

Codice Corso - P15002; P15021; P15048; P15060; P15071.

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.

Sono stati realizzati qui di seguito due indici con collegamenti ipertestuali che consentono, cliccando con il *mouse* sul relativo link, di accedere direttamente al testo del riferimento normativo selezionato.

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

Terminata la lettura, 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

[1] a cura di Pietro Lupi, giudice del Tribunale di Napoli.

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 teste 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 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

1. Legge 21 gennaio 1994, n. 53 (Estratto) (*Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali*).
2. Legge 15 marzo 1997, n. 59 (art. 15) (*legge Bassanini*).
3. 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*).
4. Decreto legislativo 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*) (Estratto).
5. 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*).
6. Decreto legislativo 7 marzo 2005, n. 82 (Estratto) (*C.A.D.*).
7. D.P.C.M. 2 novembre 2005 (*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*).
8. 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).
9. Decreto legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 (art. 16, commi dal 6 al 9, estratto) (*Obbligo delle imprese, dei professionisti e della Pubbliche Amministrazioni di comunicazione del proprio indirizzo PEC*).
10. Decreto Ministeriale 27 aprile 2009 - Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia. Pubblicato nella Gazz. Uff. 11 maggio 2009, n. 107.
11. Decreto legge 29 dicembre 2009, n. 193, convertito con modificazioni in legge 22 febbraio 2010, n. 24 (art. 4, estratto) (*Interventi urgenti in materia di funzionalità del sistema giudiziario*).
12. D.M.G. 21 febbraio 2011, n. 44 (con le modifiche apportate dal D.M.G. 209/2012 e dal D.M.G. 48/2013) (*Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione*).
13. 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).

14. Provvedimento del Responsabile S.I.A. del 16 aprile 2014 (*Specifiche tecniche previste dall'art. 34, c.1, D.M. 44/2011*).
15. 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).
16. 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).
17. 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*).

B - Indice dei riferimenti normativi degli argomenti principali.

Deposito telematico degli atti del Giudice.

- Art. 15 DM 44/2011
- Art. 16 Provv. DGSIA 16.4.2014

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

- Artt. 13 e 14 DM 44/2011
- Artt. 12, 13, 14 e 15 Provv. DGSIA 16.4.2014

Documento informatico.

- 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 (Regole Tecniche)
- D.P.C.M. 13 novembre 2014 (Regole Tecniche)

Domicilio digitale del cittadino

- Art. 3bis CAD
- Art. 62 CAD (Anagrafe nazionale della popolazione residente – ANPR)

Fascicolo informatico.

- Art. 41 CAD
- Art. 9 DM 44/2011
- Art. 11 Provv. DGSIA 16.4.2014
- Artt. 12 e 13 DPR 123/2001
- Art. 13 DPCM 13 novembre 2014

Firma digitale.

- Art. 1 CAD, lett. q, q*bis*, r, s (Definizioni delle firme elettroniche)
- 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 certificatore)

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

Notificazioni e comunicazioni effettuate dalla Cancelleria.

Art. 4 d.l. 193/2009

Art. 16 d.l. 179/2012

Art. 18 Provv. DGSIA 16.4.2014 (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. 18 DM44/20011

Art. 19bis Provv. DGSIA 16.4.2014

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

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

Art. 47, co. 3, CAD (Obbligo per le P.A. di comunicare un proprio indirizzo PEC)

Art. 57 *bis* CAD (Indice degli indirizzi delle pubbliche amministrazioni)

Notifiche telematiche tramite UNEP

Art. 17 Dm 44/2011

Art. 19 Provv. DGSIA 16.4.2014

Obbligatorietà del PCT.

Art. 44 d.l. 90/2014

Art. 16bis d.l. 179/2012

Pagamenti telematici.

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

Art. 4 d.l. 193/2009

Artt. 30 e segg. DM 44/2011

Art. 26 Provv DGSIA 16.4.2014

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

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)

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

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

Portale dei servizi telematici

Art. 6 D.M. 44/2011

Art. 5 Provv. DGSIA 16.4.2014

Protezione dati personali nell'attività giudiziaria

Decreto legislativo 30 giugno 2003, n. 196

REGINDE

Art. 7 D.M. 44/2011

Art. 7, 8, 9 e 9bis Provv. DGSIA 16.4.2014

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. 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 all'originale a norma dell' articolo 22, comma 2, del decreto legislativo 7 marzo 2005, n. 82 . La notifica si esegue mediante allegazione dell'atto da notificarsi al messaggio di posta elettronica certificata.
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 e' 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. 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.
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. 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 e dell'art. 123 delle disposizioni per l'attuazione, transitorie e di coordinamento del codice di procedura civile, 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.

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).

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).

(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*)

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 13 febbraio 2001, n. 123 (in Gazz. Uff., 17 aprile, n. 89). - 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.

(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. E' 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[2]

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)

[2] 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, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, 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 32 della legge 11 febbraio 1994, n. 109, 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)

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 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.[3]

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

[3] 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.

elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi è acquisito il concerto del Ministro delle comunicazioni[4].

ART. 18
Disposizioni finali

1. (omissis)

(ritorna all'indice cronologico)

[4] Per le regole tecniche c.f.r. Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie 2 novembre 2005)

(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:
a) **allineamento dei dati**: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;
b) **autenticazione del documento informatico**: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;
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) **certificati elettronici**: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;
f) **certificato qualificato**: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
g) **certificatore**: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;
h) **chiave privata**: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
i) **chiave pubblica**: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;
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;
l) **dato a conoscibilità limitata**: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;
m) **dato delle pubbliche amministrazioni**: il dato formato, o comunque trattato da una pubblica amministrazione;
n) **dato pubblico**: il dato conoscibile da chiunque;
n-bis) **riutilizzo**: uso del dato di cui all'articolo 2, comma 1, lettera e), del decreto legislativo 24 gennaio 2006, n. 36;
o) **disponibilità**: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;

p) **documento informatico**: 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) **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
q-bis) **firma elettronica avanzata**: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
r) **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
s) **firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario 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) **fruibilità di un dato**: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;
u) **gestione informatica dei documenti**: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
u-bis) **gestore di posta elettronica certificata**: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;
u-ter) **identificazione informatica**: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;
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) **pubbliche amministrazioni centrali**: 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 istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;
aa) **titolare**: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
bb) **validazione temporale**: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

(*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 alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione,

come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.
3. Le disposizioni di cui al capo II, agli articoli 40, 43 e 44 del capo III, nonché al capo IV, si applicano ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.
5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante 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. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.
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, e consultazioni elettorali. Con decreti del Presidente del Consiglio dei Ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria.

SEZIONE II
Diritti dei cittadini e delle imprese

Art. 3
Diritto all'uso delle tecnologie

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni , con i soggetti di cui all'articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.
1-bis. (abrogato)
1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.

Art. 3bis
Domicilio digitale del cittadino
1. Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, è facoltà di ogni cittadino indicare alla pubblica amministrazione, secondo le modalità stabilite al comma 3, un proprio indirizzo di posta elettronica certificata, rilasciato ai sensi dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, quale suo domicilio digitale.
2. L'indirizzo di cui al comma 1 è inserito nell'Anagrafe nazionale della popolazione residente-ANPR e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi.
3. Con decreto del Ministro dell'interno, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro delegato per l'innovazione tecnologica, sentita l'Agenzia per l'Italia digitale, sono definite le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino, nonché le modalità di consultazione dell'ANPR da parte dei gestori o esercenti di pubblici servizi ai fini del reperimento del domicilio digitale dei propri utenti.
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 il cittadino esclusivamente tramite il domicilio digitale dallo stesso 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 di cui al comma 1, le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, 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 comma 4-bis 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 cittadino contenga una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso l'amministrazione in conformità alle regole tecniche di cui all'articolo 71.
4-quater. Le modalità di predisposizione della copia analogica di cui ai commi 4-bis e 4-ter soddisfano le condizioni di cui all'articolo 23-ter, comma 5, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.
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*)

Art.4
Partecipazione al procedimento amministrativo informatico

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

Art. 5
Effettuazione di pagamenti con modalità informatiche

1. I soggetti di cui all' **articolo** 2, comma 2 , e, [limitatamente ai rapporti con l'utenza,] i gestori di pubblici servizi nei rapporti con l'utenza sono tenuti a far data dal 1° giugno 2013 ad accettare i pagamenti ad essi spettanti, a qualsiasi titolo dovuti, anche con l'uso delle tecnologie dell'informazione e della comunicazione. A tal fine:

a) sono tenuti a pubblicare nei propri siti istituzionali e a specificare nelle richieste di pagamento:
   1) i codici IBAN identificativi del conto di pagamento, ovvero dell'imputazione del versamento in Tesoreria, di cui all'articolo 3 del decreto del Ministro dell'economia e delle finanze 9 ottobre 2006, n. 293 , tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale;
   2) i codici identificativi del pagamento da indicare obbligatoriamente per il versamento;

b) si avvalgono di prestatori di servizi di pagamento, individuati mediante ricorso agli strumenti di acquisto e negoziazione messi a disposizione da Consip o dalle centrali di committenza regionali di riferimento costituite ai sensi dell' articolo 1, comma 455, della legge 27 dicembre 2006, n. 296 , per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito, prepagate ovvero di altri strumenti di pagamento elettronico disponibili, che consentano anche l'addebito in conto corrente, indicando sempre le condizioni, anche economiche, per il loro utilizzo. Il prestatore dei servizi di pagamento, che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito, i codici identificativi del pagamento medesimo, nonché i codici IBAN identificativi dell'utenza bancaria ovvero

dell'imputazione del versamento in Tesoreria. Le modalità di movimentazione tra le sezioni di Tesoreria e Poste Italiane S.p.A. dei fondi connessi alle operazioni effettuate sui conti correnti postali intestati a pubbliche amministrazioni sono regolate dalla convenzione tra il Ministero dell'economia e delle finanze e Poste Italiane S.p.A. stipulata ai sensi dell'articolo 2, comma 2, del decreto-legge 1° dicembre 1993, n. 487, convertito, con modificazioni, dalla legge 29 gennaio 1994, n. 71.
2. Per le finalità di cui al comma 1, lettera b), le amministrazioni e i soggetti di cui al comma 1 possono altresì avvalersi dei servizi erogati dalla piattaforma di cui all'articolo 81 comma 2-bis e dei prestatori di servizi di pagamento abilitati.
3. [Dalle previsioni di cui al comma 1 sono escluse le operazioni di competenza delle Agenzie fiscali, ai sensi degli articoli 62 e 63 del decreto legislativo 30 luglio 1999, n. 300 , nonché delle entrate riscosse a mezzo ruolo.] Dalle previsioni di cui alla lettera a) del comma 1 possono essere escluse le operazioni di pagamento per le quali la verifica del buon fine dello stesso debba essere contestuale all'erogazione del servizio; in questi casi devono comunque essere rese disponibili modalità di pagamento di cui alla lettera b) del medesimo comma 1 .
3-bis. I micro-pagamenti dovuti a titolo di corrispettivo dalle pubbliche amministrazioni di cui all'articolo 1, comma 450, della legge 27 dicembre 2006, n. 296, come modificato dall' articolo 7, comma 2, del decreto- legge 7 maggio 2012, n. 52 , convertito, con modificazioni, dalla legge 6 luglio 2012, n. 94, per i contratti di acquisto di beni e servizi conclusi tramite gli strumenti elettronici di cui al medesimo articolo 1, comma 450, stipulati nelle forme di cui all'**articolo** 11, comma 13, del **codice** di cui al decreto legislativo 12 aprile 2006, n. 163, e successive modificazioni, sono effettuati mediante strumenti elettronici di pagamento se richiesto dalle imprese fornitrici.
3-ter. Con decreto del Ministero dell'economia e delle finanze da pubblicare entro il 1° marzo 2013 sono definiti i micro-pagamenti in relazione al volume complessivo del contratto e sono adeguate alle finalità di cui al comma 3-bis le norme relative alle procedure di pagamento delle pubbliche amministrazioni di cui al citato articolo 1, comma 450, della legge n. 296 del 2006 . Le medesime pubbliche amministrazioni provvedono ad adeguare le proprie norme al fine di consentire il pagamento elettronico per gli acquisti di cui al comma 3-bis entro il 1° gennaio 2013.
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, lettere a) e b) 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.

(*torna all'indice per argomenti*)

Art. 5 bis
Comunicazioni tra imprese e amministrazioni pubbliche

(omissis)

Art. 6
Utilizzo della posta elettronica certificata

1. Per le comunicazioni di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.
1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali.

Art. 6bis
Indice nazionale degli indirizzi PEC 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 la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (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 .
3. L'accesso all'INI-PEC è consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web e senza necessità di autenticazione. L'indice è realizzato in formato aperto, secondo la definizione di cui all'articolo 68, comma 3.
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 decreto, da emanare entro 60 giorni dalla data di entrata in vigore della presente disposizione, le modalità di accesso e di aggiornamento.
5. Nel decreto 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.

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

(omissis)

Art. 8
Alfabetizzazione informatica dei cittadini

1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.

Art. 9
Partecipazione democratica elettronica

(omissis)

Art. 10
Sportello unico per le attività produttive

(omissis)

Art. 11
Registro informatico degli adempimenti amministrativi per le imprese

(omissis)

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

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 la garanzia dei diritti dei cittadini e delle imprese di cui al capo I, sezione II, del presente decreto.

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 decreto.

1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto 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 decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.

2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le 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.

4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.

5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

5-bis. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione attraverso le tecnologie dell'informazione e della comunicazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

Art. 13

Formazione informatica dei dipendenti pubblici

1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'ambito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di 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.

Art. 14

Rapporti tra Stato, Regioni e autonomie locali

(omissis)

Art. 15

Digitalizzazione e riorganizzazione

(omissis)

Art. 16

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

(omissis)

Art. 17

Strutture per l'organizzazione, l'innovazione e le tecnologie

1. Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine, le predette amministrazioni individuano un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, responsabile del coordinamento funzionale. Al predetto ufficio afferiscono i compiti relativi a:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di [sicurezza,] accessibilità e fruibilità.

1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.

1-ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalità di cui all'articolo 51.

Art. 18

Conferenza permanente per l'innovazione tecnologica

(omissis)

Art. 19

Banca dati per la legislazione in materia di pubblico impiego

(omissis)

CAPO II
DOCUMENTO INFORMATICO E FIRME ELETTRONICHE; TRASFERIMENTI DI FONDI, LIBRI E SCRITTURE

SEZIONE I
Documento informatico

Art. 20

Documento informatico

1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

2. (abrogato)

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71.

La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

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 regole tecniche dettate ai sensi dell'articolo 71.

(*torna all'indice per argomenti*)

Art. 21

Documento informatico sottoscritto con firma elettronica.

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità , sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria[5].

2-bis). Salvo quanto previsto dall'articolo 25, 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, numero 13) del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.[6]

---

[5] Art. 2702. (Efficacia della scrittura privata): "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".

[6] 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".

3. L'apposizione ad 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. 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. 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 di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
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.
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 ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.[7]
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, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.
3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 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, 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.[8]
6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione

---

[7] Art. 2714 (copie di atti pubblici): "Le copie di atti pubblici spedite nelle forme prescritte da depositari pubblici autorizzati fanno fede come l'originale. La stessa fede fanno le copie di atti pubblici originali, spedite da depositari pubblici di esse, a ciò autorizzati".
Art. 2715 (copie di scritture private originali): "Le copie delle scritture private depositate presso pubblici uffici e spedite da pubblici depositari autorizzati hanno la stessa efficacia della scrittura originale da cui sono estratte".

[8] Cfr: DPCM 21 marzo 2013 che tra i documenti analogici originali unici per i quali permane l'obbligo della conservazione dell'originale cartaceo indica nell'allegato "gli atti giudiziari, processuali e di polizia giudiziaria per i venti anni successivi".

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.

(*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.

(*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 regole tecniche di cui all'articolo 71.
2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, 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.
2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.[9]
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 regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.
4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentiti DigitPA e il Garante per la protezione dei dati personali.
5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il 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

[9] Art. 2702. (Efficacia della scrittura privata): "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".

legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.
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".[10]

SEZIONE II
Firme elettroniche e certificatori

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 regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.[11]

(*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 avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato[12].
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*)

---

[10] 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".

[11] Cfr.: DPCM 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 CAD.

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

Art. 26
Certificatori

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, qualora emettano certificati qualificati, devono 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.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE .

(*torna all'indice per argomenti*)

Art. 27
Certificatori qualificati

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1, devono inoltre:
a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
b) utilizzare 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 delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;
c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;
e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.
3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.
4. Il CNIPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

Art. 28
Certificati qualificati

1. I certificati qualificati devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.
2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui 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 generale.
3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:
a) le qualifiche specifiche del titolare, 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.
3-bis. Le informazioni di cui al comma 3 possono essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con decreto del Presidente del Consiglio dei Ministri sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali.
4. Il titolare, 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.

Art. 29
Accreditamento

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.
2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:
a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;
b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.
4. La domanda 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 del CNIPA 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 CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
8. Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo.
9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 30
Responsabilità del certificatore

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:
a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
d) sull'adempimento degli obblighi a suo carico previsti dall' articolo 32.
2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto. dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.
3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato. secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite (1).

(1) Comma modificato dall'articolo 13 del D.Lgs. 4 aprile 2006, n. 159.

Art. 31
Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata.

1. DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.

Art. 32
Obblighi del titolare e del certificatore

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma 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 certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:
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 regole tecniche di cui all'articolo 71, 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 regole tecniche di cui all'articolo 71;
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) *soppressa*;]
g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;
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 DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.
4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, 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 certificatori qualificati e per i gestori di posta elettronica certificata.

1. Qualora si verifichi, salvi i casi di forza maggiore o caso fortuito, un malfunzionamento nel sistema che determini un disservizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se il disservizio ovvero la mancata o

intempestiva comunicazione sono reiterati per due volte nel corso di un biennio, successivamente alla seconda diffida si applica la sanzione della cancellazione dall'elenco pubblico.
2. Qualora si verifichi, fatti salvi i casi di forza maggiore o di caso fortuito, un malfunzionamento nel sistema che determini l'interruzione del servizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi 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 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. Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto da DigitPA nell'esercizio delle attività di vigilanza di cui all'articolo 31 si applica la disposizione di cui al comma 2.

Art. 33
Uso di pseudonimi

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale.
Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno venti anni decorrenti dall'emissione del certificato stesso.

Art. 34
Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati

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 accreditarsi 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. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;
b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.
5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

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.
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, 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 qualificata prescritti dall'allegato III della direttiva 1999/93/CE 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 11, paragrafo 1, lettera b), della direttiva 1999/93/CE.

(*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 regole tecniche di cui all'articolo 71.
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 regole tecniche di cui all'articolo 71.

Art. 37

Cessazione dell'attività

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al CNIPA 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 certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.
4. Il CNIPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.
4-bis. Qualora il certificatore qualificato cessi la propria attività senza indicare, ai sensi del comma 2, un certificatore 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 DigitPA che ne garantisce la conservazione e la disponibilità.

(omissis)

CAPO III

FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

(omissis)

Art. 41
Procedimento e fascicolo informatico

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.
1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all' articolo 54 , commi 2-ter e 2-quater .
2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque 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. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo 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; regole tecniche specifiche possono essere dettate ai sensi dell' articolo 71 , di concerto con il Ministro della funzione pubblica.
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 .
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; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 .

3. Ai sensi degli articoli da 14 a 14-quinquies della legge 7 agosto 1990, n. 241 , previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

(*torna all'indice per argomenti*)

(omissis)

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[, ivi compreso il fax], idoneo ad accertarne la fonte di 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
(omissis)

Art. 47
Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono [di norma] 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.
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 decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all' articolo 71. È in ogni caso esclusa la trasmissione di documenti a mezzo fax;
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
3. Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. La 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).

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 decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

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 al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

(*torna all'indice per argomenti*)

(omissis)

CAPO V
DATI DELLE PUBBLICHE AMMINISTRAZIONI E SERVIZI IN RETE

SEZIONE I
Dati delle pubbliche amministrazioni

(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 [della rete Internet] 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 [della rete Internet], 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
(*omissis*)

Art. 57 *bis*
Indice degli indirizzi delle pubbliche amministrazioni

1. Al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è istituito l'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi, nel quale sono indicati gli indirizzi di posta elettronica certificata 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 ed i privati.
2. La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.
3. Le amministrazioni aggiornano gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale secondo le indicazioni di DigitPA. 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*)

(omissis)

Art. 62
Anagrafe nazionale della popolazione residente - ANPR

1. È istituita presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente (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 quinto comma 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 di cui all'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del Garante 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 altresi' 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.
3. L'ANPR assicura al singolo comune la disponibilità dei dati anagrafici della popolazione residente 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, nonché la disponibilità dei dati anagrafici e dei servizi per l'interoperabilità con le banche dati tenute dai comuni per lo svolgimento delle funzioni di competenza. L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafici nel rispetto di quanto previsto dall'articolo 33 del decreto del Presidente della Repubblica 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 alle pubbliche amministrazioni e agli organismi che erogano pubblici servizi 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, le pubbliche amministrazioni di cui all' articolo 2, comma 2, del presente Codice 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, la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nonché 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 58;
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 decreto, 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 e dei certificati di cui all' articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, 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*)

CAPO VII
REGOLE TECNICHE

Art. 71
Regole tecniche[13]

1. Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ed il Garante per la protezione dei dati personali nelle materie di competenza, previa acquisizione obbligatoria del parere tecnico di DigitPA.
[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. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.

(omissis)

Per le regole tecniche in materia di documento informatico v. D.P.C.M. 13 novembre 2014.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

[13] Per le regole tecniche in materia di documento informatico v. D.P.C.M. 13 novembre 2014.

DECRETO 2 novembre 2005
PRESIDENZA DEL CONSIGLIO DEI MINISTRI DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE
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 ettronica 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 é 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 é 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 é 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 é 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 é 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 é 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, é 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 é 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 é 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 é 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 é tenuto a trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato.
2. Il gestore é tenuto ad informare il mittente che il messaggio inviato contiene virus.
3. Il gestore é 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, é 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 é 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 é 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 é 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 é 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 é 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-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.] [14]

[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.] [15]

[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.] [16]

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.

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" [17];

---

[14] Il testo originario del primo 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.

[15] 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.

[16] 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.

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 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*)

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

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*)[18]

(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[19].

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*)

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

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

Decreto Ministeriale 27 aprile 2009 - Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia. Pubblicato nella Gazz. Uff. 11 maggio 2009, n. 107.

(ritorna all'indice cronologico)

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. E' 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. E' 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 (in Gazz. Uff., 30 dicembre, n. 302). - Decreto convertito con modificazioni in legge 22 febbraio 2010, n. 24. - Interventi urgenti in materia di funzionalità del sistema giudiziario. (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*)

DECRETO DEL MINISTERO DELLA GIUSTIZIA 21 febbraio 2011 n. 44 (in Gazz. Uff., 18 aprile, n. 89). - 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.
(testo vigente)

(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*)

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.[20]
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.[21]
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,

---

[20] 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".

[21] Comma così modificato dal D.M. 209/2012.

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*)

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[22]

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.

(*torna all'indice per argomenti*)

Art. 19

Disposizioni particolari per la fase delle indagini preliminari

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

(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.

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)

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) [23].

(ritorna all'indice cronologico)

Art. 4
Domicilio digitale del cittadino

1. Dopo l'articolo 3 del decreto legislativo 7 marzo 2005, n. 82, e' 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, e' 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, e' 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 e' aggiunto il seguente: «Quando viene trasmesso a mezzo posta elettronica certificata il biglietto di cancelleria e' 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

[23] Testo aggiornato al D.l. 132/2014 conv., con modificazioni, nella legge 162/2014.

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 e' redatta in forma automatica dai sistemi informatici in dotazione alla cancelleria.
5. La notificazione o comunicazione che contiene dati sensibili e' 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 modalita' 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 puo' 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 e' 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.
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 e' 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 e' 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 e' autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

(*torna all'indice per argomenti*)

Art. 16-bis
(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.
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 presente comma, il difensore attesta la conformità delle copie agli originali, anche fuori dai casi previsti dal comma 9-bis.[24]
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

[24] 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.

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 è 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 e' eseguito entro la fine del giorno di scadenza.[25]
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.
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 dei procedimenti indicati nel presente articolo, equivalgono all'originale anche se prive della firma digitale del cancelliere. Il difensore, 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 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.
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

[25] Comma così modificato dall'art. 51 del d.l. 90/2014, conv. con modif. dalla legge 114/2014.

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.
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.
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-ter, sostituendo il commissario al curatore.
9-sexies. Entro dieci giorni dall'approvazione del progetto di distribuzione, il professionista delegato a norma dell'articolo 591-bis del codice di procedura civile deposita un rapporto riepilogativo finale delle attività svolte.
9-septies. I rapporti riepilogativi periodici e finali previsti per le procedure concorsuali e il rapporto riepilogativo finale previsto 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.

(*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 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.

(ritorna all'indice cronologico)

(*torna all'indice per argomenti*)

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.*

(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

1. 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

1. Ai fini del presente provvedimento, oltre alle definizioni contenute nell'articolo 2 del regolamento, si intende:
    1. **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 modificazioni;

2. **CAD**: codice dell'amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni);
3. **CNS**: Carta Nazionale dei Servizi;
4. **CSV**: Comma-separated values;
5. **DTD**: Document Type Definition;
6. **DGSIA**: Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia;
7. **GSU**: Sistema di gestione informatizzata dei registri per gli uffici notifiche e protesti;
8. **HSM**: Hardware Security Module;
9. **HTTPS**: HyperText Transfer Protocol over Secure Socket Layer;
10. **IMAP**: Internet Message Access Protocol;
11. **PdA**: Punto di Accesso, come definito all'art. 23 del regolamento;
12. **PEC**: Posta Elettronica Certificata;
13. POP: Post Office Protocol;
14. **PP.AA**.: Pubbliche Amministrazioni;
15. **RdA**: Ricevuta di Accettazione della Posta Elettronica Certificata;
16. **RdAC**: Ricevuta di Avvenuta Consegna della Posta Elettronica Certificata;
17. **ReGIndE**: Registro Generale degli Indirizzi Elettronici, come definito all'art. 7 del regolamento;
18. **SMTP**: Simple Mail Transfer Protocol;
19. **UU.GG**.: Uffici Giudiziari;
20. **WSDL**: Web Services Definition Language;
21. **XML**; eXtensible Markup Language;
22. **XSD**: XML Schema Definition;
23. **SPC**: Sistema Pubblico di Connettività;
24. **PKCS#11**: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite apposita sequenza di chiamate al token per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di identificazione;
25. **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;
26. **PAdES** (PDF Advanced Electronic Signature): formato di busta crit-tografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;
27. **OID** (Object IDentifier): codice univoco basato su una sequenza ordi-nata 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 univoca in ambito mondiale;
28. **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).

CAPO II – SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Art. 3

Infrastrutture informatiche – art. 3 del regolamento

1. 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).

2. Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.
3. 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.
4. 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".
5. 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.
6. 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

1. 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.
2. 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.
3. Il gestore dei servizi telematici utilizza i protocolli POP3, POP3S, IMAP, IMAPS e SMTP per collegarsi al gestore di posta elettronica certificata del Ministero.
4. 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.
5. Non possono essere utilizzate caselle di PEC diverse da quelle di cui ai commi precedenti per la trasmissione e il deposito di atti processuali.
6. 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:
    1. il codice identificativo univoco assegnato al messaggio originale;
    2. la data e l'ora dell'evento;
    3. il mittente del messaggio originale;
    4. i destinatari del messaggio originale;
    5. l'oggetto del messaggio originale;
    6. il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
    7. il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
    8. il gestore mittente.
7. 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.
8. I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.
9. 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

1. 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".
2. 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:
    1. Informazioni e documentazione sui servizi telematici del dominio giustizia;
    2. Raccolte giurisprudenziali;
    3. Informazioni essenziali sullo stato dei procedimenti pendenti, rese di-sponibili 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).
3. 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.
4. 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.
5. 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

1. 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:
    1. 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.
    2. 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.
    3. 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.
    4. 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.

2. 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.
3. Il Ministero della giustizia verifica, anche attraverso opportune visite ispettive, che i punti di accesso rispettino i predetti requisiti.
4. 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.
5. 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

1. 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.
2. Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al presente regolamento.
3. I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l'inserimento manuale dei dati.
4. Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:
    1. 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.);
    2. professionisti iscritti in albi ed elenchi istituiti con legge (ad esempio Consiglio dell'ordine degli avvocati o Consiglio nazionale del Notariato);
    3. 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).
5. 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.
6. Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.
7. 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

1. 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:
    1. l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;
    2. 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;
    3. la casella di PEC utilizzata per l'invio dell'albo.

2. 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.
3. Terminate le operazioni di censimento da parte del responsabile per i si-stemi 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:
    1. il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;
    2. non vi sono vincoli sull'oggetto né sul corpo del messaggio;
    3. l'indirizzo di PEC mittente deve essere censito tra quelli delegati all'invio e riportati nel documento di censimento;
    4. deve essere allegato un solo file (ComunicazioniSoggetti.xml o, per le Pubbliche Amministrazioni, ComunicazioneSoggettiPPAA.xml), sotto-scritto con firma digitale o firma elettronica qualificata;
    5. 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;
    6. il file ComunicazioniSoggetti.xml o il file ComunicazioneSogget-tiPP.AA.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;
    7. il codice ente specificato nel file deve essere tra quelli censiti.
4. 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.
5. 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.
6. 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).
7. 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

1. 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.
2. 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.
3. 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

1. 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.

2. 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:
    1. descrizione e codice fiscale della pubblica amministrazione;
    2. nominativo, codice fiscale e recapiti del soggetto incaricato di inserire o modificare gli indirizzi di PEC della pubblica amministrazione sul portale dei servizi telematici;
3. 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:
    1. l'indirizzo di PEC della pubblica amministrazione;
    2. 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.
4. 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.
5. 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

1. 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:
    1. ricezione, accettazione e trasmissione dei dati e dei documenti informatici;
    2. consultazione e gestione del fascicolo informatico.
2. 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.
3. 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

1. 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.
2. 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.

3. Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:
    1. il codice fiscale del soggetto che ha effettuato l'accesso;
    2. il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);
    3. 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

1. L'atto del processo in forma di documento informatico, da depositare telematicamente all'ufficio giudiziario, rispetta i seguenti requisiti:
    1. è in formato PDF;
    2. è privo di elementi attivi;
    3. 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;
    4. è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;
    5. 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.
2. 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.
3. 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

1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:
    1. .pdf
    2. .rtf
    3. .txt
    4. .jpg
    5. .gif
    6. .tiff
    7. .xml
    8. .eml, purché contenenti file nei formati di cui alle lettere precedenti.

9. .msg, purché contenenti file nei formati di cui alle lettere da a ad h.

2. È consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti al comma precedente:
    1. .zip
    2. .rar
    3. .arj.
3. 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

1. 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:
    1. 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).
    2. DatiAtto.xml: gli XSD sono riportati nell'Allegato 5.
    3. <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.
    4. 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.
2. 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).
3. La dimensione massima consentita per la busta telematica è pari a 30 Megabyte.
4. 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.
5. 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:
    1. T001: l'indirizzo del mittente non è censito in ReGIndE;
    2. T002: Il formato del messaggio non è aderente alle specifiche;
    3. T003: la dimensione del messaggio eccede la dimensione massima consentita.
6. 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.
7. 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:
    1. 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);

2. 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);
3. FATAL: eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fondamentali per l'elaborazione).

8. La codifica puntuale degli errori indicati al comma precedente è pubblicata e aggiornata nell'area pubblica del portale dei servizi telematici.
9. 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.
10. 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.

(*torna all'indice per argomenti*)

Art. 15

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

1. 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:
    1. numero di ruolo della causa;
    2. progressivo dell'allegato;
    3. 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

1. 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.
2. 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.
3. 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

1. 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).
2. 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 PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.
3. 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.

Art. 18

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

1. 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.
2. 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.
3. 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:
    1. il codice fiscale del soggetto che ha effettuato il prelievo o la consultazione;
    2. il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 4);
    3. la data e l'ora di invio dell'avviso;
    4. la data e l'ora del prelievo o della consultazione.
4. Le informazioni di cui al comma precedente vengono conservate per cinque anni.
5. 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

1. 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.
2. 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.
3. All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.
4. 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.
5. 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:
    1. 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;
    2. imprese iscritte nel relativo registro: ai sensi dell'articolo 7, comma 5;
    3. cittadini: ai sensi dell'articolo 7, comma 5.

6. 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

1. 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.
2. 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.
3. 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.
4. 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.
5. 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. 20

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

1. (omissis)

Art. 21

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

1. 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

1. 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.
2. Il soggetto che ne ha diritto può richiedere:
    1. copia semplice in formato digitale;
    2. copia semplice per l'avvocato non costituito in formato digitale;
    3. copia autentica in formato digitale;
    4. copia esecutiva in formato digitale;
    5. copia semplice in formato cartaceo;
    6. copia autentica in formato cartaceo;
    7. copia esecutiva in formato cartaceo.
3. 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.

4. 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

1. 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.
2. 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

1. 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).
2. 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.
3. 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.
4. I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne.
5. Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

11. 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.
12. I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
13. 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.
14. 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:
    1. struttura logistica e operativa dell'organizzazione;
    2. ripartizione e definizione delle responsabilità del personale addetto;
    3. descrizione dei dispositivi installati;
    4. descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);
    5. descrizione delle procedure di registrazione delle utenze;
    6. descrizione relativa all'implementazione dei meccanismi di identificazione informatica;
    7. qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;
    8. procedura di gestione delle copie di sicurezza dei dati;
    9. procedura di gestione dei disastri;
    10. analisi dei rischi e contromisure previste;
    11. 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;
    12. descrizione della modalità di verifica dell'effettiva funzionalità e adeguatezza del sistema di sicurezza del punto di accesso.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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

1. L'utente accede ai servizi di consultazione previa registrazione presso un punto di accesso autorizzato o presso il portale dei servizi telematici.

2. 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:
    1. nome e cognome
    2. luogo e data di nascita
    3. residenza
    4. domicilio
    5. ruolo
    6. consiglio dell'ordine o ente di appartenenza.
3. I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per cinque anni.
4. 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.
5. 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.
6. 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.
7. 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

1. 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.
2. 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.
3. 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.
4. 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;
5. 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.
6. 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.

7. 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.
8. 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.
9. 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
10. 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

1. 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:
    1. definisce gli elementi necessari a caratterizzare i pagamenti, in particolare qualifica il versamento attraverso un identificativo univoco di cui al successivo comma 5;
    2. 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;
    3. viene predisposta dal soggetto che procede al pagamento ed inviata dal portale dei servizi telematici al Nodo dei Pagamenti-SPC;
2. 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:
    1. 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);
    2. trasferisce inalterate le stesse informazioni ricevute in ingresso (RPT) relative alla parte riservata (Dati Specifici Riscossione) a disposizione della PA
3. 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.
4. 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.
5. 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:
    1. <check digit> costituisce il codice numerico di controllo (2 posizioni);
    2. <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.

6. 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).
7. 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

1. 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.
2. 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
3. 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.
4. Il sistema RRT permette la gestione delle RT e dei relativi identificativi univoci di pagamento secondo le modalità indicate nell'articolo 27.
5. 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.
6. 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

1. 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.
2. 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

1. 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.

2. 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.
3. A decorrere dalla comunicazione di cui al comma 1, il gestore dei servizi telematici:
    1. Invia comunicazioni e notificazioni solamente alla casella di PEC ivi indicata;
    2. Consente la ricezione di atti solo tramite PEC, rifiutando automatica-mente il deposito tramite altro canale.
4. 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

1. 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.

(ritorna all'indice cronologico)

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)

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 (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. Quando è eseguita dopo le ore 21, la notificazione si considera perfezionata alle ore 7 del giorno successivo».
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)[26]
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, e' 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 e' 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

[26] Cfr: legge 53/1994 come modificata da questo comma.

elettronica certificata. Il deposito è tempestivo quando è eseguito entro la fine del giorno di scadenza».

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:
«9 -*bis* . (*omissis*) »;[27]
b) dopo l'art. 16 -*quinquies* è inserito il seguente:
«Art. 16-sexies (Domicilio digitale). — 1. Salvo quanto previsto dall'art. 366 del codice di procedura civile, 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.».
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)

[27] Cfr.: art. 16bis d.l. 179/2012 come modificato da quest'articolo.

Decreto-legge 12 settembre 2014, n. 132, recante "Misure urgenti di degiurisdizionalizzazione ed altri interventi per la definizione dell'arretrato in materia di processo civile" coordinato con la Legge di conversione 10 novembre 2014, n. 162 (Estratto).

(ritorna all'indice cronologico)

(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, nonchè 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, puo' 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)[28]

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.

[28] Cfr.: art. 16bis d.l. 179/2012 come modificato da questo articolo.

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, 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 puo' 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 puo' 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 puo' 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 puo' interrogare tramite collegamento telematico diretto o mediante richiesta al titolare dei dati.
Il Ministro della giustizia puo' 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, puo' 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)[29]
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 e' 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*)

[29] 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*).

(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.

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 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*)

FINE