giustizia di cui al primo comma.
L'accesso da parte dell'ufficiale giudiziario alle banche dati di cui all'articolo 492-bis del codice e a quelle individuate con il decreto di cui al primo comma è gratuito. La disposizione di cui al periodo precedente si applica anche all'accesso effettuato a norma dell'articolo 155-quinquies di queste disposizioni.
Art. 155-quinquies (Accesso alle banche dati tramite i gestori). - Quando le strutture tecnologiche, necessarie a consentire l'accesso diretto da parte dell'ufficiale giudiziario alle banche dati di cui all'articolo 492-bis del codice e a quelle individuate con il decreto di cui all'articolo 155-quater, primo comma, non sono funzionanti, il creditore procedente, previa autorizzazione a norma dell'articolo 492-bis, primo comma, del codice, può ottenere dai gestori delle banche dati previste dal predetto articolo e dall'articolo 155-quater di queste disposizioni le informazioni nelle stesse contenute.»;
Art. 155-sexies. - (Ulteriori casi di applicazione delle disposizioni per la ricerca con modalità telematiche dei beni da pignorare). - Le disposizioni in materia di ricerca con modalità telematiche dei beni da pignorare si applicano anche per l'esecuzione del sequestro conservativo e per la ricostruzione dell'attivo e del passivo nell'ambito di procedure concorsuali di procedimenti in materia di famiglia e di quelli relativi alla gestione di patrimoni altrui ;
b) al titolo IV, capo I, dopo l'articolo 164 è aggiunto il seguente:
«Art. 164-bis (Infruttuosità dell'espropriazione forzata). – Quando risulta che non è piu' possibile conseguire un ragionevole soddisfacimento delle pretese dei creditori, anche tenuto conto dei costi necessari per la prosecuzione della procedura, delle probabilità di liquidazione del bene e del presumibile valore di realizzo, è disposta la chiusura anticipata del processo esecutivo.».
3. Al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, sono apportate le seguenti modificazioni:
a) all'articolo 13, dopo il comma 1-quater è inserito il seguente:
«1-quinquies. Per il procedimento introdotto con l'istanza di cui all'articolo 492-bis, primo comma, del codice di procedura civile il contributo dovuto è pari ad euro 43 e non si applica l'articolo 30»;
b) all'articolo 14, dopo il comma 1, è aggiunto il seguente:

«1-bis. La parte che fa istanza a norma dell'articolo 492-bis, primo comma, del codice di procedura civile è tenuta al pagamento contestuale del contributo unificato.».
4. Al decreto del Presidente della Repubblica 15 dicembre 1959, n. 1229, sono apportate le seguenti modificazioni:
a) all'articolo 107, secondo comma, dopo le parole «sono addetti» sono aggiunte le seguenti:
«, del verbale di cui all'articolo 492-bis del codice di procedura civile»;
b) all'articolo 122, dopo il primo comma, sono aggiunti i seguenti:
«Quando si procede alle operazioni di pignoramento presso terzi a norma dell'articolo 492-bis del codice di procedura civile o di pignoramento mobiliare, gli ufficiali giudiziari sono retribuiti mediante un ulteriore compenso, che rientra tra le spese di esecuzione ed è dimezzato nel caso in cui le operazioni non vengano effettuate entro quindici giorni dalla richiesta, stabilito dal giudice dell'esecuzione:
a) in una percentuale del 5 per cento sul valore di assegnazione o sul ricavato della vendita dei beni mobili pignorati fino ad euro 10.000,00, in una percentuale del 2 per cento sul ricavato della vendita o sul valore di assegnazione dei beni mobili pignorati da euro 10.001,00 fino ad euro 25.000,00 e in una percentuale del 1 per cento sull'importo superiore;
b) in una percentuale del 6 per cento sul ricavato della vendita o sul valore di assegnazione dei beni e dei crediti pignorati ai sensi degli articoli 492-bis del codice di procedura civile fino ad euro 10.000,00, in una percentuale del 4 per cento sul ricavato della vendita o sul valore di assegnazione dei beni e dei crediti pignorati da euro 10.001,00 fino ad euro 25.000,00 ed in una percentuale del 3 per cento sull'importo superiore.
In caso di conversione del pignoramento ai sensi dell'articolo 495 del codice di procedura civile, il compenso è determinato secondo le percentuali di cui alla lettera a) ridotte della metà, sul valore dei beni o dei crediti pignorati o, se maggiore, sull'importo della somma versata.
In caso di estinzione o di chiusura anticipata del processo esecutivo il compenso è posto a carico del creditore procedente ed è liquidato dal giudice dell'esecuzione nella stessa percentuale di cui al comma precedente calcolata sul valore dei beni pignorati o, se maggiore, sul valore del credito per cui si procede.
In ogni caso il compenso dell'ufficiale giudiziario calcolato ai sensi dei commi secondo, terzo e quarto non può essere superiore ad un importo pari al 5 per cento del valore del credito per cui si procede.
Le somme complessivamente percepite a norma dei commi secondo, terzo, quarto e quinto sono attribuite dall'ufficiale giudiziario dirigente l'ufficio nella misura del sessanta per cento all'ufficiale o al funzionario che ha proceduto alle operazioni di pignoramento. La residua quota del quaranta per cento è distribuita dall'ufficiale giudiziario dirigente l'ufficio, in parti uguali, tra tutti gli altri ufficiali e funzionari preposti al servizio esecuzioni. Quando l'ufficiale o il funzionario che ha eseguito il pignoramento è diverso da colui che ha interrogato le banche dati previste dall'articolo 492-bis del codice di procedura civile e dal decreto di cui all'articolo 155-quater delle disposizioni per l'attuazione del codice di procedura civile, il compenso di cui al primo periodo del presente comma è attribuito nella misura del cinquanta per cento ciascuno.».
5. All'articolo 7, nono comma, del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, è inserito, in fine, il seguente periodo:
«Le informazioni comunicate sono altresì utilizzabili dall'autorità giudiziaria ai fini della ricostruzione dell'attivo e del passivo nell'ambito di procedure concorsuali, di procedimenti in materia di famiglia e di quelli relativi alla gestione di patrimoni altrui. Nei casi di cui al periodo precedente l'autorità giudiziaria si avvale per l'accesso dell'ufficiale giudiziario secondo le disposizioni relative alla ricerca con modalità telematiche dei beni da pignorare.».
6. L'articolo 155-quinquies delle disposizioni per l'attuazione del codice di procedura civile, di cui al regio decreto 18 dicembre 1941, n. 1368, introdotto dal comma 2, lettera a), del presente articolo, si applica anche ai procedimenti di cui al comma 5.
6-bis. Le disposizioni del presente articolo, fatta eccezione per quelle previste al comma 2, lettera a), limitatamente alle disposizioni di cui all'articolo 155-sexies, e lettera b), e al comma 5, si applicano ai procedimenti iniziati a decorrere dal trentesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto.

Art. 20.
Monitoraggio delle procedure esecutive individuali e concorsuali e deposito della nota di iscrizione a ruolo con modalità telematiche.

1. All'articolo 16-bis del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, dopo il comma 9-ter, sono aggiunti, in fine, i seguenti commi:

(omissis)[76]
2. Al decreto legislativo 8 luglio 1999, n. 270, sono apportate le seguenti modificazioni:
a) all'articolo 40, dopo il comma 1, è aggiunto il seguente:
«1-bis. Il commissario straordinario, redige ogni sei mesi una relazione sulla situazione patrimoniale dell'impresa e sull'andamento della gestione in conformità a modelli standard stabiliti con decreto, avente natura non regolamentare, del Ministero dello sviluppo economico. La relazione di cui al periodo precedente é trasmessa al predetto Ministero con modalità telematiche.»;
b) all'articolo 75, al comma 1, dopo il primo periodo è inserito il seguente:
«Il bilancio finale della procedura e il conto della gestione sono redatti in conformità a modelli standard stabiliti con decreto, avente natura non regolamentare, del Ministero di cui al periodo che precede, al quale sono sottoposti con modalità telematiche.».
3. I dati risultanti dai rapporti riepilogativi periodici e finali di cui agli articoli 40 e 75, comma 1, del decreto legislativo 8 luglio 1999, n. 270, sono estratti ed elaborati, a cura del Ministero dello sviluppo economico, nell'ambito di rilevazioni statistiche nazionali.
4. Per l'attuazione delle disposizioni dei commi 1 e 2 il Ministero competente provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.».
5. Le disposizioni di cui al comma 1 si applicano anche alle procedure concorsuali ed ai procedimenti di esecuzione forzata pendenti, a decorrere dal novantesimo giorno dalla pubblicazione nella Gazzetta Ufficiale del provvedimento contenente le specifiche tecniche di cui all'articolo 16-bis, comma 9-septies del decreto-legge n. 179 del 2012, convertito, con modificazioni, dalla legge n. 221 del 2012.
6. Le disposizioni di cui ai commi 2 e 3 si applicano, anche alle procedure di amministrazione straordinaria pendenti, a decorrere dal novantesimo giorno dalla pubblicazione nella Gazzetta Ufficiale dei decreti previsti all'articolo 40, comma 1-bis, e 75, comma 1, secondo periodo, del decreto legislativo 8 luglio 1999, n. 270. *(ritorna all'indice cronologico)* (*torna all'indice per argomenti*)

[76] Vedi art. 16bis d.l. 179/2012 come modificato dal presente articolo.

D.P.C.M. 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione, dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23bis, 23ter , 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.[77]

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Capo I
DEFINIZIONI E AMBITO DI APPLICAZIONE

(omissis)

Capo II
DOCUMENTO INFORMATICO

Art. 3
Formazione del documento informatico

1. Il documento informatico è formato mediante una delle seguenti principali modalità:

a) redazione tramite l'utilizzo di appositi strumenti software;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

2. Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

3. Il documento informatico, identificato in modo univoco e persistente, è memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.

4. Nel caso di documento informatico formato ai sensi del comma 1, lettera a), le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;

b) l'apposizione di una validazione temporale;

c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;

d) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;

e) il versamento ad un sistema di conservazione.

5. Nel caso di documento informatico formato ai sensi del comma 1, lettera b), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione.

6. Nel caso di documento informatico formato ai sensi del comma 1, lettere c) e d), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

7. Laddove non sia presente, al documento informatico immodificabile è associato un riferimento temporale.

---

[77] L'art. 65, ult. comma, del D.lvo 217/2017 ha stabilito che "Le regole tecniche emanate ai sensi dell'articolo 71 del decreto legislativo n. 82 del 2005, nel testo vigente prima dell'entrata in vigore del presente decreto, restano efficaci fino all'eventuale modifica o abrogazione da parte delle Linee guida di cui al predetto articolo 71, come modificato dal presente decreto".

8. L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'allegato 2 del presente decreto in modo da assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo dei dati in termini di accesso e di leggibilità. Formati diversi possono essere scelti nei casi in cui la natura del documento informatico lo richieda per un utilizzo specifico nel suo contesto tipico.

9. Al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'allegato 5 al presente decreto, è costituito da:

a) l'identificativo univoco e persistente;
b) il riferimento temporale di cui al comma 7;
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento informatico.

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

Art. 4.
Copie per immagine su supporto informatico
di documenti analogici

1. La copia per immagine su supporto informatico di un documento analogico di cui all'art. 22, commi 2 e 3, del Codice è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.
2. Fermo restando quanto previsto dall'art. 22, comma 3, del Codice, la copia per immagine di uno o più documenti analogici può essere sottoscritta con firma digitale o firma elettronica qualificata da chi effettua la copia.
3. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico di cui all'art. 22, comma 2, del Codice, può essere inserita nel documento informatico contenente la copia per immagine. Il documento informatico così formato è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

(*torna all'indice per argomenti*)

Art. 5.
Duplicati informatici di documenti informatici

1. Il duplicato informatico di un documento informatico di cui all'art. 23 -*bis* , comma 1, del Codice è prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

(*torna all'indice per argomenti*)

Art. 6.
Copie e estratti informatici di documenti informatici

1. La copia e gli estratti informatici di un documento informatico di cui all'art. 23-*bis* , comma 2, del Codice sono prodotti attraverso l'utilizzo di uno dei formati idonei di cui all'allegato 2 al presente decreto, mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.
2. La copia o l'estratto di uno o più documenti informatici di cui al comma 1, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua la copia ha la stessa efficacia probatoria dell'originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.
3. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o dell'estratto informatico di un documento informatico di cui al comma 1, può essere inserita nel documento informatico contenente la copia o l'estratto. Il documento informatico così formato è sottoscritto con

firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

(*torna all'indice per argomenti*)

(omissis)

Capo III
DOCUMENTO AMMINISTRATIVO INFORMATICO
Art. 9.
Formazione del documento amministrativo informatico

1. Al documento amministrativo informatico si applica quanto indicato nel Capo II per il documento informatico, salvo quanto specificato nel presente Capo.
2. Le pubbliche amministrazioni, ai sensi dell'art. 40, comma 1, del Codice, formano gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione ovvero acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -*bis*, 40 -*bis* e 65 del Codice.
3. Il documento amministrativo informatico, di cui all'art 23-*ter* del Codice, formato mediante una delle modalità di cui all'art. 3, comma 1, del presente decreto, è identificato e trattato nel sistema di gestione informatica dei documenti di cui al Capo IV del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, comprensivo del registro di protocollo e degli altri registri di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, dei repertori e degli archivi, nonché degli albi, degli elenchi, e di ogni raccolta di dati concernente stati, qualità personali e fatti già realizzati dalle amministrazioni su supporto informatico, in luogo dei registri cartacei, di cui all'art. 40, comma 4, del Codice, con le modalità descritte nel manuale di gestione.
4. Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-*bis* , 40-*bis* e 65 del Codice sono identificate e trattate come i documenti amministrativi informatici nel sistema di gestione informatica dei documenti di cui al comma 3 ovvero, se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto, memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione.
5. Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui all'art. 3, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti di cui al comma 3.
6. Fermo restando quanto stabilito nell'art. 3, comma 8, eventuali ulteriori formati possono essere utilizzati dalle pubbliche amministrazioni in relazione a specifici contesti operativi che vanno esplicitati, motivati e riportati nel manuale di gestione.
7. Al documento amministrativo informatico viene associato l'insieme minimo dei metadati di cui all'art. 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, fatti salvi i documenti soggetti a registrazione particolare che comunque possono contenere al proprio interno o avere associati l'insieme minimo dei metadati di cui all'art. 3, comma 9, come descritto nel manuale di gestione.
8. Al documento amministrativo informatico sono associati eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, e descritti nel manuale di gestione.
9. I metadati associati al documento amministrativo informatico, di tipo generale o appartenente ad una tipologia comune a più amministrazioni, sono definiti dalle pubbliche amministrazioni competenti, ove necessario sentito il Ministero dei beni e delle attività culturali e del turismo, e trasmessi all'Agenzia per l'Italia digitale che ne cura la pubblicazione on line sul proprio sito.
10. Ai fini della trasmissione telematica di documenti amministrativi informatici, le pubbliche amministrazioni pubblicano sui loro siti gli standard tecnici di riferimento, le codifiche utilizzate e le specifiche per lo sviluppo degli applicativi software di colloquio, rendendo eventualmente disponibile gratuitamente sul proprio sito il software per la trasmissione di dati coerenti alle suddette codifiche e specifiche. Al fine di abilitare alla trasmissione telematica gli applicativi software sviluppati da terzi, le amministrazioni provvedono a richiedere a questi opportuna certificazione di correttezza funzionale dell'applicativo e di conformità dei dati trasmessi alle codifiche e specifiche pubblicate.

Art. 10.
Copie su supporto informatico di documenti amministrativi analogici

1. Fatto salvo quanto previsto all'art. 4, l'attestazione di conformità, di cui all'art. 23-*ter* , comma 3, del Codice, della copia informatica di un documento amministrativo analogico, formato dalla pubblica amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica. Il documento informatico così formato è sottoscritto con firma digitale o firma elettronica qualificata del funzionario delegato.
2. L'attestazione di conformità di cui al comma 1, anche nel caso di uno o più documenti amministrativi informatici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia, può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia. Il documento informatico prodotto è sottoscritto con firma digitale o con firma elettronica qualificata del funzionario delegato.

(omissis)

Capo IV
FASCICOLI INFORMATICI,
REGISTRI E REPERTORI INFORMATICI
DELLA PUBBLICA AMMINISTRAZIONE

Art. 13.
Formazione dei fascicoli informatici

1. I fascicoli di cui all'art. 41 del Codice e all'art. 64, comma 4, e all'art. 65 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 fanno parte del sistema di gestione informatica dei documenti e contengono l'insieme minimo dei metadati indicati al comma 2 –*ter* del predetto art. 41 del Codice, nel formato specificato nell'allegato 5 del presente decreto, e la classificazione di cui al citato art. 64 del citato decreto n. 445 del 2000.
2. Eventuali aggregazioni documentali informatiche sono gestite nel sistema di gestione informatica dei documenti e sono descritte nel manuale di gestione. Ad esse si applicano le regole che identificano univocamente l'aggregazione documentale informatica ed è associato l'insieme minimo dei metadati di cui al comma 1.

(*torna all'indice per argomenti*)

Art. 14.
Formazione dei registri e repertori informatici

1. Il registro di protocollo e gli altri registri di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei di cui all'art. 40, comma 4, del Codice sono formati ai sensi dell'art. 3, comma 1, lettera *d)* .
2. Le pubbliche amministrazioni gestiscono registri particolari informatici, espressamente previsti da norme o regolamenti interni, generati dal concorso di più aree organizzative omogenee con le modalità previste ed espressamente descritte nel manuale di gestione, individuando un'area organizzativa omogenea responsabile.

(*torna all'indice per argomenti*)

(omissis)

Capo V
DISPOSIZIONI FINALI

Art. 17.
Disposizioni finali

1. Il presente decreto entra in vigore decorsi trenta giorni dalla data della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.
2. Le pubbliche amministrazioni adeguano i propri sistemi di gestione informatica dei documenti entro e non oltre diciotto mesi dall'entrata in vigore del presente decreto.
Fino al completamento di tale processo possono essere applicate le previgenti regole tecniche. Decorso tale termine si applicano le presenti regole tecniche.

Allegati (Omissis)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Decreto del Ministero della Giustizia 26 febbraio 2015, n. 32 - Regolamento recante le regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche nei casi previsti dal codice di procedura civile, ai sensi dell'articolo 161-ter delle disposizioni per l'attuazione del codice di procedura civile (*GU n. 69 del 24-3-2015*)

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

IL MINISTRO DELLA GIUSTIZIA

Visto l'articolo 161-ter delle disposizioni per l'attuazione del codice di procedura civile, recante disposizioni per le vendite con modalità telematiche;
Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;
Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 29 gennaio 2015;
Sentito il Garante per la protezione dei dati personali, ai sensi dell'articolo 154, comma 4, del decreto legislativo 20 giugno 2003, n. 196, che ha espresso parere favorevole con provvedimento reso nel corso della riunione del 15 maggio 2014;
Vista la comunicazione al Presidente del Consiglio dei ministri, a norma dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, effettuata con nota del 12 febbraio 2015, ai sensi del predetto articolo;
Adotta
il seguente regolamento:

Capo I
Disposizioni generali

Art. 1
Oggetto

1. Il presente regolamento stabilisce le regole tecniche e operative per lo svolgimento delle vendite dei beni mobili e immobili mediante gara telematica nei casi previsti dal codice di procedura civile.

Art. 2
Definizioni

1. Ai fini del presente decreto si intende per:
a) «operazioni di vendita telematica»: le attività compiute tra il momento della connessione degli offerenti al portale del gestore della vendita telematica e l'aggiudicazione o l'individuazione del migliore offerente;
b) «gestore della vendita telematica»: il soggetto costituito in forma societaria autorizzato dal giudice a gestire la vendita telematica;
c) «referente della procedura»: la persona fisica incaricata dal giudice che procede alle operazioni di vendita;
d) «offerta per la vendita telematica»: l'offerta d'acquisto di beni mobili o immobili nella vendita telematica senza incanto o tramite commissionario ovvero la domanda di partecipazione alla vendita telematica all'incanto dei medesimi beni;
e) «rilancio»: l'offerta in aumento nella gara relativa alla vendita con e senza incanto o tramite commissionario;
f) «vendita sincrona telematica»: modalità di svolgimento dell'incanto o della gara nella vendita immobiliare senza incanto in cui i rilanci vengono formulati esclusivamente in via telematica nella medesima unità di tempo e con la simultanea connessione del giudice o del referente della procedura e di tutti gli offerenti;
g) «vendita sincrona mista»: modalità di svolgimento dell'incanto o della gara nella vendita immobiliare senza incanto in cui i rilanci possono essere formulati, nella medesima unità di tempo, sia in via telematica sia comparendo innanzi al giudice o al referente della procedura;
h) «vendita asincrona»: modalità di svolgimento delle vendite mobiliari senza incanto o tramite commissionario o della gara nella vendita immobiliare senza incanto in cui i rilanci vengono formulati, esclusivamente in via telematica, in un lasso temporale predeterminato e senza la simultanea connessione del giudice o del referente della procedura;
i) «Ministero»: il Ministero della giustizia;
l) «registro»: il registro dei gestori della vendita telematica;
m) «responsabile»: il responsabile della tenuta del registro;

n) «casella di posta elettronica certificata per la vendita telematica»: la casella di posta elettronica certificata richiesta dalla persona fisica o giuridica che intende formulare l'offerta, le cui credenziali di accesso sono rilasciate, previa identificazione del richiedente, a norma dell'articolo 13;
o) «portale del gestore»: il sistema telematico predisposto dal gestore della vendita telematica e accessibile agli offerenti e al pubblico tramite rete Internet ed al giudice o ad altri utenti legittimati tramite rete Internet o servizi telematici del Ministero; i servizi del portale sono erogati in conformità ai protocolli di comunicazione crittografica SSL/TLS (Secure Sockets Layer e Transport Layer Security); il portale deve essere munito di un valido certificato di autenticazione emesso da un certificatore accreditato per la firma digitale o da un certificatore riconosciuto a livello internazionale alla emissione di certificati di autenticazione per protocolli SSL/TLS.

Capo II
Registro dei gestori della vendita telematica
Sezione I
Requisiti e procedimento di iscrizione

Art. 3
Istituzione del registro

1. è istituito il registro dei gestori della vendita telematica.
2. Il registro è tenuto dal Dipartimento per gli affari di giustizia del Ministero e ne è responsabile il direttore generale della giustizia civile. Il direttore generale della giustizia civile può delegare una persona con qualifica dirigenziale o un magistrato ed avvalersi della Direzione generale dei sistemi informativi automatizzati del Ministero nonché, al fine di esercitare la vigilanza, dell'Ispettorato generale del Ministero. Il Ministero è titolare del trattamento dei dati personali.
3. I dati del registro e le relative annotazioni sono continuamente aggiornati in conformità alle previsioni del presente regolamento.
4. La gestione del registro ha luogo con modalità informatiche che assicurino la possibilità di una rapida elaborazione dei dati con finalità statistica e ispettiva o, comunque, connessa ai compiti di tenuta di cui al presente regolamento.
5. A cura del responsabile è formato un elenco dei gestori della vendita telematica iscritti nel registro contenente i dati identificativi degli stessi e i distretti di Corte di appello per i quali sono iscritti. L'elenco di cui al periodo precedente non comprende i gestori della vendita telematica sospesi dal registro a norma dell'articolo 8. L'elenco è pubblicato sul portale dei servizi telematici del Ministero.

Art. 4
Requisiti per l'iscrizione nel registro

1. Nel registro sono iscritti, a domanda, i gestori della vendita telematica costituiti in forma di società di capitali. La domanda di iscrizione deve contenere l'indicazione di uno o più distretti di Corte di appello in cui si intende svolgere il servizio di vendita telematica.
2. Il responsabile prima di procedere all'iscrizione verifica:
a) il rilascio di una polizza assicurativa per le conseguenze patrimoniali comunque derivanti dallo svolgimento del servizio di gestione della vendita telematica, con massimale non inferiore a:
1) tre milioni di euro se l'iscrizione è richiesta per due o più distretti di Corte di appello o per uno dei seguenti distretti:
Roma, Milano, Napoli, Palermo;
2) un milione di euro nei casi diversi da quelli di cui al numero 1);
b) l'adozione di un manuale operativo dei servizi, in conformità a quanto previsto dal presente decreto;
c) l'adozione di un piano di sicurezza in cui vengano descritte tutte le misure e gli accorgimenti adottati dal gestore per garantire la protezione dei dati anche personali trattati tramite il portale e la sicurezza delle operazioni, la loro integrità, e la disponibilità dei servizi; il piano comprenderà le misure per il salvataggio periodico dei dati e il loro ripristino in caso di danneggiamento o perdita dei dati e dei sistemi;
d) la conformità dei portali dei gestori della vendita telematica ai requisiti tecnici di cui agli articoli 10 e 11 della legge 9 gennaio 2004, n. 4 e al decreto 8 luglio 2005 del Ministro per l'innovazione e la tecnologia, pubblicato nella Gazzetta Ufficiale 8 agosto 2005, n. 183, nonché al decreto del Presidente della Repubblica 1° marzo 2005, n. 75.
3. Il contratto di assicurazione deve prevedere a carico dell'assicuratore l'obbligo di comunicare immediatamente al responsabile la cessazione di efficacia del medesimo contratto per qualsiasi motivo.

4. Prima di procedere all'iscrizione il responsabile verifica altresì il possesso da parte degli amministratori, dei sindaci e dei procuratori speciali e generali della società richiedente dei seguenti requisiti di onorabilità:
a) non versare in una delle condizioni di ineleggibilità o decadenza previste dall'articolo 2382 del codice civile;
b) non essere stati sottoposti a misure di prevenzione personali disposte dall'autorità giudiziaria ai sensi del decreto legislativo 6 settembre 2011, n. 159;
c) non essere stati condannati con sentenza passata in giudicato, salvi gli effetti della riabilitazione:
1) a pena detentiva per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
2) alla reclusione per uno dei delitti previsti dagli articoli 351, 353 e 354 del codice penale e nel titolo XI del libro V del codice civile, nel regio decreto 16 marzo 1942, n. 267, nonché dall'articolo 16 della legge 27 gennaio 2012, n. 3 e successive modificazioni;
3) alla reclusione per un tempo non inferiore a un anno per un delitto contro la pubblica amministrazione diverso da quelli di cui al numero 2), contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;
4) alla reclusione per un tempo superiore a due anni per un qualunque delitto non colposo.
5. Quando la società richiedente è soggetta al controllo di un'altra società, a norma dell'articolo 2359, primo e secondo comma, del codice civile, il responsabile verifica il possesso dei requisiti di cui al comma 4 anche con riguardo agli amministratori, ai sindaci e ai procuratori speciali e generali della società controllante. Nel caso previsto dall'articolo 2359, primo comma, n. 3), del codice civile, l'influenza dominante deve essere stata accertata con sentenza passata in giudicato.
6. La documentazione comprovante il possesso dei requisiti di cui al presente articolo, salvo quello di cui al comma 2, lettera a), è presentata ai sensi degli articoli 46 e 47 del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. Il possesso del requisito di cui al comma 2, lettera a), è dimostrato mediante la produzione di copia autentica della polizza assicurativa.

Art. 5
Procedimento per l'iscrizione

1. Il responsabile approva il modello della domanda per l'iscrizione, con l'indicazione degli atti e dei documenti idonei a comprovare il possesso dei requisiti previsti dall'articolo 4, di cui la domanda deve essere corredata. Il modello approvato è pubblicato sul sito internet del Ministero.
2. La domanda è sottoscritta con firma digitale. è trasmessa, unitamente agli allegati, a mezzo posta elettronica certificata.
3. Il procedimento di iscrizione deve essere concluso entro trenta giorni a decorrere dalla data di ricevimento della domanda. La richiesta di integrazione della domanda o dei suoi allegati è ammessa per una sola volta e sospende il predetto termine per un periodo non superiore a trenta giorni. La mancata adozione del provvedimento di iscrizione nel termine di cui al presente comma equivale a diniego dello stesso.

Art. 6
Effetti dell'iscrizione

1. Il provvedimento di iscrizione, con il numero d'ordine attribuito nel registro, è comunicato al richiedente ed al presidente della Corte di appello alla quale si riferisce l'iscrizione.
2. Dalla data della comunicazione di cui al comma precedente, il gestore della vendita telematica è tenuto a fare menzione, negli atti, nella corrispondenza e nella pubblicità, del numero d'ordine attribuitogli.

Art. 7
Obblighi di comunicazione dei gestori delle vendite telematiche

1. Il gestore della vendita telematica è obbligato a comunicare immediatamente al responsabile, a mezzo posta elettronica certificata, tutte le vicende modificative dei requisiti di cui all'articolo 4.
2. L'autorità giudiziaria provvede alla segnalazione al responsabile di tutti i fatti e le notizie rilevanti ai fini dell'esercizio dei poteri previsti nel presente regolamento.
3. Il gestore della vendita telematica trasmette entro cinque giorni da ciascun esperimento di vendita i dati relativi ai beni immobili che ne costituiscono oggetto nonché i dati identificativi dei relativi offerenti. La trasmissione è effettuata con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici, nonché delle apposite specifiche tecniche del responsabile per i sistemi informativi ed automatizzati del Ministero. I

relativi dati sono estratti ed elaborati dal Ministero, per il tramite della direzione generale di statistica, anche nell'ambito di rilevazioni su base nazionale. La disposizione di cui al presente comma si applica anche agli esperimenti di vendita di beni mobili, anche tramite commissionario, di valore pari o superiore a quello di cui all'articolo 525, secondo comma, del codice di procedura civile.

Art. 8
Sospensione e cancellazione dal registro

1. Quando dopo l'iscrizione il gestore della vendita telematica perde i requisiti di cui all'articolo 4, il responsabile provvede a sospenderlo dal registro per un periodo non superiore a novanta giorni, decorso il quale, persistendo la mancanza dei requisiti, provvede alla cancellazione.
2. Quando risulta che i requisiti di cui all'articolo 4 non sussistevano al momento dell'iscrizione il responsabile provvede a norma del comma 1 ovvero, nei casi più gravi, alla cancellazione del gestore della vendita telematica dal registro.
3. è disposta la cancellazione dei gestori di vendita telematica che hanno prestato il servizio in forza di incarico ricevuto da uffici giudiziari siti in distretti di Corti di appello diversi da quelli per i quali sono iscritti o che violano gli obblighi previsti dall'articolo 7.
4. Il gestore della vendita telematica cancellato dal registro non può essere nuovamente iscritto prima che sia decorso un biennio dalla cancellazione.
5. Ai fini del presente articolo, il responsabile può acquisire informazioni relative all'attività dei gestori delle vendite telematiche dai medesimi gestori e dagli uffici giudiziari nei modi e nei tempi stabiliti da circolari o atti amministrativi generali equipollenti.

Sezione II
Obblighi del gestore della vendita telematica

Art. 9
Registro degli incarichi di vendita telematica

1. Ciascun gestore della vendita telematica è tenuto a istituire un registro informatico degli incarichi di vendita telematica, indicando:
a) il numero d'ordine progressivo per anno;
b) l'ufficio giudiziario innanzi al quale pende la procedura rispetto alla quale è stato incaricato;
c) se l'incarico riguarda una procedura di espropriazione forzata mobiliare o immobiliare;
d) se si tratta di vendita senza incanto, con incanto o tramite commissionario;
e) se procede alle operazioni di vendita con modalità sincrona, asincrona o mista;
f) il numero dei lotti posti in vendita;
g) per ciascun lotto: il prezzo al quale i beni sono stati per la prima volta posti in vendita, il numero degli esperimenti di vendita, il prezzo di vendita;
h) le spese e i compensi, per ciascuna procedura, liquidati dall'autorità competente.
2. Ulteriori registri o annotazioni possono essere stabiliti con determinazione del responsabile, comunicata ai gestori mediante pubblicazione nell'area pubblica del portale dei servizi telematici del Ministero.
3. Entro il 31 gennaio di ciascun anno il gestore della vendita telematica trasmette al responsabile i dati indicati nel registro e relativi agli eventi verificatisi nel corso dell'anno precedente. La trasmissione ha luogo con modalità telematiche ed in conformità alle specifiche tecniche di cui all'articolo 26.
4. Il gestore della vendita telematica è tenuto a trattare i dati raccolti nel rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali».

Art. 10
Obblighi del gestore

1. Il gestore della vendita telematica non può partecipare, neppure per interposta persona, alle operazioni di vendita dei beni oggetto delle procedure pendenti innanzi agli uffici giudiziari compresi nel distretto di Corte d'appello rispetto al quale è stato iscritto.
2. Il legale rappresentante del gestore della vendita telematica, o un suo procuratore, sottoscrive una dichiarazione dalla quale risulti che il gestore non si trova in conflitto d'interesse con la procedura. La dichiarazione è portata a conoscenza del giudice al momento dell'accettazione dell'incarico.
3. I gestori della vendita telematica si dotano di un manuale operativo dei servizi, in cui vengono descritti le modalità di esecuzione dei servizi, nonché i prezzi praticati con indicazione di eventuali differenziazioni per distretto o circondario. Le modalità di esecuzione dei servizi e i relativi prezzi dovranno essere pubblicati sui siti dei gestori delle vendite telematiche.

4. Nel caso di violazione degli obblighi del gestore della vendita telematica previsti dal presente decreto il responsabile dispone la sospensione e, nei casi più gravi, la cancellazione del gestore dal registro.

Art. 11
Monitoraggio

1. Il Ministero procede annualmente al monitoraggio statistico delle operazioni di vendita telematica svolte dai gestori, anche sulla base dei dati trasmessi a norma dell'articolo 9. Il Ministero, per il tramite della Direzione generale per i sistemi informativi automatizzati e della Direzione generale di statistica, provvede al monitoraggio statistico di cui al periodo precedente nei modi e nei tempi stabiliti da circolari o atti amministrativi equipollenti.

Capo III
Vendite immobiliari
Sezione I
Disposizioni generali

Art. 12
Modalità di presentazione dell'offerta e dei documenti allegati

1. L'offerta per la vendita telematica deve contenere:
a) i dati identificativi dell'offerente, con l'espressa indicazione del codice fiscale o della partita IVA;
b) l'ufficio giudiziario presso il quale pende la procedura;
c) l'anno e il numero di ruolo generale della procedura;
d) il numero o altro dato identificativo del lotto;
e) la descrizione del bene;
f) l'indicazione del referente della procedura;
g) la data e l'ora fissata per l'inizio delle operazioni di vendita;
h) il prezzo offerto e il termine per il relativo pagamento, salvo che si tratti di domanda di partecipazione all'incanto;
i) l'importo versato a titolo di cauzione;
l) la data, l'orario e il numero di CRO del bonifico effettuato per il versamento della cauzione;
m) il codice IBAN del conto sul quale è stata addebitata la somma oggetto del bonifico di cui alla lettera l);
n) l'indirizzo della casella di posta elettronica certificata di cui al comma 4 o, in alternativa, quello di cui al comma 5, utilizzata per trasmettere l'offerta e per ricevere le comunicazioni previste dal presente regolamento;
o) l'eventuale recapito di telefonia mobile ove ricevere le comunicazioni previste dal presente regolamento.
2. Quando l'offerente risiede fuori dal territorio dello Stato, e non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo. In ogni caso deve essere anteposto il codice del paese assegnante, in conformità alle regole tecniche di cui allo standard ISO 3166-1 alpha-2code dell'International Organization for Standardization.
3. L'offerta per la vendita telematica è redatta e cifrata mediante un software realizzato dal Ministero, in forma di documento informatico privo di elementi attivi e in conformità alle specifiche tecniche di cui all'articolo 26 del presente decreto. Il software di cui al periodo precedente è messo a disposizione degli interessati da parte del gestore della vendita telematica e deve fornire in via automatica i dati di cui al comma 1, lettere b), c), d), e), f) e g), nonché i riferimenti dei gestori del servizio di posta elettronica certificata per la vendita telematica iscritti a norma dell'articolo 13, comma 4.
4. L'offerta è trasmessa mediante la casella di posta elettronica certificata per la vendita telematica. La trasmissione sostituisce la firma elettronica avanzata dell'offerta, sempre che l'invio sia avvenuto richiedendo la ricevuta completa di avvenuta consegna di cui all'articolo 6, comma 4 del decreto del Presidente della Repubblica, 11 febbraio 2005, n. 68 e che il gestore del servizio di posta elettronica certificata attesti nel messaggio o in un suo allegato di aver rilasciato le credenziali di accesso in conformità a quanto previsto dall'articolo 13, commi 2 e 3. Quando l'offerta è formulata da più persone alla stessa deve essere allegata la procura rilasciata dagli altri offerenti al titolare della casella di posta elettronica certificata per la vendita telematica. La procura è redatta nelle forme dell'atto pubblico o della scrittura privata autenticata e può essere allegata anche in copia per immagine.

5. L'offerta, quando è sottoscritta con firma digitale, può essere trasmessa a mezzo di casella di posta elettronica certificata anche priva dei requisiti di cui all'articolo 2, comma 1, lettera n). Si applica il comma 4, terzo periodo, e la procura è rilasciata a colui che ha sottoscritto l'offerta a norma del presente comma.
6. I documenti sono allegati all'offerta in forma di documento informatico o di copia informatica, anche per immagine, privi di elementi attivi. I documenti allegati sono cifrati mediante il software di cui al comma 3. Le modalità di congiunzione mediante strumenti informatici dell'offerta con i documenti alla stessa allegati sono fissate dalle specifiche tecniche di cui all'articolo 26.

Art. 13
Modalità di trasmissione dell'offerta

1. L'offerta e i documenti allegati sono inviati a un apposito indirizzo di posta elettronica certificata del Ministero mediante la casella di posta elettronica certificata indicata a norma dell'articolo 12, comma 1, lettera n).
2. Ciascun messaggio di posta elettronica certificata per la vendita telematica contiene, anche in un allegato, l'attestazione del gestore della casella di posta elettronica certificata per la vendita telematica di aver provveduto al rilascio delle credenziali previa identificazione del richiedente a norma del presente regolamento.
3. Quando l'identificazione è eseguita per via telematica, la stessa può aver luogo mediante la trasmissione al gestore di cui al comma 1 di una copia informatica per immagine, anche non sottoscritta con firma elettronica, di un documento analogico di identità del richiedente. La copia per immagine è priva di elementi attivi ed ha i formati previsti dalle specifiche tecniche stabilite a norma dell'articolo 26. Quando l'offerente non dispone di un documento di identità rilasciato da uno dei Paesi dell'Unione europea, la copia per immagine deve essere estratta dal passaporto.
4. Il responsabile per i sistemi informativi automatizzati del Ministero verifica, su richiesta dei gestori di cui al comma 1, che il procedimento previsto per il rilascio delle credenziali di accesso sia conforme a quanto previsto dal presente articolo e li iscrive in un'apposita area pubblica del portale dei servizi telematici del Ministero.

Art. 14
Deposito e trasmissione dell'offerta al gestore per la vendita telematica

1. L'offerta si intende depositata nel momento in cui viene generata la ricevuta completa di avvenuta consegna da parte del gestore di posta elettronica certificata del ministero della giustizia.
2. L'offerta pervenuta all'indirizzo di posta elettronica certificata di cui all'articolo 13, comma 1, è automaticamente decifrata non prima di centottanta e non oltre centoventi minuti antecedenti l'orario fissato per l'inizio delle operazioni di vendita.
3. Il software di cui all'articolo 12, comma 3, elabora un ulteriore documento testuale, privo di restrizioni per le operazioni di selezione e copia, in uno dei formati previsti dalle specifiche tecniche dell'articolo 26. Il documento deve contenere i dati dell'offerta, salvo quelli di cui all'articolo 12, comma 1, lettere a), n) ed o).
4. L'offerta e il documento di cui al comma 2 sono trasmessi ai gestori incaricati delle rispettive vendite nel rispetto del termine di cui al comma 1.

Art. 15
Mancato funzionamento dei servizi informatici del dominio giustizia

1. Il responsabile per i sistemi informativi automatizzati del ministero comunica preventivamente ai gestori della vendita telematica i casi programmati di mancato funzionamento dei sistemi informativi del dominio giustizia. I gestori ne danno notizia agli interessati mediante avviso pubblicato sui propri siti internet e richiedono di pubblicare un analogo avviso ai soggetti che gestiscono i siti internet ove è eseguita la pubblicità di cui all'articolo 490 del codice di procedura civile. Nei casi di cui al presente comma le offerte sono formulate a mezzo telefax al recapito dell'ufficio giudiziario presso il quale è iscritta la procedura, indicato negli avvisi di cui al periodo precedente. Non prima del giorno precedente l'inizio delle operazioni di vendita il gestore ritira le offerte formulate a norma del presente comma dall'ufficio giudiziario.
2. Nei casi di mancato funzionamento dei sistemi informativi del dominio giustizia non programmati o non comunicati a norma del comma 1, l'offerta si intende depositata nel momento in cui viene generata la ricevuta di accettazione da parte del gestore di posta elettronica certificata del mittente. Il gestore è tenuto

a permettere la partecipazione alle operazioni di vendita dell'offerente che documenta la tempestiva presentazione dell'offerta a norma del periodo precedente.

Art. 16
Avviso di connessione

1. Almeno trenta minuti prima dell'inizio delle operazioni di vendita il gestore della vendita telematica invia all'indirizzo di posta elettronica certificata indicato nell'offerta un invito a connettersi al proprio portale. Un estratto dell'invito di cui al periodo precedente è trasmesso dal gestore, a mezzo SMS, al recapito di telefonia mobile di cui all'articolo 12, comma 1, lettera o).
2. Al fine di consentire la partecipazione alle operazioni di vendita, il gestore, entro il termine di cui al comma 1, invia alla casella di cui all'articolo 12, comma 1, lettera n), le credenziali per l'accesso al proprio portale.

Art. 17
Verifiche del gestore per le operazioni di vendita

1. Alle operazioni di vendita possono partecipare gli offerenti. L'identificazione dei partecipanti ha luogo mediante le credenziali di cui all'articolo 16, comma 2. 2. Il gestore verifica che il messaggio di posta elettronica certificata mediante il quale è stata trasmessa l'offerta contiene l'attestazione di cui all'articolo 13, comma 2, nonché l'effettivo versamento della cauzione. Dell'esito di tali verifiche il gestore informa immediatamente il giudice o il referente della procedura.

Art. 18
Ammissione degli offerenti alle operazioni di vendita

1. In sede di incanto o di deliberazione sull'offerta, a norma dell'articolo 572 del codice di procedura civile, il giudice o il referente della procedura, verificata la regolarità delle offerte dà inizio alle operazioni di vendita.

Art. 19
Obblighi del gestore per le operazioni di vendita

1. Il gestore della vendita telematica allestisce e visualizza sul proprio portale un sistema automatico di computo del termine fissato per la formulazione dei rilanci.
2. I rilanci e le osservazioni di ciascun offerente sono riportati nel portale del gestore della vendita telematica e resi visibili agli altri partecipanti, al giudice o al referente della procedura; allo stesso modo si procede per ogni determinazione di questi ultimi.

Art. 20
Accesso al portale nel corso delle operazioni di vendita

1. Alle operazioni di vendita senza incanto possono prendere parte con modalità telematiche il giudice, il referente della procedura e il cancelliere. Con le medesime modalità possono partecipare anche altri soggetti se autorizzati dal giudice o dal referente della procedura.
2. Alle operazioni di vendita con incanto può assistere chiunque, connettendosi all'indirizzo internet indicato nell'avviso di cui all'articolo 490 del codice di procedura civile, previa registrazione sul portale.
3. In ogni caso, il portale del gestore della vendita telematica assicura l'accesso degli offerenti ai dati contenuti nel documento informatico di cui all'articolo 14, comma 3, e sostituisce i nominativi degli offerenti con pseudonimi o altri elementi distintivi in grado di assicurare l'anonimato. Il giudice, il referente della procedura ed il cancelliere possono comunque accedere a tutti i dati contenuti nell'offerta di cui all'articolo 14, comma 2.

Sezione II
Modalità della vendita telematica

Art. 21
Vendita sincrona telematica

1. Nel caso di vendita sincrona, l'offerta e la domanda di partecipazione all'incanto possono essere presentate esclusivamente con modalità telematiche a norma degli articoli 12 e 13.

Art. 22
Vendita sincrona mista

1. Quando il giudice lo dispone, l'offerta di acquisto e la domanda di partecipazione all'incanto possono essere presentate a norma degli articoli 12 e 13 o su supporto analogico mediante deposito in cancelleria.
2. Coloro che hanno formulato l'offerta o la domanda con modalità telematiche partecipano alle operazioni di vendita con le medesime modalità. Coloro che hanno formulato l'offerta o la domanda su supporto analogico partecipano comparendo innanzi al giudice o al referente della procedura.
3. Fermo quanto previsto dall'articolo 20, comma 3, i dati contenuti nelle offerte o nelle domande formate su supporto analogico nonché i rilanci e le osservazioni dei partecipanti alle operazioni di vendita comparsi innanzi al giudice o al referente della procedura sono riportati nel portale del gestore della vendita telematica e resi visibili a coloro che partecipano alle operazioni di vendita con modalità telematiche.

Art. 23
Verbale della vendita sincrona e sincrona mista

1. Per la redazione del verbale, il giudice o il referente della procedura può utilizzare i dati riportati nel portale della vendita telematica e quelli ivi immessi nel corso delle operazioni. I predetti dati sono trasmessi dal gestore al giudice o al referente della procedura al termine delle operazioni di vendita. In ogni caso, il gestore deve trasmettere un elenco, sottoscritto con firma digitale, dei rilanci e di coloro che li hanno effettuati, i dati identificativi dell'aggiudicatario, la cauzione da quest'ultimo versata e il prezzo di aggiudicazione, nonché i dati identificativi degli altri offerenti, le cauzioni dagli stessi versate e gli estremi dei conti bancari o postali sui quali sono state addebitate.

Art. 24
Vendita asincrona

1. Il giudice può disporre che nella vendita senza incanto la gara si svolga mediante rilanci compiuti nell'ambito di un determinato lasso temporale.
2. L'offerta è presentata esclusivamente in via telematica a norma degli articoli 12 e 13. Ricevute le offerte, il giudice o il referente della procedura sente le parti e i creditori iscritti non intervenuti, compie le verifiche di cui all'articolo 18 e invita gli offerenti a una gara sull'offerta più alta con le modalità di cui al comma 1. Il gestore della vendita telematica comunica ai partecipanti ogni rilancio all'indirizzo di posta elettronica di cui all'articolo 12, comma 1, lettera n) e con SMS.
3. Al termine del lasso temporale fissato per lo svolgimento della gara, il gestore della vendita telematica comunica, con le modalità di cui al comma 2, a tutti i partecipanti la maggiore offerta formulata. Al giudice o al referente della procedura il gestore trasmette l'elenco dei rilanci e di coloro che li hanno effettuati, comunica i dati identificativi del maggiore offerente, la cauzione da quest'ultimo versata e il prezzo offerto, nonché i dati identificativi degli altri offerenti, le cauzioni dagli stessi versate e gli estremi dei conti bancari o postali sui quali sono state addebitate. Il giudice o il referente della procedura fa luogo alla vendita e provvede a norma dell'articolo 574 del codice di procedura civile.

Capo IV
Vendite mobiliari senza incanto e a mezzo commissionario

Art. 25
Modalità di presentazione dell'offerta e di svolgimento delle operazioni di vendita

1. Per la presentazione dell'offerta per la vendita dei beni mobili con modalità asincrona, l'interessato si registra sul portale del gestore della vendita telematica, fornendo i dati identificativi, il codice fiscale, un indirizzo di posta elettronica anche ordinaria per le comunicazioni del gestore, il luogo in cui intende ricevere le comunicazioni di cancelleria, il recapito di telefonia mobile. All'esito della registrazione, il sistema genera le credenziali per la partecipazione dell'interessato alla vendita telematica per la quale la registrazione è stata effettuata e assegna uno pseudonimo o altri elementi distintivi in grado di assicurare l'anonimato.
2. L'offerta è presentata indicando:
a) l'ufficio giudiziario presso il quale pende la procedura;
b) l'anno e il numero di ruolo generale della procedura;
c) il numero o altro dato identificativo del lotto;
d) la descrizione del bene;
e) l'indicazione del referente della procedura;
f) il prezzo offerto;
g) l'importo della cauzione prestata.

4. Il portale del gestore deve fornire in via automatica i dati di cui al comma 3, lettere a), b), c) d), ed e).
5. La cauzione è prestata con sistemi telematici di pagamento ovvero con carte di debito, di credito o prepagate, nonché con altri mezzi di pagamento con moneta elettronica disponibili nei circuiti bancario e postale.
6. Quando sono fissate modalità di versamento della cauzione che consentono al gestore di verificare l'effettivo pagamento della stessa con modalità automatizzate e contestualmente alla presentazione dell'offerta, la registrazione può essere effettuata nell'ambito del lasso temporale stabilito per la presentazione delle offerte. Nei casi diversi da quelli di cui al periodo precedente, la registrazione e il versamento della cauzione sono effettuati almeno cinque giorni prima dell'inizio del lasso temporale fissato per lo svolgimento delle operazioni di vendita; il gestore abilita a partecipare alla gara gli offerenti che hanno effettivamente versato la cauzione.
7. Nel corso della gara gli offerenti sono individuati esclusivamente mediante lo pseudonimo o gli altri elementi distintivi di cui al comma 1. Entro il secondo giorno successivo alla chiusura della gara, il gestore trasmette al referente della procedura l'elenco delle offerte e i dati identificativi di coloro che le hanno effettuate. Deve altresì comunicare e documentare gli estremi dei conti bancari o postali sui quali sono state addebitate le cauzioni accreditate sul conto vincolato, di aver accreditato sul conto corrente bancario o postale vincolato al referente della procedura la cauzione versata da colui che ha formulato l'offerta più alta e di aver svincolato le cauzioni prestate dagli altri offerenti, nonché di aver restituito le cauzioni dagli stessi versate mediante accredito sui conti bancari o postali di provenienza.
8. Per l'accesso al portale si applica l'articolo 20, commi 1 e 3.

Capo V
Disposizioni finanziarie e finali

Art. 26
Specifiche tecniche

1. Le specifiche tecniche sono stabilite dal responsabile per i sistemi informativi automatizzati del Ministero, sentito, limitatamente ai profili inerenti alla protezione dei dati personali, il Garante per la protezione dei dati personali.
2. Le specifiche di cui al comma precedente vengono rese disponibili mediante pubblicazione nell'area pubblica del portale dei servizi telematici del Ministero.

Art. 27
Clausola di invarianza

1. All'attuazione delle disposizioni contenute nel presente decreto si provvede nell'ambito delle risorse umane, finanziarie e strumentali già esistenti e disponibili a legislazione vigente e senza e nuovi o maggiori oneri a carico della finanza pubblica.

Art. 28
Acquisto di efficacia e oneri informativi

1. Le disposizioni del presente decreto sono applicabili decorsi dodici mesi dalla sua entrata in vigore.
2. La tabella con la specifica degli oneri informativi di cui al decreto del Presidente del Consiglio dei ministri 14 novembre 2012 n. 252 è allegata al presente regolamento.
Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. è fatto obbligo a chiunque spetti di osservarlo e farlo osservare.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Decreto Legge 27 giugno 2015, n. 83, coordinato con la legge di conversione 6 agosto 2015, n. 132 - Misure urgenti in materia fallimentare, civile e processuale civile e di organizzazione e funzionamento dell'amministrazione giudiziaria (GU 20 agosto 2015, n. 192) (ESTRATTO).

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

Art. 19
Disposizioni in materia di processo civile telematico

1. Al decreto-legge 18 ottobre 2012, n. 179[78], convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:

a) all'articolo 16-bis, sono apportate le seguenti modificazioni:

01) al comma 1 è aggiunto, in fine, il seguente periodo: "In ogni caso, i medesimi dipendenti possono depositare, con le modalità previste dal presente comma, gli atti e i documenti di cui al medesimo comma.";

1) dopo il comma 1 è inserito il seguente:

«1-bis. Nell'ambito dei procedimenti civili, contenziosi e di volontaria giurisdizione innanzi ai tribunali e, a decorrere dal 30 giugno 2015, innanzi alle corti di appello è sempre ammesso il deposito telematico di ogni atto diverso da quelli previsti dal comma 1 e dei documenti che si offrono in comunicazione, da parte del difensore o del dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente, con le modalità previste dalla normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. In tal caso il deposito si perfeziona esclusivamente con tali modalità.»;

1-bis) al comma 2, quarto periodo, dopo le parole: "dal comma 9-bis" sono inserite le seguenti: "e dall'articolo 16-decies";

1-ter) al comma 9 sono aggiunti, in fine, i seguenti periodi:

"Fatto salvo quanto previsto dal periodo precedente, con decreto non avente natura regolamentare il Ministro della giustizia stabilisce misure organizzative per l'acquisizione anche di copia cartacea degli atti depositati con modalità telematiche nonché per la riproduzione su supporto analogico degli atti depositati con le predette modalità, nonché per la gestione e la conservazione delle predette copie cartacee. Con il medesimo decreto sono altresì stabilite le misure organizzative per la gestione e la conservazione degli atti depositati su supporto cartaceo a norma dei commi 4 e 8, nonchè ai sensi del periodo precedente.";

2) al comma 9-bis:

2.1) al primo periodo, dopo le parole: "presenti nei fascicoli informatici" sono inserite le seguenti: "o trasmessi in allegato alle comunicazioni telematiche" e dopo le parole: "firma digitale del cancelliere" sono aggiunte, in fine, le seguenti: "di attestazione di conformità all'originale";

2.2) al secondo periodo, dopo la parola: "difensore," sono inserite le seguenti: "il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente,"));

2-bis) al comma 9-septies sono aggiunti, in fine, i seguenti periodi: "I rapporti riepilogativi di cui al presente comma devono contenere i dati identificativi dell'esperto che ha effettuato la stima. Le disposizioni di cui al presente comma si applicano anche ai prospetti riepilogativi delle stime e delle vendite di cui all'articolo 169-quinquies delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie. Il prospetto riepilogativo deve contenere anche i dati identificativi dell'ufficiale giudiziario che ha attribuito il valore ai beni pignorati a norma dell'articolo 518 del codice di procedura civile.";

2-ter) dopo il comma 9-septies è aggiunto il seguente:

"9-octies. Gli atti di parte e i provvedimenti del giudice depositati con modalità telematiche sono redatti in maniera sintetica";

b) dopo l'articolo 16-novies, introdotto dall'articolo 14, comma 2, del presente decreto, sono aggiunti i seguenti:

«Art. 16-decies. (Potere di certificazione di conformità delle copie degli atti e dei provvedimenti - 1. Il difensore, il dipendente di cui si avvale la pubblica amministrazione per stare in giudizio personalmente, il consulente tecnico, il professionista delegato, il curatore ed il commissario giudiziale, quando

[78] Il testo del d.l. 179/12 riportato nel presente ipertesto è stato integrato con le modifiche del d.l. 83/2015 convertito, con modificazioni, dalla legge n. 132/2015.

depositano con modalità telematiche la copia informatica, anche per immagine, di un atto processuale di parte o di un provvedimento del giudice formato su supporto analogico e detenuto in originale o in copia conforme, attestano la conformità della copia al predetto atto. La copia munita dell'attestazione di conformità equivale all'originale o alla copia conforme dell'atto o del provvedimento».

«Art. 16-undecies (Modalità dell'attestazione di conformità) –

1. Quando l'attestazione di conformità prevista dalle disposizioni della presente sezione, dal codice di procedura civile e dalla legge 21 gennaio 1994, n. 53, si riferisce ad una copia analogica, l'attestazione stessa è apposta in calce o a margine della copia o su foglio separato, che sia pero' congiunto materialmente alla medesima.

2. Quando l'attestazione di conformità si riferisce ad una copia informatica, l'attestazione stessa è apposta nel medesimo documento informatico.

3. Nel caso previsto dal comma 2, l'attestazione di conformità può alternativamente essere apposta su un documento informatico separato e l'individuazione della copia cui si riferisce ha luogo esclusivamente secondo le modalità stabilite nelle specifiche tecniche stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia. Se la copia informatica è destinata alla notifica, l'attestazione di conformità è inserita nella relazione di notificazione.

3-bis. I soggetti di cui all'articolo 16-decies, comma 1, che compiono le attestazioni di conformità previste dalle disposizioni della presente sezione, dal codice di procedura civile e dalla legge 21 gennaio 1994, n. 53, sono considerati pubblici ufficiali ad ogni effetto».

1-bis. All'articolo 3-bis, comma 2, della legge 21 gennaio 1994, n. 53, le parole: "attestandone la conformità all'originale a norma dell'articolo 22, comma 2, del decreto legislativo 7 marzo 2005, n. 82" sono sostituite dalle seguenti: "attestandone la conformità con le modalità previste dall'articolo 16-undecies del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221".

2. Per gli interventi necessari al completamento del processo civile telematico e degli ulteriori processi di digitalizzazione del Ministero della giustizia, ivi compresa la tenuta, con modalità informatiche, degli albi e degli elenchi dei consulenti tecnici, dei periti presso il tribunale, dei professionisti disponibili a provvedere alle operazioni di vendita, è autorizzata la spesa di euro 44,85 milioni per l'anno 2015, di euro 3 milioni per l'anno 2016, di euro 2 milioni per l'anno 2017 e di euro 1 milione annui a decorrere dall'anno 2018.

2-bis. Al codice di cui al decreto legislativo 7 marzo 2005, n. 82, sono apportate le seguenti modificazioni:

a) all'articolo 58, comma 2, dopo le parole: "comunicazione telematica," sono inserite le seguenti: "ivi incluso il Ministero della giustizia,";

b) all'articolo 71, comma 1, dopo le parole: "di concerto con" sono inserite le seguenti: "il Ministro della giustizia e con".

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

(omissis)

Art. 23

Disposizioni transitorie e finali

1. Le disposizioni di cui all'articolo 1 si applicano ai procedimenti di concordato preventivo introdotti anche anteriormente alla data di entrata in vigore del presente decreto. Le disposizioni di cui agli articoli 2, comma 1 si applicano ai procedimenti di concordato preventivo introdotti successivamente all'entrata in vigore del presente decreto. Le disposizioni di cui all'articolo 3 e quelle di cui all'articolo 4, si applicano ai procedimenti di concordato preventivo introdotti successivamente all'entrata in vigore della legge di conversione del presente decreto.

2. Le disposizioni di cui all'articolo 2, comma 2, lettera b), all'articolo 11 nella parte in cui introduce l'ultimo periodo dell'articolo 107, primo comma, del regio decreto 16 marzo 1942, n. 267, all'articolo 13, comma 1, lettera b), numero 1), lettera e), numero 1, lettera ee) e all'articolo 14, comma 1, lettere b) e c) si applicano decorsi trenta giorni dalla pubblicazione in Gazzetta Ufficiale delle specifiche tecniche previste dall'articolo 161-quater delle disposizioni per l'attuazione del codice di procedura civile.

3. Le disposizioni di cui all'articolo 5, comma 1, lettere a) e b), primo e secondo capoverso, e quelle di cui all'articolo 6 si applicano ai fallimenti dichiarati successivamente alla data di entrata in vigore del presente decreto.
4. Le disposizioni di cui all'articolo 5, comma 1, lettera b), terzo capoverso, acquistano efficacia decorsi sessanta giorni dalla pubblicazione sul sito internet del Ministero della giustizia delle specifiche tecniche previste dall'articolo 16-bis, comma 9-septies, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, da adottarsi entro sei mesi dalla data di entrata in vigore del presente decreto.
5. Le disposizioni di cui agli articoli 11, e 2, comma 2, lettere a), b), primo periodo e lettera c) si applicano anche ai fallimenti e ai procedimenti di concordato preventivo pendenti alla data di entrata in vigore del presente decreto.
6. Le disposizioni di cui agli articoli 12 e 13, comma 1, lettere d), l), m), n), si applicano esclusivamente alle procedure esecutive iniziate successivamente alla data di entrata in vigore del presente decreto.
7. Le disposizioni di cui agli articoli 7, 13, comma 1, lettere a), f), numero 1) si applicano a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto.
8. Le disposizioni di cui all'articolo 8 si applicano alle istanze di scioglimento depositate successivamente alla data di entrata in vigore del presente decreto.
9. Le disposizioni di cui all'articolo 13, diverse da quelle indicate nel presente articolo, si applicano anche ai procedimenti pendenti alla data di entrata in vigore del presente decreto. Quando è già stata disposta la vendita, la stessa ha comunque luogo con l'osservanza delle norme precedentemente in vigore e le disposizioni di cui al presente decreto si applicano quando il giudice o il professionista delegato dispone una nuova vendita.
10. Le disposizioni di cui all'articolo 13, comma 1, lettera f), numero 2) e lettera g), si applicano alle vendite disposte dal giudice o dal professionista delegato successivamente alla data di entrata in vigore del presente decreto, anche nelle procedure esecutive pendenti alla medesima data.
11. La disposizione di cui all'articolo 503 del codice di procedura civile, nel testo modificato dall'articolo 19, comma 1, lettera d-bis) del decreto-legge 12 settembre 2014, n. 132, convertito, con modificazioni, dalla legge 10 novembre 2014, n. 162, si applica, a far data dall'entrata in vigore del presente decreto, anche ai procedimenti pendenti alla data di entrata in vigore della legge n. 162 del 2014.
11-bis. Il deposito telematico delle note di iscrizione a ruolo ai sensi dell'articolo 159-ter delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie può essere effettuato dai soggetti di cui all'articolo 16-bis, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, diversi dal creditore, a decorrere dal 2 gennaio 2016.[79].

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

[79] L'art. 14 del d.l. 83/2015 convertito, con modificazioni, dalla legge 132/2015 ha inserito, dopo l'art. 159-bis disp. att. c.p.c., l'art. 159-ter: (Iscrizione a ruolo del processo esecutivo per espropriazione a cura di soggetto diverso dal creditore). - Colui che, prima che il creditore abbia depositato la nota di iscrizione a ruolo prevista dagli articoli 518, 521-bis, 543 e 557 del codice, deposita per primo un atto o un'istanza deve depositare la nota di iscrizione a ruolo e una copia dell'atto di pignoramento. Quando al deposito della nota di iscrizione a ruolo procede uno dei soggetti di cui all'articolo 16-bis, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, diverso dal creditore, il deposito può aver luogo con modalità non telematiche e la copia dell'atto di pignoramento può essere priva dell'attestazione di conformità. Quando l'istanza proviene dall'ufficiale giudiziario, anche nel caso di cui all'articolo 520, primo comma, del codice, all'iscrizione a ruolo provvede d'ufficio il cancelliere. Quando l'iscrizione a ruolo ha luogo a norma del presente articolo, il creditore, nei termini di cui agli articoli 518, 521-bis, 543 e 557 del codice, provvede, a pena di inefficacia del pignoramento, al deposito delle copie conformi degli atti previsti dalle predette disposizioni e si applica l'articolo 164-ter delle presenti disposizioni".

Decreto Legge 3 maggio 2016, n. 59 - Disposizioni urgenti in materia di procedure esecutive e concorsuali, nonché a favore degli investitori in banche in liquidazione *(GU n. 102 del 3-5-2016)* convertito con modificazioni dalla L. 30 giugno 2016, n. 119 (in *G.U. 02/07/2016, n. 153*) (ESTRATTO).

Art. 4
Disposizioni in materia espropriazione forzata

1. Al codice di procedura civile sono apportate le seguenti modificazioni:
a) all'articolo 492, terzo comma, è aggiunto in fine il seguente periodo: «Il pignoramento deve contenere l'avvertimento che, a norma dell'articolo 615, secondo comma, terzo periodo, l'opposizione è inammissibile se è proposta dopo che è stata disposta la vendita o l'assegnazione a norma degli articoli 530, 552 e 569, salvo che sia fondata su fatti sopravvenuti ovvero che l'opponente dimostri di non aver potuto proporla tempestivamente per causa a lui non imputabile.»;
b) all'articolo 503, secondo comma, dopo le parole «dell'articolo 568» sono aggiunte le seguenti: «nonché, nel caso di beni mobili, degli articoli 518 e 540-bis»;
c) all'articolo 532, secondo comma, il secondo e il terzo periodo sono sostituiti dai seguenti: «Il giudice fissa altresì il numero complessivo, non superiore a tre, degli esperimenti di vendita, i criteri per determinare i relativi ribassi, le modalità di deposito della somma ricavata dalla vendita e il termine finale non superiore a sei mesi, alla cui scadenza il soggetto incaricato della vendita deve restituire gli atti in cancelleria. Quando gli atti sono restituiti a norma del periodo precedente, il giudice, se non vi sono istanze a norma dell'articolo 540-bis, dispone la chiusura anticipata del processo esecutivo, anche quando non sussistono i presupposti di cui all'articolo 164-bis delle disposizioni di attuazione del presente codice.»;
d) all'articolo 560:
01) il terzo comma è sostituito dal seguente: "Il giudice dell'esecuzione dispone, con provvedimento impugnabile per opposizione ai sensi dell'articolo 617, la liberazione dell'immobile pignorato senza oneri per l'aggiudicatario o l'assegnatario o l'acquirente, quando non ritiene di autorizzare il debitore a continuare ad abitare lo stesso, o parte dello stesso, ovvero quando revoca l'autorizzazione, se concessa in precedenza, ovvero quando provvede all'aggiudicazione o all'assegnazione dell'immobile. Per il terzo che vanta la titolarità di un diritto di godimento del bene opponibile alla procedura, il termine per l'opposizione decorre dal giorno in cui si è perfezionata nei confronti del terzo la notificazione del provvedimento".
1) il quarto comma è sostituito dal seguente: «Il provvedimento è attuato dal custode secondo le disposizioni del giudice dell'esecuzione immobiliare, senza l'osservanza delle formalità di cui agli articoli 605 e seguenti, anche successivamente alla pronuncia del decreto di trasferimento nell'interesse dell'aggiudicatario o dell'assegnatario se questi non lo esentano. Per l'attuazione dell'ordine il giudice può avvalersi della forza pubblica e nominare ausiliari ai sensi dell'articolo 68. Quando nell'immobile si trovano beni mobili che non debbono essere consegnati ovvero documenti inerenti lo svolgimento di attività imprenditoriale o professionale, il custode intima alla parte tenuta al rilascio ovvero al soggetto al quale gli stessi risultano appartenere di asportarli, assegnandogli il relativo termine, non inferiore a trenta giorni, salvi i casi di urgenza. Dell'intimazione si dà atto a verbale ovvero, se il soggetto intimato non è presente, mediante atto notificato dal custode. Qualora l'asporto non sia eseguito entro il termine assegnato, i beni o i documenti sono considerati abbandonati e il custode, salvo diversa disposizione del giudice dell'esecuzione, ne dispone lo smaltimento o la distruzione»;
2) al quinto comma, è aggiunto, in fine, il seguente periodo: «Gli interessati a presentare l'offerta di acquisto hanno diritto di esaminare i beni in vendita entro quindici giorni dalla richiesta. La richiesta è formulata mediante il portale delle vendite pubbliche e non può essere resa nota a persona diversa dal custode. La disamina dei beni si svolge con modalità idonee a garantire la riservatezza dell'identità degli interessati e ad impedire che essi abbiano contatti tra loro.»;
e) all'articolo 569, quarto comma, le parole «può stabilire» sono sostituite dalle seguenti: «stabilisce, salvo che sia pregiudizievole per gli interessi dei creditori o per il sollecito svolgimento della procedura,» e dopo le parole «con modalità telematiche» sono aggiunte le seguenti: «, nel rispetto della normativa regolamentare di cui all'articolo 161-ter delle disposizioni per l'attuazione del presente codice»;
e-bis) all'articolo 587, primo comma, le parole: "costituisce titolo esecutivo per il rilascio" sono sostituite dalle seguenti: " é attuato dal custode a norma dell'articolo 560, quarto comma";
f) all'articolo 588, dopo le parole «istanza di assegnazione» sono aggiunte le seguenti: «, per sé o a favore di un terzo,»;

g) dopo l'articolo 590, è inserito il seguente: «Art. 590-bis (Assegnazione a favore di un terzo). - «Il creditore che è rimasto assegnatario a favore di un terzo deve dichiarare in cancelleria, nei cinque giorni dalla pronuncia in udienza del provvedimento di assegnazione ovvero dalla comunicazione, il nome del terzo a favore del quale deve essere trasferito l'immobile, depositando la dichiarazione del terzo di volerne profittare. In mancanza, il trasferimento è fatto a favore del creditore. In ogni caso, gli obblighi derivanti dalla presentazione dell'istanza di assegnazione a norma del presente articolo sono esclusivamente a carico del creditore.»;
h) all'articolo 591, secondo comma, dopo le parole «fino al limite di un quarto» sono aggiunte le seguenti: «e, dopo il quarto tentativo di vendita andato deserto, fino al limite della metà»;
i) all'articolo 596, primo comma: 1) dopo le parole: «provvede a formare un progetto di distribuzione,» sono aggiunte le seguenti: «anche parziale,»;
2) è aggiunto, in fine, il seguente periodo: «Il progetto di distribuzione parziale non può superare il novanta per cento delle somme da ripartire.».
i-bis) all'articolo 596, dopo il secondo comma è aggiunto, in fine, il seguente: "Il giudice dell'esecuzione può disporre la distribuzione, anche parziale, delle somme ricavate, in favore di creditori aventi diritto all'accantonamento a norma dell'articolo 510, terzo comma, ovvero di creditori i cui crediti costituiscano oggetto di controversia a norma dell'articolo 512, qualora sia presentata una fideiussione autonoma, irrevocabile e a prima richiesta, rilasciata da uno dei soggetti di cui all'articolo 574, primo comma, secondo periodo, idonea a garantire la restituzione alla procedura delle somme che risultino ripartite in eccesso, anche in forza di provvedimenti provvisoriamente esecutivi sopravvenuti, oltre agli interessi, al tasso applicato dalla Banca centrale europea alle sue più recenti operazioni di rifinanziamento principali, a decorrere dal pagamento e sino all'effettiva restituzione. La fideiussione è escussa dal custode o dal professionista delegato su autorizzazione del giudice. Le disposizioni del presente comma si applicano anche ai creditori che avrebbero diritto alla distribuzione delle somme ricavate nel caso in cui risulti insussistente, in tutto o in parte, il credito del soggetto avente diritto all'accantonamento ovvero oggetto di controversia a norma del primo periodo del presente comma";
l) all'articolo 615, secondo comma, è aggiunto, in fine, il seguente periodo: «Nell'esecuzione per espropriazione l'opposizione è inammissibile se è proposta dopo che è stata disposta la vendita o l'assegnazione a norma degli articoli 530, 552, 569, salvo che sia fondata su fatti sopravvenuti ovvero l'opponente dimostri di non aver potuto proporla tempestivamente per causa a lui non imputabile.»;
m) all'articolo 648, primo comma, la parola «concede» è sostituita dalle seguenti: «deve concedere».
1-bis. All'articolo 2929-bis del codice civile, i commi secondo e terzo sono sostituiti dai seguenti: "Quando il bene, per effetto o in conseguenza dell'atto, è stato trasferito a un terzo, il creditore promuove l'azione esecutiva nelle forme dell'espropriazione contro il terzo proprietario ed è preferito ai creditori personali di costui nella distribuzione del ricavato. Se con l'atto è stato riservato o costituito alcuno dei diritti di cui al primo comma dell'articolo 2812, il creditore pignora la cosa come libera nei confronti del proprietario. Tali diritti si estinguono con la vendita del bene e i terzi titolari sono ammessi a far valere le loro ragioni sul ricavato, con preferenza rispetto ai creditori cui i diritti sono opponibili. Il debitore, il terzo assoggettato a espropriazione e ogni altro interessato alla conservazione del vincolo possono proporre le opposizioni all'esecuzione di cui al titolo V del libro terzo del codice di procedura civile quando contestano la sussistenza dei presupposti di cui al primo comma o che l'atto abbia arrecato pregiudizio alle ragioni del creditore o che il debitore abbia avuto conoscenza del pregiudizio arrecato. L'azione esecutiva di cui al presente articolo non può esercitarsi in pregiudizio dei diritti acquistati a titolo oneroso dall'avente causa del contraente immediato, salvi gli effetti della trascrizione del pignoramento".
2. All'articolo 16-bis del decreto-legge 18 ottobre 2012 n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni:
a) il comma 9-sexies è sostituito dal seguente: "9-sexies. Il professionista delegato a norma dell'articolo 591-bis del codice di procedura civile, entro trenta giorni dalla notifica dell'ordinanza di vendita, deposita un rapporto riepilogativo iniziale delle attività svolte. A decorrere dal deposito del rapporto riepilogativo iniziale, il professionista deposita, con cadenza semestrale, un rapporto riepilogativo periodico delle attività svolte. Entro dieci giorni dalla comunicazione dell'approvazione del progetto di distribuzione, il professionista delegato deposita un rapporto riepilogativo finale delle attività svolte successivamente al deposito del rapporto di cui al periodo precedente";
b) al comma 9-septies, primo periodo, le parole: «il rapporto riepilogativo finale previsto per i procedimenti di esecuzione forzata» sono sostituite dalle seguenti: «i rapporti riepilogativi previsti per i procedimenti di esecuzione forzata».
2-bis. All'articolo 23, comma 2, del decreto-legge 12 settembre 2014, n. 133, convertito, con modificazioni, dalla legge 11 novembre 2014, n. 164, è aggiunto, in fine, il seguente periodo: "Per il

rilascio dell'immobile il concedente può avvalersi del procedimento per convalida di sfratto, di cui al libro quarto, titolo I, capo II, del codice di procedura civile".
3. Le disposizioni di cui al comma 1, lettere a) e l), si applicano ai procedimenti di esecuzione forzata per espropriazione iniziati successivamente all'entrata in vigore della legge di conversione del presente decreto.
3-bis. Con decreto del Ministro della giustizia, da adottare entro il 30 giugno 2017, è accertata la piena funzionalità del portale delle vendite pubbliche previsto dall'articolo 161-quater delle disposizioni per l'attuazione del codice di procedura civile e disposizioni transitorie, di cui al regio decreto 18 dicembre 1941, n. 1368. Il portale è operativo a decorrere dalla pubblicazione del decreto nella Gazzetta Ufficiale.
4. La disposizione di cui al comma 1, lettera d), n. 1), si applica agli ordini di liberazione disposti, nei procedimenti di esecuzione forzata per espropriazione immobiliare, successivamente al decorso del termine di trenta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.
4-bis. La richiesta di visita di cui all'articolo 560, quinto comma, quarto periodo, del codice di procedura civile[80], introdotto dal comma 1, lettera d), numero 2), del presente articolo, è formulata esclusivamente mediante il portale delle vendite pubbliche a decorrere dal novantesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale del decreto di cui al comma 3-bis.
5. La disposizione di cui al comma 1, lettera e), si applica alle vendite forzate di beni immobili disposte dal giudice dell'esecuzione o dal professionista delegato dopo il novantesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale del decreto di cui al comma 3-bis.
6. Le disposizioni di cui al comma 1, lettere f) e g), si applicano alle istanze di assegnazione presentate, nei procedimenti di esecuzione forzata per espropriazione immobiliare, successivamente al decorso del termine di trenta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.
7. Ai fini dell'applicazione della disposizione di cui alla lettera h), si tiene conto, per il computo del numero degli esperimenti di vendita anche di quelli svolti prima dell'entrata in vigore del presente decreto.

[80] Dal 19 febbraio 2019 per effetto delle modifiche apportate dal D.L. 14 dicembre 2018, n. 135, convertito con modificazioni dalla L. 11 febbraio 2019, n. 12 (in G.U. 12/02/2019, n. 36), l'art. 560 c.p.c. (Modo della custodia) così recita: "Il debitore e il terzo nominato custode debbono rendere il conto a norma dell'articolo 593. Il custode nominato ha il dovere di vigilare affinché il debitore e il nucleo familiare conservino il bene pignorato con la diligenza del buon padre di famiglia e ne mantengano e tutelino l'integrità. Il debitore e i familiari che con lui convivono non perdono il possesso dell'immobile e delle sue pertinenze sino al decreto di trasferimento, salvo quanto previsto dal sesto comma. Il debitore deve consentire, in accordo con il custode, che l'immobile sia visitato da potenziali acquirenti. Le modalità del diritto di visita sono contemplate e stabilite nell'ordinanza di cui all'articolo 569. Il giudice ordina, sentiti il custode e il debitore, la liberazione dell'immobile pignorato per lui ed il suo nucleo familiare, qualora sia ostacolato il diritto di visita di potenziali acquirenti, quando l'immobile non sia adeguatamente tutelato e mantenuto in uno stato di buona conservazione, per colpa o dolo del debitore e dei membri del suo nucleo familiare, quando il debitore viola gli altri obblighi che la legge pone a suo carico, o quando l'immobile non è abitato dal debitore e dal suo nucleo familiare. Al debitore è fatto divieto di dare in locazione l'immobile pignorato se non è autorizzato dal giudice dell'esecuzione. Fermo quanto previsto dal sesto comma, quando l'immobile pignorato è abitato dal debitore e dai suoi familiari il giudice non può mai disporre il rilascio dell'immobile pignorato prima della pronuncia del decreto di trasferimento ai sensi dell'articolo 586".

Decreto del Ministro della Giustizia 5 dicembre 2017 - Accertamento della piena funzionalità dei servizi del Portale delle vendite pubbliche. (18A00149) (GU Serie Generale n.7 del 10-01-2018)

IL MINISTRO DELLA GIUSTIZIA

Visto il regio decreto 28 ottobre 1940, n. 1443, e successive modificazioni, concernente «Codice di procedura civile»;
Visto il regio decreto 18 dicembre 1941, n. 1368, concernente «Disposizioni per l'attuazione del codice di procedure civile e disposizioni transitorie»;
Visto l'art. 18-bis del decreto del Presidente della Repubblica 30maggio 2002, n. 115;
Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale»;
Visto l'art. 7 del decreto del Ministro della giustizia 31 ottobre2006 recante «Individuazione dei siti internet destinati all'inserimento degli avvisi di vendita di cui all'art. 490 del codice di procedura civile»;
Visto il decreto legislativo 14 marzo 2013, n. 33, concernente «Riordino della disciplina riguardante il diritto di accesso civico egli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni»;
Visto il decreto del Ministro della giustizia 26 febbraio 2015, n.32, concernente «Regolamento recante le regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche nei casi previsti dal codice di procedura civile, ai sensi dell'art. 161-ter delle disposizioni per l'attuazione del codice di procedura civile»;
Visto il decreto-legge 27 giugno 2015, n. 83, recante «Misure urgenti in materia fallimentare, civile e processuale civile e di organizzazione e funzionamento dell'amministrazione giudiziaria», convertito con modificazioni dalla legge 6 agosto 2015, n. 132;
Visto il decreto-legge 3 maggio 2016, n. 59, recante «Disposizioni urgenti in materia di procedure esecutive e concorsuali nonché a favore degli investitori in banche in liquidazione» convertito con modificazioni dalla legge 30 giugno 2016, n. 119;
Viste le specifiche tecniche D.G.S.I.A. relative alle modalità di pubblicazione sul Portale delle vendite pubbliche, ai sensi dell'art.161-quater disp. att. codice di procedura civile, nonché relative alle modalità di acquisizione dei dati relativi alle pubblicazioni ed alle informazioni minime relative ai dati da pubblicare sui siti per consentire il monitoraggio ad opera del Portale tramite funzionalità informatizzate ai sensi di quanto previsto dall'art. 7del decreto ministeriale 31 ottobre 2006;
Viste le specifiche tecniche D.G.S.I.A., previste dall'art. 26 del decreto del Ministro della giustizia 26 febbraio 2015, n. 32, recante le regole tecniche e operative per lo svolgimento della vendita dei beni mobili ed immobili con modalità telematiche nei casi previsti dal codice di procedura civile, ai sensi dell'art. 161-ter delle disposizioni per l'attuazione del codice di procedura civile;

E m a n a
il seguente decreto:

Art. 1

è accertata la piena funzionalità dei servizi del Portale delle vendite pubbliche, in conformità all'art. 4, comma 3-bis, del decreto-legge 3 maggio 2016, n. 59, convertito con modificazioni dalla legge 30 giugno 2016 n. 119, concernente «Disposizioni urgenti in materia di procedure esecutive e concorsuali nonché a favore degli investitori in banche in liquidazione»;

Art. 2

Il presente decreto entra in vigore a decorrere dalla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

FINE