DIRETTIVA (UE) 2019/770 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

20 Maggio 2019

relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali (Testo rilevante ai fini del SEE)

Leggi: DIRETTIVA (UE) 2019-770 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 20 05 2019

Responsabilità del cancelliere e dell'ufficiale giudiziario, c.p.c. art. 60

20 Maggio 2019

c.p.c. art. 60. Responsabilità del cancelliere e dell'ufficiale giudiziario

Il cancelliere e l'ufficiale giudiziario sono civilmente responsabili [Cost. 28]:

1) quando, senza giusto motivo, ricusano di compiere gli atti che sono loro legalmente richiesti oppure omettono di compierli nel termine che, su istanza di parte, è fissato dal giudice dal quale dipendono o dal quale sono stati delegati;

2) quando hanno compiuto un atto nullo con dolo o colpa grave.

Codice dei Contratti pubblici: i chiarimenti dell'ANAC sugli acquisti di importo inferiore ad € 1.000

20 Maggio 2019

L'Autorità Nazionale anti corruzione con comunicato del Presidente del 30.11.2018 pubblicato sul sito istituzionale in data 12.11-2018 ha reso noto che sono giunte richieste di chiarimento in merito all'applicabilità dell'art.40, comma 2, del Codice dei contratti pubblici agli acquisti di importo inferiore a 1.000 euro.

In particolare, è stato chiesto se, in relazione alla disposizione recata dall'art. 40, co. 2 del Codice, sia consentito, per gli affidamenti infra 1.000 euro, procedere senza utilizzare mezzi telematici, in attuazione di quanto previsto dall'art. 1, co. 450 della legge 27 dicembre 2006, n. 296.

L’Autorità ritiene che, per gli acquisti infra 1.000 euro, permanga la possibilità di procedere senza l’acquisizione di comunicazioni telematiche, in forza della disposizione normativa da ultimo citata, non abrogata a seguito dell’emanazione del Codice dei contratti pubblici.

Legge 27/12/2006 n. 296

AMMINISTRAZIONE DEL PATRIMONIO E CONTABILITÀ DELLO STATO

Art. 1, co. 450

Le amministrazioni statali centrali e periferiche, ad esclusione degli istituti e delle scuole di ogni ordine e grado, delle istituzioni educative e delle istituzioni universitarie, nonché gli enti nazionali di previdenza e assistenza sociale pubblici e le agenzie fiscali di cui al decreto legislativo 30 luglio 1999, n. 300, per gli acquisti di beni e servizi di importo di importo pari o superiore a 1.000 euro e al di sotto della soglia di rilievo comunitario, sono tenute a fare ricorso al mercato elettronico della pubblica amministrazione di cui all’articolo 328, comma 1, del regolamento di cui al decreto del Presidente della Repubblica 5 ottobre 2010, n. 207. Fermi restando gli obblighi e le facoltà previsti al comma 449 del presente articolo, le altre amministrazioni pubbliche di cui all’articolo 1 del decreto legislativo 30 marzo 2001, n. 165, nonché le autorità indipendenti, per gli acquisti di beni e servizi di importo pari o superiore a 1.000 euro e inferiore alla soglia di rilievo comunitario sono tenute a fare ricorso al mercato elettronico della pubblica amministrazione ovvero ad altri mercati elettronici istituiti ai sensi del medesimo articolo 328 ovvero al sistema telematico messo a disposizione dalla centrale regionale di riferimento per lo svolgimento delle relative procedure. Per gli istituti e le scuole di ogni ordine e grado, le istituzioni educative, tenendo conto delle rispettive specificità, sono definite, con decreto del Ministro dell’istruzione, dell’università e della ricerca, linee guida indirizzate alla razionalizzazione e al coordinamento degli acquisti di beni e servizi omogenei per natura merceologica tra più istituzioni, avvalendosi delle procedure di cui al presente comma. A decorrere dal 2014 i risultati conseguiti dalle singole istituzioni sono presi in considerazione ai fini della distribuzione delle risorse per il funzionamento *(215) (216)*.

(215) Comma così modificato dal comma 2 dell’art. 7, D.L. 7 maggio 2012, n. 52, come sostituito dalla legge di conversione 6 luglio 2012, n. 94, dai nn. 1) e 2) della lettera a) e dalla lettera b) del comma 149 dell’art. 1, L. 24 dicembre 2012, n. 228, a decorrere dal 1° gennaio 2013, ai sensi di quanto disposto dall’art. 1, comma 561, della medesima legge n. 228/2012, dalla lettera b) del comma 8 dell’art. 22, D.L. 24 giugno 2014, n. 90, dall’art. 1, commi 495, lett. b), e 502, lett. a), b) e c), L. 28 dicembre 2015, n. 208, a decorrere dal 1° gennaio 2016, e, successivamente, dall’art. 1, comma 1, D.Lgs. 22 gennaio 2016, n. 10, a decorrere dal 29 gennaio 2016, ai sensi di quanto disposto dall’art. 3, comma 1 del medesimo D.Lgs. n. 10/2016. Vedi, anche, il comma 3-bis dell’art. 5, D.Lgs. 7 marzo 2005, n. 82, aggiunto dal comma 1 dell’art. 15, D.L. 18 ottobre 2012, n. 179, come modificato dalla legge di conversione 17 dicembre 2012, n. 221.

(216) Sull’applicabilità delle disposizioni di cui al primo periodo del presente comma vedi l’art. 10, comma 3, D.Lgs. 25 novembre 2016, n. 218.

A.N.A.C. : Comunicato del Presidente del 30

ottobre 2018

20 Maggio 2019

Com.pres.30.10.2018 acquisti di importo inferiore a 1.000 euro

---

Contratto Collettivo Nazionale di Lavoro del comparto Funzioni Locali 2016-2018

20 Maggio 2019

Contratto Collettivo Nazionale di Lavoro del comparto
FUNZIONI LOCALI
Periodo 2016-2018

Leggi: CCNL Funzioni Locali 21 maggio 2018

Decreto Ministero dell'Interno del 18.12.2017

20 Maggio 2019

Decreto del Ministero dell'Interno sulla disciplina delle procedure per la notificazione dei verbali di accertamento delle violazioni del Codice della Strada, tramite posta elettronica certificata

Leggi: DECRETO 18 dicembre 2017 Notifiche tramite PEC

Regolamento recante modalità per lo svolgimento delle visite fiscali

20 Maggio 2019

Approvato il nuovo Regolamento recante modalità per lo svolgimento delle visite fiscali e per l'accertamento delle assenze dal servizio per malattia, nonché l'individuazione delle fasce orarie di reperibilità, ai sensi dell'articolo 55-septies, comma 5-bis, del decreto

legislativo 30 marzo 2001, n. 165.

Entrata in vigore del provvedimento: 13/01/2018

Testo del Regolamento DECRETO ottobre 2017, Regolamento visite fiscali

---

D.Lgs. 7-3-2005 n. 82 – Codice dell'amministrazione digitale (2016)

20 Maggio 2019

D.Lgs. 7-3-2005 n. 82 – Codice dell'amministrazione digitale

Aggiornamento entrato in vigore il 14.09.2016

D.Lgs. n. 82, 7 marzo 2005 Codice dell'Amministrazione Digitale 2016

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 10 novembre 2014, n. 194

20 Maggio 2019

Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente.
(GU n.5 del 8-1-2015)
Vigente al: 23-1-2015

Allegato A – Piano per il graduale subentro dell'ANPR alle Anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni e modalità di subentro

Allegato B – Campi relativi ai dati contenuti nell'ANPR

Allegato C

Allegato D

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto l'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, introdotto dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e, in particolare, il comma 6, lettere a) e b) del medesimo articolo 62;

Vista la legge 24 dicembre 1954, n. 1228, recante "Ordinamento delle anagrafi della popolazione residente";

Visto il decreto del Presidente della Repubblica 29 settembre 1973, n. 605, recante "Disposizioni relative all'anagrafe tributaria e al codice fiscale dei contribuenti", e successive modificazioni;

Vista la legge 27 ottobre 1988, n. 470, recante "Anagrafe e censimento degli italiani all'estero";

Visto il decreto del Presidente della Repubblica 30 maggio 1989, n. 223, recante "Approvazione del nuovo regolamento anagrafico della popolazione residente";

Visto il decreto legislativo 6 settembre 1989, n. 322, recante "Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'articolo 24 della legge 23 agosto 1988, n. 400";

Visto il decreto del Presidente della Repubblica 6 settembre 1989, n. 323, recante "Regolamento per l'esecuzione della legge 27 ottobre 1988, n. 470, sull'anagrafe e il censimento degli italiani all'estero";

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421", e successive modificazioni, e, in particolare, l'articolo 3;

Visto il decreto del Presidente della Repubblica 3 novembre 2000, n. 396, recante "Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile";

Visto il decreto legislativo del 30 marzo 2001, n. 165, recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";

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

Visto il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", e successive modificazioni;

Visto il Regolamento (CE) n. 862/2007 del Parlamento europeo e del Consiglio dell'11 luglio 2007 relativo alle statistiche comunitarie in materia di migrazione e di protezione internazionale;

Visto il Regolamento (CE) n. 763/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 relativo ai censimenti della popolazione e delle abitazioni;

Visto il Regolamento (CE) n. 1201/2009 della Commissione del 30 novembre 2009 recante attuazione del Regolamento (CE) n. 763/2008 del Parlamento europeo e del Consiglio, per quanto riguarda le specifiche tecniche delle variabili e delle loro classificazioni;

Visti il Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio e, in particolare, l'articolo 13 che disciplina il Programma Statistico europeo, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il Regolamento (CE) n. 322/1997 del Consiglio, relativo alle statistiche comunitarie, e la Decisione 89/382/CEE, Euratom del Consiglio che istituisce un comitato del programma statistico delle Comunità europee;

Visto il Regolamento (UE) n. 1260/2013 del Parlamento europeo e del Consiglio del 20 novembre 2013 relativo alle statistiche demografiche europee;

Visto il decreto del Presidente della Repubblica 7 settembre 2010, n. 166, recante "Approvazione del Regolamento recante il riordino dell'Istituto nazionale di statistica" e, in particolare, l'articolo 2, comma 2, lettera c)";
Visto l'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilità 2013)", e successive modificazioni;
Visto il decreto del Presidente del Consiglio dei ministri 23 agosto 2013, n. 109, recante "Disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR)";
Visto il decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, recante "Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari";
Sentito l'Istituto Nazionale di Statistica, che si è espresso con pareri del 26 febbraio 2014 e del 12 giugno 2014;
Acquisito il parere del Garante per la protezione dei dati personali, che si è espresso con nota in data 17 aprile 2014;
Acquisita l'intesa con l'Agenzia per l'Italia digitale;
Acquisita l'intesa con la Conferenza unificata nella seduta del 5 agosto 2014;
Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, e successive modificazioni;
Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 25 settembre 2014;
Su proposta del Ministero dell'interno, del Ministro per la semplificazione e la pubblica amministrazione, di concerto con il Ministro dell'economia e delle finanze;
Adotta il seguente regolamento:

Art. 1

Subentro alle anagrafi tenute dai comuni

1. L'Anagrafe Nazionale della Popolazione Residente (ANPR) subentra gradualmente alle anagrafi tenute dai comuni secondo il piano di subentro e le modalità, idonee a garantire l'integrità, l'univocità e la sicurezza dei dati, descritti nell'Allegato A, che costituisce parte integrante del presente regolamento. Nel subentro sono compresi i dati informatizzati relativi alle situazioni anagrafiche pregresse alla data del subentro e alle schede archiviate in formato elettronico.
2. I dati anagrafici inviati dai comuni ai fini del subentro sono sottoposti ai seguenti controlli formali da parte del Ministero dell'interno:
a) validazione del codice fiscale previo confronto con l'anagrafe tributaria, di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605;
b) verifica di congruità con i dati contenuti nell'ANPR al momento del subentro.
3. Il Ministero dell'Interno e l'Istituto nazionale di statistica, sentito il Garante per la protezione dei dati personali, definiscono standard e indicatori finalizzati a monitorare la qualità dei dati registrati nell'ANPR nella fase di subentro.
4. L'ANPR rende disponibile ai comuni, a seguito del subentro, i dati necessari all'allineamento delle banche dati eventualmente conservate dagli stessi.

Art. 2

Dati contenuti nell'ANPR e modalità di conservazione

1. Nell'ANPR sono contenuti i dati del cittadino, della famiglia anagrafica e della convivenza di cui agli articoli 20, 21 e 22 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, e successive modificazioni, i dati dei cittadini italiani residenti all'estero, registrati dai Comuni ai sensi del decreto del Presidente della Repubblica 6 settembre 1989, n. 323, nonché il domicilio digitale, di cui all'articolo 3-bis, del decreto legislativo 7 marzo 2005, n. 82.
2. I campi relativi ai dati di cui al comma 1 sono descritti nell'Allegato B, che costituisce parte

integrante del presente regolamento.
3. L'ANPR conserva le variazioni anagrafiche e i dati relativi alle situazioni anagrafiche pregresse.
4. L'ANPR conserva, in una distinta sezione, le schede anagrafiche relative alle persone cancellate.

Art. 3

Garanzie e misure di sicurezza nel trattamento dei dati personali

1. I dati contenuti nell'ANPR sono trattati secondo le modalità e le misure di sicurezza per la protezione dei dati descritte nell'Allegato C, che costituisce parte integrante del presente regolamento, adottate nel quadro delle più ampie misure di cui agli articoli da 31 a 36 e all'allegato B del decreto legislativo 30 giugno 2003, n. 196.
2. Titolare del trattamento dei dati contenuti nell'ANPR, ai sensi dell'articolo 4, comma 1, lettera a), del citato decreto legislativo n. 196 del 2003, è il Ministero dell'interno, il quale provvede alla conservazione, alla comunicazione dei dati, nonché all'adozione delle misure di sicurezza di cui al comma 1.
3. Il sindaco, nell'esercizio delle attribuzioni di cui all'articolo 54 del decreto legislativo 18 agosto 2000, n. 267, e successive modificazioni, è titolare del trattamento dei dati di propria competenza, limitatamente alla registrazione dei dati stessi.
4. La società di cui all'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, è designata responsabile del trattamento dei dati dal Ministero dell'Interno ai sensi dell'articolo 29 del decreto legislativo n. 196, del 2003.

Art. 4

Servizi resi disponibili dall'ANPR ai Comuni

1. L'ANPR rende disponibili ai Comuni per i quali è completato il subentro di cui all'articolo 1, i servizi descritti nell'Allegato D, che costituisce parte integrante del presente regolamento, secondo le modalità indicate nell'Allegato C.

Art. 5

Servizi resi disponibili dall'ANPR alle pubbliche amministrazioni

1. Le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, e gli organismi che erogano pubblici servizi, fruiscono dei servizi di cui all'Allegato D, per l'espletamento dei propri compiti istituzionali, secondo le modalità indicate nell'Allegato C.
2. L'ANPR rende disponibili all'Istituto nazionale di statistica, mediante i servizi previsti nell'Allegato D, i dati di cui all'articolo 2, concernenti la popolazione, il movimento naturale e i trasferimenti di residenza, necessari alla produzione delle statistiche ufficiali sulla popolazione e sulla dinamica demografica, nel rispetto della normativa nazionale e della legislazione dell'Unione Europea.
3. Il Ministero dell'interno – Direzione Centrale per i Servizi Demografici verifica i presupposti e le condizioni di legittimità dell'accesso ai servizi di cui al presente articolo.
4. Il comune, anche mediante le convenzioni previste dall'articolo 62, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, consente la fruizione dei dati anagrafici della popolazione residente nel proprio territorio, con riguardo altresì agli elenchi di cui all'articolo 34 del decreto del Presidente della Repubblica n. 223 del 1989. La verifica dei presupposti e delle condizioni di legittimità dell'accesso ai dati è svolta dal sindaco.

Art. 6

Accesso all'ANPR da parte del cittadino

1. Il cittadino registrato nell'ANPR può esercitare il diritto di accesso ai propri dati personali e gli altri diritti di cui all'articolo 7 del decreto legislativo n. 196 del 2003 presso gli uffici anagrafici, anche consolari, ovvero tramite sito web dell'ANPR, in modalità diretta e sicura, e previa identificazione informatica ai sensi dell'articolo 64 del citato decreto legislativo n. 82 del 2005 e trasmissione dei dati in modalità protetta.

Art. 7

Clausola di invarianza finanziaria

1. Ai fini dell'attuazione delle disposizioni del presente regolamento si provvede con le risorse

umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.
Il presente decreto sarà trasmesso alla Corte dei conti per la registrazione.
Il presente decreto, munito di sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.
Roma, 10 novembre 2014

Il Presidente del Consiglio dei ministri
Renzi
Il Ministro dell'interno
Alfano
Il Ministro per la semplificazione e la pubblica amministrazione
Madia
Il Ministro dell'economia e delle finanze
Padoan
Visto, il Guardasigilli: Orlando
Registrato alla Corte dei conti il 18 dicembre 2014
Ufficio controllo atti P.C.M. Ministeri giustizia e affari esteri, Reg.ne – Prev. n. 3258

Allegato A

Piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni e modalità di subentro

A) Piano per il graduale subentro.

Il Piano per il graduale subentro (nel seguito "Piano") riguarda la progressiva migrazione delle basi dati comunali (APR ed AIRE) verso la base dati centrale ANPR.
Al fine di garantire la predisposizione della base di dati da utilizzare per la migrazione dei Comuni, l'ANPR è preliminarmente popolata con i dati presenti nelle partizioni della stessa, corrispondenti ai sistemi informativi INA e AIRE, attualmente ubicate presso il Centro Nazionale dei Servizi (CNSD) e i Servizi Informativi e Elettorali (SIE) del Ministero dell'Interno.
Tale popolamento iniziale anticipa la fase di validazione dei dati che contribuiscono alla determinazione del codice fiscale (cognome e nome; sesso; luogo e data di nascita), previo confronto con l'anagrafe tributaria di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605 e la verifica di congruità a livello nazionale.
Il Comune riceverà la segnalazione di eventuali anomalie rilevate che dovrà rimuovere utilizzando le proprie applicazioni e provvedendo ad un nuovo invio dei dati con le modalità attualmente previste nell'ambito dei sistemi INA ed AIRE.
Il Piano individua su base mensile, a decorrere dal completamento di tale popolamento iniziale, i comuni che avviano la migrazione delle proprie banche dati APR ed AIRE locali verso l'ANPR, previo assolvimento dell'obbligo di revisione di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223.
I comuni sono individuati sulla base di criteri di distribuzione geografica e di dimensione demografica, descritti nel seguito, assicurando un popolamento medio mensile di 8.000.000 di soggetti residenti, per dieci periodi della durata di 30 giorni ciascuno.
La pianificazione è cadenzata per settimane, secondo il piano seguente.
Settimana dalla 1 alla 20: comuni con popolazione fino a 100.000 abitanti, individuati, per ciascuna settimana, secondo i criteri di distribuzione geografica e dimensione demografica, espressi dai seguenti valori percentuali:

Distribuzione geografica	Dimensione demografica
Nord: 56 %	fino a 5.000 abitanti: 70 %

Centro:12 % |tra 5.001 e 20.000 abitanti: 24%
Sud e isole: 32 % |tra 20.001 e 100.000 abitanti: 6%
Settimana dalla 21 alla 24: comuni con popolazione compresa tra 100.001 e 200.000 abitanti, individuati, per ciascuna settimana, secondo il criterio di distribuzione geografica e degli ulteriori criteri riferiti al grado di informatizzazione e all'uniformità dei sistemi informativi.
Settimana dalla 25 alla 32: comuni di città metropolitane, individuati, per ciascuna settimana, secondo criteri riferiti al grado di informatizzazione e all'uniformità dei sistemi informativi.
La durata delle procedure di subentro per ogni comune è stimata in due settimane, di cui la prima è dedicata agli invii e la seconda al completamento delle elaborazioni.
Il comune trasmette i dati relativi alle posizioni informatizzate anagrafiche pregresse e alle schede archiviate alla data di inizio del subentro, dopo il completamento dell'invio dei dati relativi alla popolazione residente.
B) Modalità di subentro.
Il Piano di subentro è pubblicato sul sito del Ministero dell'interno, Direzione Centrale per i Servizi Demografici, entro trenta giorni dalla pubblicazione del presente decreto nella Gazzetta Ufficiale della Repubblica Italiana.
Sono pubblicati:
• l'elenco dei Comuni che dovranno migrare le proprie banche dati (APR), con indicazione della data in cui, per ciascun Comune, è previsto l'avvio delle operazioni di subentro. L'elenco è reso disponibile con congruo anticipo rispetto all'avvio delle suddette operazioni e può essere oggetto di aggiornamento con cadenza mensile;
• le specifiche tecniche e le relative modalità per l'utilizzo dei servizi di cui all'allegato D, compresi quelli che i Comuni devono utilizzare per inviare i dati contenuti nelle proprie APR, nonché le relative modalità di invio. Tali informazioni sono rese disponibili almeno centoventi giorni prima dell'avvio operativo del Piano di subentro.
I dati inviati dai comuni al fine del subentro sono sottoposti ai seguenti controlli formali:
a) verifica di conformità del messaggio allo standard definito dal Ministero dell'Interno e pubblicato nel sito WEB di ANPR;
b) validazione del codice fiscale previo confronto con l'anagrafe tributaria, di cui al decreto del Presidente della Repubblica 29 settembre 1973, n. 605;
c) verifica di congruità con i dati contenuti nell'ANPR al momento del subentro.
Il sistema segnala al comune le anomalie relative al codice fiscale e le altre eventuali anomalie ed incongruenze mediante un apposito messaggio.
Il sistema invia al comune, via posta elettronica certificata, un apposito messaggio di conferma del subentro con indicazione di data e ora.
Il comune risolve le anomalie e le incongruenze segnalate entro trenta giorni, utilizzando i servizi di registrazione dati di cui all'allegato D.

ALLEGATO B

CAMPI RELATIVI AI DATI CONTENUTI NELL'ANPR

A) SCHEDA INDIVIDUALE DELLA POPOLAZIONE RESIDENTE IN ITALIA
– Codice comunale identificativo di individuo – Denominazione indirizzo
– Numero civico (N)
– Codice fiscale – Scala o corte
– Comune – Interno
– Cognome – Numero isolato
– Nome – Domicilio digitale
– Paternità – Indirizzo estero
– Maternità – Motivo Cancellazione /Reiscrizione
– Luogo Nascita
– Atto Nascita – Descrizione Motivo Cancellazione /Reiscrizione
– Data Nascita

– Sesso – Data Cancellazione/ Reiscrizione
– Stato Civile
– Cognome Coniuge – Motivo Mutazione
– Nome Coniuge – Descrizione Motivo Mutazione
– Data matrimonio
– Luogo matrimonio – Data Mutazione
– Atto matrimonio – Numero pratica
– Ordine del matrimonio – Data perfezionamento pratica
– Data morte coniuge – Data morte
– Luogo morte coniuge – Luogo morte
– Atto morte coniuge – Atto di morte
– Ordine del matrimonio precedente la vedovanza – Anno censimento
– Sezione censimento
– Data sentenza divorzio – Numero foglio censimento
– Numero sentenza divorzio – Numero Carta d'Identità
– Ordine del matrimonio precedente il divorzio – Data Rilascio Carta d'Identità
– Estremi del permesso di soggiorno
– Cittadinanza
– Data prima iscrizione – Lista elettorale
– Motivo iscrizione – Lista di leva
– Numero pratica – Titolo di studio
– Data perfezionamento pratica – Posizione nella professione/condizione non professionale
– Data decorrenza indirizzo
– Specie indirizzo
– Codice identificativo di toponimo

B) SCHEDA DI FAMIGLIA DEI RESIDENTI IN ITALIA

Comune
Provincia Per ogni familiare:
Data costituzione Progressivo d'ordine
Motivo costituzione Relazione di parentela
Data eliminazione Cognome
Motivo eliminazione Nome
Intestatario famiglia Sesso
Data intestatario famiglia Paternità
Cognome tutore intestatario Maternità
minorenne Luogo Nascita
Nome tutore intestatario minorenne Data Nascita
Data decorrenza indirizzo Atto Nascita
Specie indirizzo Stato Civile
Denominazione indirizzo Cittadinanza
Numero civico (N) Data matrimonio
Scala o corte Luogo matrimonio
Interno Cognome Coniuge
Numero isolato Nome Coniuge
Frazione Atto matrimonio
Anno censimento Data morte coniuge
Sezione censimento Luogo morte coniuge
Numero foglio censimento Atto morte coniuge
Numero di componenti minorenni presenti nella scheda di famiglia Data sentenza divorzio
Numero sentenza divorzio
Professione/condizione non professionale

Anno censimento
Sezione censimento
Numero foglio censimento
C) SCHEDA DI CONVIVENZA DEI RESIDENTI IN ITALIA
Comune Maternità
Provincia Luogo Nascita
Specie della convivenza Data Nascita
Denominazione della convivenza Atto Nascita
Responsabile della convivenza Stato Civile
Data responsabile convivenza Cittadinanza
Data decorrenza indirizzo Data matrimonio
Specie indirizzo Luogo matrimonio
Denominazione indirizzo Cognome Coniuge
Numero civico (N) Nome Coniuge
Scala o corte Atto matrimonio
Interno Data morte coniuge
Numero isolato Luogo morte coniuge
Frazione Atto morte coniuge
Anno censimento Data sentenza divorzio
Sezione censimento Numero sentenza divorzio
Numero foglio censimento Professione/condizione non professionale
Per ogni convivente:
Progressivo d'ordine convivenza Anno censimento
Cognome Sezione censimento
Nome Numero foglio censimento
Sesso
Paternità
D) SCHEDA DEI CITTADINI ITALIANI RESIDENTI ALL'ESTERO
codice famiglia data arrivo nel consolato
codice territorio estero di residenza anno espatrio
codice consolato di residenza comune estremi nascita
provincia/contea anno estremi nascita
c.a.p. serie estremi nascita
località parte estremi nascita
indirizzo numero estremi nascita
numero civico data stato civile
presso comune stato civile
cognome territorio estero stato civile
nome luogo stato civile
data nascita comune registrazione stato civile
codice iscrizione anno registrazione stato civile
comune nascita serie registrazione stato civile
luogo nascita parte registrazione stato civile
territorio estero nascita numero registrazione stato civile
stato civile titolo di studio
codice sesso attualmente disoccupato
codice relazione parentela posizione professionale
comune iscrizione settore di attività
data iscrizione codice fiscale
motivo iscrizione tipo elettore
iniziativa iscrizione data inizio istruttoria

iniziativa aggiornamento data fine istruttoria
individuazione comune di iscrizione flag stato istruttoria
comune di provenienza documenti espatrio
territorio estero di provenienza note
cognome coniuge

E) ULTERIORI CAMPI RELATIVI A DATI DI SERVIZIO
Nell'ANPR sono altresì contenuti gli ulteriori campi relativi ai dati di servizio necessari a garantire l'interoperabilità con le banche dati di rilevanza nazionale e regionale, nonché con le banche dati comunali, ai fini dell'esercizio delle funzioni di competenza.

ALLEGATO C

Misure di sicurezza

Il presente allegato descrive le caratteristiche della piattaforma e le misure adottate per garantire l'integrità e la riservatezza dei dati scambiati e conservati, la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate, in conformità agli articoli 64, comma 2 e 65, comma 1, lettera c), del decreto legislativo 7 marzo 2005, n. 82.

Per le predette finalità, l'ANPR è dotata di:

• un sistema di Identity & Access Management per l'identificazione dell'utente e della postazione, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni;
• un sistema di tracciamento e di conservazione dei dati di accesso alle componenti applicative e di sistema;
• sistemi di sicurezza per la protezione delle informazioni e dei servizi erogati dalla base dati;
• un sistema di log analysis per l'analisi periodica dei file di log, in grado di individuare, sulla base di regole predefinite e formalizzate eventi potenzialmente anomali e di segnalarli al Ministero dell'interno tramite funzionalità di alert;
• una Certification Authority;
• sistemi e servizi di backup per il salvataggio dei dati e delle applicazioni;
• sistemi e servizi di Disaster Recovery.

Il piano di continuità operativa di cui all'articolo 50-bis del decreto legislativo 7 marzo 2005, n. 82, espliciterà le procedure relative ai sistemi ed ai servizi di backup e di Disaster Recovery.

1. Infrastruttura fisica

L'infrastruttura di ANPR è installata nella sede della Società di cui all'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228 (nel seguito "la Società") ed è gestita dalla Società stessa.

I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi necessari a garantire la continuità operativa del sistema.

Qualsiasi altra operazione manuale è consentita solo a personale autorizzato dal Ministero dell'interno.

La suddetta infrastruttura, oltre alle componenti di sicurezza, comprende i sistemi e le basi dati di cui al punto 4.1 dell'allegato al decreto del Presidente del Consiglio di Ministri 23 agosto 2013, n. 109.

2. Accesso alla base dati

L'accesso nell'ANPR avviene in condizioni di pieno isolamento operativo e di esclusività, in conformità ai principi di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati, dei sistemi e delle infrastrutture, di cui all'articolo 51 del decreto legislativo n. 82 del 2005.

I sistemi di sicurezza garantiscono che l'infrastruttura di produzione sia logicamente distinta dalle altre infrastrutture della Società e che l'accesso alla stessa avvenga in modo sicuro, controllato, e costantemente tracciato, esclusivamente da parte di personale autorizzato dal Ministero dell'interno, e con il tracciamento degli accessi e di qualsiasi attività eseguita.

L'ANPR invia e riceve le comunicazioni in modalità sicura, su rete di comunicazione SPC ovvero, tramite Internet, mediante protocollo SSL per garantire la riservatezza dei dati su reti pubbliche.

Le modalità di accesso da parte dei comuni, delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi si applicano fino alla piena attuazione delle disposizioni di cui all'articolo 64 del decreto legislativo n. 82 del 2005.

2.1 Accesso dei comuni

L'accesso dei comuni all'ANPR avviene tramite sito web o mediante web service.

Accesso del comune tramite sito web dell'ANPR.

I requisiti di sicurezza prevedono il riconoscimento dell'operatore e della postazione, autorizzata dal comune, e dotata dei seguenti dispositivi:

• certificato identificativo, riferito alla postazione, memorizzato al suo interno, emesso dalla Certification Authority;

• smart-card dedicata e personale, e relativo lettore, con certificato client di autenticazione, intestato all'operatore, emesso dalla Certification Authority.

L'infrastruttura di Identity & Access Management garantisce l'autenticazione dell'utente e la verifica dei diritti di accesso dello stesso alle varie risorse, in base al relativo profilo autorizzativo.

L'operatore accede dalla postazione certificata autenticandosi tramite certificato client.

La postazione è identificata mediante la connessione del browser dell'utente a un indirizzo gestito da un apparato di sicurezza specializzato, che verifica la validità del certificato identificativo della postazione e, in caso di esito positivo, la validità del certificato client.

Il sistema di Identity & Access management autorizza l'utente in base al profilo assegnato ed effettua i controlli formali sui messaggi ricevuti.

Il sistema di tracciamento conserva le informazioni relative alla associazione utente – postazione – dati acceduti, inclusi i riferimenti temporali.

Tutte le informazioni relative al tracciamento dei dati sono accessibili solo dagli incaricati autorizzati su specifica richiesta da parte degli organi competenti.

Tutte le operazioni effettuate sono tracciate e conservate.

Accesso del comune mediante web service.

I requisiti di sicurezza prevedono:

• il certificato identificativo, riferito alla postazione, memorizzato al suo interno, emesso dalla Certification Authority;

• il riconoscimento dell'operatore tramite la userid e password utilizzata per accedere ai servizi dei sistemi informativi comunali, che garantiscono l'autenticazione dell'utente e la verifica dei diritti di accesso dello stesso alle varie funzionalità applicative;

• il certificato identificativo, riferito al server ospitante l'applicazione che utilizza il web service, memorizzato al suo interno, emesso dalla Certification Authority.

• L'operatore accede autenticandosi tramite la userid e la password utilizzata per accedere ai servizi dei sistemi informativi comunali.

• Per garantire il riconoscimento dell'operatore e della postazione, autorizzata dal comune, nonché l'integrità dei dati, i messaggi inviati prevedono:

• identificativo postazione firmato con il certificato di postazione;

• identificativo utente;

• firma dell'intero messaggio mediante il certificato che identifica il server comune secondo i meccanismi standard della ws security.

Alla ricezione del messaggio, ANPR verifica la firma del messaggio ed il sistema di Identity & Access management verifica la validità dell'identificativo della postazione, nonché l'esistenza dell'utente e la rispondenza dell'operazione richiesta in base al profilo assegnato; in caso di esito positivo, ANPR elabora il messaggio.

Il sistema di tracciamento conserva le informazioni relative all'associazione utente – postazione – dati acceduti, inclusi i riferimenti temporali.

Tutte le informazioni relative al tracciamento dei dati sono accessibili solo dagli incaricati autorizzati su specifica richiesta da parte degli organi competenti.

Tutte le operazioni effettuate sono tracciate e conservate.

Il comune garantisce l'adeguamento delle applicazioni alle regole di sicurezza descritte.
2.1.1 Registrazione degli utenti ed assegnazione degli strumenti di sicurezza
L'infrastruttura di Identity e Access Management censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione delle credenziali, secondo la seguente procedura:
a) il sindaco o suo delegato individua gli operatori comunali preposti all'accesso all'ANPR e ne comunica i nominativi al Ministero dell'interno, evidenziando gli operatori che saranno titolari di smart-card;
b) sulla base della comunicazione di cui al punto a), la società registra nel sistema di Identity e Access Management gli operatori comunali ed emette le smart-card richieste, e le trasmette alle Prefetture;
c) la società predispone i plichi che contengono i PIN/PUK e li trasmette ai comuni;
d) le Prefetture consegnano al sindaco le smart-card;
e) il sindaco individua l'Amministratore locale della sicurezza e, tramite la propria smart-card personale ed una specifica applicazione, registra le generalità della persona individuata, gli consegna la smart card e il plico con i PIN/PUK, associa alla persona il ruolo di Amministratore locale della sicurezza, in possesso delle autorizzazioni descritte di seguito;
f) il sindaco comunica al Ministero dell'interno il nominativo dell'Amministratore locale della sicurezza, assicurando l'avvenuta consegna dei dispositivi;
g) l'Amministratore locale della sicurezza accede con la propria smart-card ad un'apposita applicazione dedicata alla gestione degli operatori comunali, consegna le smart-card e le relative buste con i PIN/PUK a ciascuno dei soggetti indicati dal sindaco ai sensi della lettera a), assegna i profili per l'accesso alle applicazioni, revoca le autorizzazioni, blocca le smart-card, richiede nuove smart-card in caso di impossibilità di utilizzo di quella assegnata, registra nuovi operatori comunali, prenotando contestualmente la relativa smart-card che sarà successivamente recapitata dalla società, con modalità analoghe a quelle descritte al punto d);
h) il sindaco accede alla stessa applicazione, può effettuare tutte le operazioni previste per l'Amministratore locale della sicurezza nonché la revoca delle autorizzazioni.
Tutte le funzionalità di sicurezza descritte ai punti precedenti sono disponibili all'interno di un'apposita Web application, cui si accede con autenticazione forte e canale sicuro: la smart-card, pertanto, deve essere necessariamente richiesta per l'Amministratore locale della sicurezza, oltre che per gli operatori comunali che avranno accesso al sito Web di ANPR.
Tramite la suddetta applicazione sono distribuiti i certificati che saranno utilizzati per il riconoscimento delle postazioni.
La gestione e la conservazione della smart-card è di esclusiva responsabilità dell'operatore cui è assegnata, mentre la gestione e la conservazione del certificato che identifica la postazione, memorizzato internamente ad essa, è di responsabilità di un dipendente del Comune appositamente individuato quale responsabile del certificato stesso. La non esportabilità di questo certificato dalla postazione è garantita dalla presenza di un codice PIN, generato in fase di installazione sulla specifica postazione destinataria, la cui conservazione è di esclusiva responsabilità del suddetto dipendente.
Per la gestione dei processi autorizzativi, sono previsti i seguenti ruoli amministrativi, suddivisi tra gli attori del sistema:
a) Amministratore di Infrastruttura;
b) Amministratore Applicativo;
c) Amministratore Centrale della Sicurezza;
d) Amministratori locali;
e) Amministratore di primo livello (Sindaco o suo delegato);
f) Amministratore di secondo livello (Amministratore locale della sicurezza);
g) Amministratore della postazione (responsabile dei certificati di postazione).
I primi due ruoli sono attribuiti a personale della Società dalla stessa individuato e comunicato al

Ministero dell'interno.
Il terzo ruolo è attribuito al personale del Ministero dell'interno.
2.2 Accesso delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi
L'accesso delle pubbliche amministrazioni e degli organismi che erogano pubblici servizi all'ANPR avviene tramite sito web o mediante web service.
Per l'accesso tramite sito web, i requisiti di sicurezza prevedono il riconoscimento dell'operatore e della postazione, autorizzata dalla pubblica amministrazione o dall'ente, sulla base del Sistema di Identità Federata, (che contempla anche l'identificativo dell'operatore e l'indirizzo IP della postazione), che consente il controllo degli accessi ai soli servizi di consultazione ed estrazione.
Nel modello di sicurezza dell'Identità Federata, nell'ambito dell'Access & Facility Management, alle pubbliche amministrazioni e agli enti che erogano pubblici servizi sono demandate le funzioni di autenticazione e di autorizzazione, all'interno di profili prestabiliti, assumendo rispettivamente i ruoli di Identity Provider e Attribute Authority, in conformità al modello GFID dell'Agenzia per l'Italia Digitale e mediante l'adozione di soluzioni tecnologiche che garantiscano il tracciamento sia dell'Identity Provider sia dell'operatore.
Le operazioni effettuate presso la postazione sono registrate nel sistema di Identity e Access Management, che registra le informazioni di autenticazione e gli attributi e li utilizza per verificare i diritti di accesso all'informazione e per alimentare il sistema di tracciamento.
Per l'accesso tramite web service, si utilizzano i meccanismi propri del pattern di sicurezza che consente, ove richiesto, di trasferire, ai fini del tracciamento, oltre all'identificativo dell'ente anche l'identificativo dell'utente finale e l'indirizzo IP della sua postazione. Il server applicativo viene identificato tramite apposito certificato.
3. Sistema di monitoraggio dei servizi
Il Ministero dell'interno, attraverso l'infrastruttura di cui al paragrafo 1, eroga i servizi di cui all'allegato D e assolve le funzionalità di sicurezza descritte nel presente allegato, nel rispetto delle specifiche tecniche elaborate dalla Società e approvate dal Ministero.
Per il monitoraggio dei servizi, il Ministero dell'interno si avvale di uno specifico sistema, ubicato nel Centro Nazionale per i Servizi Demografici del Ministero dell'interno (CNSD), presso il quale sono installate apposite consolle di controllo, utilizzate esclusivamente da personale autorizzato dal Ministero dell'interno per l'accesso in sola visualizzazione.
La visualizzazione completa dello stato del servizio e dell'infrastruttura tecnologica che lo supporta avviene mediante:
a) vista c.d. "ad albero" dei servizi che rendono disponibili le seguenti informazioni:
• lista dei servizi erogati (nome, descrizione, codifica, etc.);
• infrastruttura tecnologica che ospita i servizi erogati con il dettaglio dei servizi tecnici che li compongono;
• allarmi associati alle risorse infrastrutturali dei servizi tecnici che hanno impatto sui servizi erogati;
• eventuali ticket di incidenti aperti dalla Società di cui all'articolo 1, comma 306, della legge 24 dicembre 2012, n. 228, per la gestione e la risoluzione degli allarmi.
b) vista di alto livello con rappresentazione, sia real time sia giornaliera, dell'andamento dello stato dei servizi erogati e dei relativi indicatori di disponibilità (eventi di infrastruttura, eventi da sonde end-to-end, ticket di incidenti);
c) rappresentazione dell'andamento della produzione dei servizi, in funzione dei livelli di autorizzazione definiti dal Ministero dell'interno, anche in termini di analisi delle interazioni del sistema con i soggetti che accedono (comuni, pubbliche amministrazioni, ed altri enti) e degli scostamenti dal trend, compresi report sintetici sullo stato di sicurezza del sistema.
4. Protezione da attacchi informatici
Al fine di protezione dei sistemi operativi da attacchi informatici, eliminando le vulnerabilità, si utilizzano:
a) in fase di configurazione, procedure di hardening finalizzate a limitare l'operatività alle sole

funzionalità necessarie per il corretto funzionamento dei servizi;
b) in fase di messa in esercizio, oltre che ad intervalli prefissati o in presenza di eventi significativi, processi di vulnerability assessment and mitigation nei software utilizzati e nelle applicazioni dei sistemi operativi;
c) piattaforma di sistemi firewall e sonde anti-intrusione.

Allegato D

Servizi dell'ANPR

Il presente allegato descrive i servizi che ANPR assicura ai soggetti che accedono.
Le richieste di servizio sono elaborate in file XML o altri formati aperti.
La risposta del sistema può avere formato XML, ASCII o PDF o altri formati aperti.
I servizi sono erogati in modalità web service ovvero attraverso una web application fruibile dal sito internet della ANPR.

A) Servizi ai Comuni

A.1) Registrazione dei dati.

I servizi di registrazione consentono le operazioni di modificazione dei dati di competenza del comune, in tempo reale.
In risposta alla richiesta dell'operatore, in assenza di errore dell'operazione, il sistema invia la conferma di modificazione del dato ad un protocollo riferito all'operazione; in caso di errore, il comune riceve un avviso di esito negativo, con indicazione della causa.
Al comune è, inoltre, resa disponibile la consultazione delle operazioni richieste, del relativo esito, e dei relativi messaggi di conferma e di errore, per intervalli temporali, con le seguenti modalità:
• l'esito di un'operazione di registrazione è disponibile per un anno;
• gli eventi notificati al comune sono disponibili per centottanta giorni.

A. 2) Consultazione ed estrazione.

I servizi di consultazione consentono di interrogare l'ANPR per i dati di competenza, secondo i seguenti parametri:
• per campi o combinazioni di campi;
• per tipo di operazione;
• per intervalli temporali.
In esito alla richiesta, il sistema comunica il numero progressivo e la data della risposta; in presenza di errori nella richiesta, il sistema comunica l'esito negativo, con indicazione della causa.
I servizi di estrazione consentono al Comune di estrarre i dati di ANPR di propria competenza con modalità analoghe a quelle descritte per i servizi di consultazione; in alternativa, il Comune può fornire ad ANPR una lista di soggetti per i quali ANPR restituirà in risposta i dati previsti per il tipo di estrazione prescelto dal Comune.
L'esito delle operazioni di consultazione ed estrazione è disponibile per trenta giorni.
L'esito delle richieste di consultazione non esaudite in tempo reale è disponibile per trenta giorni.

A. 3) Certificazione.

I servizi di emissione delle certificazioni anagrafiche di cui al capo VI del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, nonché all'articolo 7 della legge 27 ottobre 1988, n. 470, sono erogati ai Comuni secondo le modalità stabilite dal decreto legislativo 7 marzo 2005, n. 82.
Le richieste di certificazione sono esclusivamente di tipo puntuale e sono evase contestualmente.
In presenza di errore nella richiesta di emissione, il sistema comunica l'esito negativo, con indicazione della causa.

A. 4) 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.

L'ANPR rende disponibile 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, che pervengono ai comuni con le modalità tecniche di cui al decreto del Ministro dell'interno previsto dall'articolo 2, comma 3, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

Con il medesimo servizio di invio del certificato di morte di cui al citato articolo 74, è altresì inoltrata la denuncia della causa di morte di cui all'articolo 1 del decreto del Presidente della Repubblica 10 settembre 1990, n. 285.
A. 5) Servizi accessori.
I servizi accessori consentono di verificare lo stato delle operazioni richieste.
Comprendono, in particolare:
• il servizio di notifica dell'esito delle operazioni e degli eventi di competenza per l'allineamento delle banche dati tenute dal Comune per lo svolgimento delle proprie funzioni e dei servizi non supportati dall'ANPR;
• il servizio di verifica dell'esito di un'operazione;
• il servizio di ricezione delle risposte rese disponibili da ANPR;
• il servizio di annullamento dell'operazione;
• il servizio di variazione di dati;
• il servizio di consultazione delle notifiche;
• il servizio di monitoraggio.
I dati che consentono ad ANPR di fornire i servizi in questione sono conservati per un periodo di tempo prefissato, trascorso il quale sono storicizzati nel modo seguente:
• l'esito di un'operazione di registrazione è disponibile per un anno;
• l'esito delle operazioni di consultazione è disponibile per trenta giorni;
• gli eventi notificati al Comune sono disponibili per un periodo di centottanta giorni;
• le risposte alle richieste di consultazione ed estrazione non esaudite in tempo reale rimangono disponibili per trenta giorni.
Sarà inoltre reso disponibile un servizio di interscambio in tempo reale delle comunicazioni di stato civile tra Comuni.
B) Servizi alle pubbliche amministrazioni e agli enti che erogano pubblici servizi
B.1) Consultazione ed estrazione
I servizi di consultazione ed estrazione consentono di interrogare i dati dell'ANPR di competenza, secondo specifici parametri di ricerca.
La pubblica amministrazione, utilizzando la propria applicazione, invia la richiesta di consultazione o estrazione e riceve in risposta il risultato della richiesta; qualora il numero di soggetti che verificano le condizioni richieste sia particolarmente elevato o il tipo di ricerca prescelto richieda elaborazioni complesse, ANPR attribuisce alla richiesta un numero progressivo e rende disponibile la risposta in un momento successivo. La Pubblica Amministrazione riceve in risposta il numero progressivo assegnato alla richiesta e la data in cui saranno resi disponibili gli esiti dell'elaborazione.
In presenza di errori nella struttura dei dati della richiesta, ANPR restituisce un esito negativo, motivando il motivo dello scarto.
B.2) Comunicazione dati e variazioni anagrafiche
L'ANPR rende disponibile alle pubbliche amministrazioni i dati e le variazioni anagrafiche di competenza registrate dai Comuni.
B.3) Servizi accessori
I servizi accessori consentono di verificare lo stato delle operazioni richieste e comprendono:
• il servizio di notifica dell'esito delle operazioni e degli eventi di competenza;
• il servizio di ricezione delle risposte dell'ANPR;
• il servizio di consultazione delle notifiche;
• il servizio di monitoraggio.
I dati che consentono ad ANPR di fornire i servizi in questione sono conservati per un periodo di tempo prefissato, trascorso il quale vengono storicizzati:
• l'esito delle operazioni di consultazione ed estrazione è disponibile per trenta giorni;
• gli eventi notificati alla Pubblica Amministrazione sono disponibili per un periodo di centottanta giorni;
• le risposte alle richieste di consultazione ed estrazione non esaudite in tempo reale rimangono

disponibili per trenta giorni.

DECRETO PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 novembre 2014(1).

20 Maggio 2019

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, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

(1) Pubblicato nella Gazz. Uff. 12 gennaio 2015, n. 8.

IL PRESIDENTE

DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante «Codice dell'amministrazione digitale» e, in particolare, gli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e l'71, comma 1;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;

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

Visto il decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni, recante «Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137»;

Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese», con cui è stata istituita l'Agenzia per l'Italia digitale;

Visto il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta Ufficiale dell'Unione europea serie L 257 del 28 agosto 2014;

Visto il decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, recante «Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71», pubblicato nella Gazzetta Ufficiale 21 maggio 2013, n. 117;

Visto il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante «Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4,

43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005», pubblicato nel Supplemento ordinario n. 20 alla Gazzetta Ufficiale – serie generale – 12 marzo 2014, n. 59;

Visto il decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante «Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005», pubblicato nel Supplemento ordinario n. 20 alla Gazzetta Ufficiale – serie generale – 12 marzo 2014, n. 59;

Visto il decreto del Presidente della Repubblica 21 febbraio 2014 con cui l'onorevole dottoressa Maria Anna Madia è stata nominata Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei Ministri 22 febbraio 2014 con cui al Ministro senza portafoglio onorevole dott.ssa Maria Anna Madia è stato conferito l'incarico per la semplificazione e la pubblica amministrazione;

Visto il decreto del Presidente del Consiglio dei Ministri 23 aprile 2014 recante delega di funzioni al Ministro senza portafoglio onorevole dott.ssa Maria Anna Madia per la semplificazione e la pubblica amministrazione;

Acquisito il parere tecnico dell'Agenzia per l'Italia digitale;

Sentito il Garante per la protezione dei dati personali;

Sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 nella seduta del 24 agosto 2013;

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

Di concerto con il Ministro dei beni e delle attività culturali e del turismo per le parti relative alla formazione e conservazione dei documenti informatici delle pubbliche amministrazioni;

Decreta:

Capo I

Definizioni e ambito di applicazione

Art. 1. Definizioni

1. Ai fini del presente decreto si applicano le definizioni del glossario di cui all'allegato 1 che ne costituisce parte integrante.
2. Le specifiche tecniche relative alle regole tecniche di cui al presente decreto sono indicate nell'allegato n. 2 relativo ai formati, nell'allegato n. 3 relativo agli standard tecnici di riferimento per la formazione, la gestione e la conservazione dei documenti informatici, nell'allegato n. 4 relativo alle specifiche tecniche del pacchetto di archiviazione e nell'allegato n. 5 relativo ai metadati. Le specifiche tecniche di cui al presente comma sono aggiornate con delibera dell'Agenzia per l'Italia digitale, previo parere del Garante per la protezione dei dati personali, e pubblicate sul proprio sito istituzionale.

Art. 2. Oggetto e ambito di applicazione

1. Il presente decreto detta le regole tecniche per i documenti informatici previste dall'art. 20, commi 3 e 4, dall'art. 22, commi 2 e 3, dall'art. 23, e dall'art. 23-bis, commi 1 e 2, e del decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale», di seguito Codice.
2. Il presente decreto detta le regole tecniche previste dall'art. 23-ter, commi 3 e 5, dall'art. 40, comma 1 e dall'art. 41, comma 2-bis del Codice in materia di documenti amministrativi informatici e fascicolo informatico.
3. Ai sensi dell'art. 2, comma 5, del Codice, le presenti regole tecniche si applicano nel rispetto della disciplina rilevante in materia di tutela dei dati personali e, in particolare, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.
4. Le disposizioni del presente decreto si applicano ai soggetti di cui all'art. 2, commi 2 e 3, del Codice, nonché agli altri soggetti a cui è eventualmente affidata la gestione o la conservazione dei documenti informatici.

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 un documento analogico di cui all'art. 22, commi 2 e 3, del Codice è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.
2. Fermo restando quanto previsto dall'art. 22, comma 3, del Codice, la copia per immagine di uno o più documenti analogici può essere sottoscritta con firma digitale o firma elettronica qualificata da chi effettua la copia.
3. Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico di cui all'art. 22, comma 2, del Codice, può essere inserita nel documento informatico contenente la copia per immagine. Il documento informatico così formato è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

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.

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.

Art. 7. Trasferimento nel sistema di conservazione

1. Il trasferimento dei documenti informatici nel sistema di conservazione avviene generando un pacchetto di versamento nelle modalità e con il formato previsti dal manuale di conservazione di cui all'art. 8 del decreto del Presidente del Consiglio dei ministri 3 dicembre 2013, in materia di conservazione dei documenti informatici.
2. I tempi entro cui i documenti informatici devono essere versati in conservazione sono stabiliti per le diverse tipologie di documento e in conformità alle regole tecniche vigenti in materia.
3. Il buon esito dell'operazione di versamento è verificato tramite il rapporto di versamento prodotto dal sistema di conservazione.

Art. 8. Misure di sicurezza

1. I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico di cui all'art. 3.
2. I soggetti privati, per garantire la tenuta del documento informatico di cui all'art. 3, possono adottare, quale modello di riferimento, quanto previsto dagli articoli 50-bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. I sistemi di gestione informatica dei documenti rispettano le misure di sicurezza previste dagli articoli da 31 a 36 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del predetto codice.

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.

Art. 11. Trasferimento nel sistema di conservazione

1. Il responsabile della gestione documentale, ovvero, ove nominato, il coordinatore della gestione documentale:
a) provvede a generare, per uno o più documenti informatici, un pacchetto di versamento nelle modalità e con i formati concordati con il responsabile della conservazione e previsti dal manuale di conservazione;
b) stabilisce, per le diverse tipologie di documenti, in conformità con le norme vigenti in materia, con il sistema di classificazione e con il piano di conservazione, i tempi entro cui i documenti debbono essere versati in conservazione;
c) verifica il buon esito dell'operazione di versamento tramite il rapporto di versamento prodotto dal sistema di conservazione.

Art. 12. Misure di sicurezza

1. Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale predispone, in accordo con il responsabile della sicurezza e il responsabile del sistema di conservazione, il piano della sicurezza del sistema di gestione informatica dei documenti, nell'ambito del piano generale della sicurezza ed in coerenza con quanto previsto in materia dagli articoli 50-bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. Le suddette misure sono indicate nel manuale di gestione.
2. Si applica quanto previsto dall'art. 8, comma 2, secondo periodo.

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.

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.

Art. 15. Trasferimento in conservazione

1. Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale provvede a generare, per uno o più fascicoli o aggregazioni documentali informatiche o registri o repertori informatici di cui all'art. 14, un pacchetto di versamento che contiene i riferimenti che identificano univocamente i documenti informatici appartenenti al fascicolo o all'aggregazione documentale informatica.
2. Ai fascicoli informatici, alle aggregazioni documentali informatiche, ai registri o repertori informatici si applica quanto previsto per il documento informatico all'art. 11, comma 1, lettere b) e c).

Art. 16. Misure di sicurezza

1. Ai fascicoli informatici, alle aggregazioni documentali informatiche, ai registri o repertori informatici si applicano le misure di sicurezza di cui all'art. 12.

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. (2)
Il presente decreto è inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

(2) Per la sospensione dell'obbligo previsto dal presente comma vedi l' art. 61, comma 1, D.Lgs. 26 agosto 2016, n. 179.

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014

20 Maggio 2019

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014
Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (GU Serie Generale n.285 del 9-12-2014)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI
Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale;

Visto, in particolare, l'art. 64 del decreto legislativo n. 82 del 2005, come modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 69 che, «per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese» (SPID) e demanda a un decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, la definizione delle caratteristiche del sistema SPID, nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle modalità attraverso cui le imprese possono avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti;
Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;
Visti gli articoli da 19 a 22 del decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, e successive modificazioni, con cui è stata istituita l'Agenzia per l'Italia digitale;
Visto il Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia d'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta Ufficiale dell'Unione Europea – serie L. 257 del 28 agosto 2014;
Visto il decreto del Presidente della Repubblica 21 febbraio 2014 con cui l'onorevole dott.ssa Maria Anna Madia è stato nominata Ministro senza portafoglio;
Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2014 con cui al Ministro senza portafoglio onorevole dottoressa Maria Anna Madia è stato conferito l'incarico per la semplificazione e la pubblica amministrazione;
Visto il decreto del Presidente del Consiglio dei ministri 23 aprile 2014 recante Delega di funzioni al Ministro senza portafoglio onorevole dott.ssa Maria Anna Madia per la semplificazione e la pubblica amministrazione;
Sentito il Garante per la protezione dei dati personali;
Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, recepita con legge 21 giugno 1986, n. 317, modificata dal decreto legislativo 23 novembre 2000, n. 427;
Di concerto con il Ministro dell'economia e delle finanze;
Decreta:
Art. 1
Definizioni
1. Ai fini del presente decreto si intende per:
a) Agenzia: l'Agenzia per l'Italia Digitale;
b) attributi: informazioni o qualità di un utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari;
c) attributi identificativi: nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;
d) attributi secondari: il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni;
e) attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati;
f) autenticazione informatica: verifica effettuata dal gestore dell'identità digitale, su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'utente allo stesso

gestore, al fine di convalidarne l'identificazione informatica;
g) codice identificativo: il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID;
h) credenziale di accesso: il particolare attributo di cui l'utente si avvale, unitamente al codice identificativo, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi che aderiscono allo SPID;
i) fornitore di servizi: il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita;
l) gestori dell'identità digitale: le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti;
m) gestori di attributi qualificati: i soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi;
n) identificazione informatica: l'identificazione di cui all'art. 1, comma 1, lettera u-ter) del decreto legislativo 7 marzo 2005, n. 82 (di seguito «CAD»);
o) identità digitale: la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi;
p) revoca dell'identità digitale: disattivazione definitiva dell'identità digitale;
q) sospensione dell'identità digitale: disattivazione temporanea dell'identità digitale;
r) registrazione: l'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal presente decreto e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura;
s) registro SPID: registro, tenuto dall'Agenzia, accessibile al pubblico, contenente l'elenco dei soggetti abilitati a operare in qualità di gestori dell'identità digitale, di gestori degli attributi qualificati e di fornitori di servizi;
t) servizio qualificato: servizio per la cui erogazione è necessaria l'identificazione informatica dell'utente;
u) SPID: il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98;
v) utente: persona fisica o giuridica, titolare di un'identità digitale SPID, che utilizza i servizi erogati in rete da un fornitore di servizi, previa identificazione informatica.

Art. 2

Oggetto e finalità

1. Il presente decreto stabilisce le caratteristiche dello SPID ai sensi dell'art. 64 del CAD, come modificato dall'art. 17-ter del decreto-legge n. 69 del 2013.
2. Ai sensi di tali disposizioni lo SPID consente agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

Art. 3

Soggetti partecipanti allo SPID

1. I soggetti pubblici o privati che partecipano allo SPID sono:
a) i gestori dell'identità digitale;
b) i gestori degli attributi qualificati;
c) i fornitori di servizi;
d) l'Agenzia;
e) gli utenti.
2. I soggetti di cui al comma 1, esclusi gli utenti, costituiscono un sistema aperto e cooperante che consente loro di comunicare utilizzando meccanismi di interazione, standard tecnologici e protocolli indicati nel presente decreto e precisati nelle regole tecniche definite dall'Agenzia nell'ambito dei regolamenti di cui all'art. 4.

Art. 4

Ruolo dell'Agenzia

1. L'Agenzia cura l'attivazione dello SPID, svolgendo, in particolare, le seguenti attività:
a) gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni. Con i regolamenti di cui al presente articolo sono disciplinate le convenzioni per l'adesione allo SPID da parte dei fornitori di servizi ed è regolato il contributo che i gestori dell'identità digitale accreditati allo SPID riconoscono all'Agenzia, da determinarsi nella misura necessaria alla copertura dei costi sostenuti da quest'ultima;
b) cura l'aggiornamento del registro SPID e vigila sull'operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate;
c) stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità. A tali convenzioni i gestori dell'identità digitale e i gestori degli attributi qualificati sono tenuti ad aderire secondo le modalità indicate nei regolamenti di cui al presente articolo.
2. Entro trenta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le regole tecniche e le modalità attuative per la realizzazione dello SPID.
3. Entro sessanta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le modalità di accreditamento dei soggetti SPID.
4. Entro sessanta giorni dalla pubblicazione del presente decreto, l'Agenzia, sentito il Garante per la protezione dei dati personali, definisce con proprio regolamento le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale.

Art. 5

Attributi dell'identità digitale

1. Le identità digitali rilasciate all'utente contengono obbligatoriamente il codice identificativo, gli attributi identificativi e almeno un attributo secondario, funzionale alle comunicazioni tra il gestore dell'identità digitale e l'utente.
2. Al momento della richiesta di rilascio dell'identità digitale, l'utente può chiedere che siano registrati ulteriori attributi secondari.
3. L'Agenzia stabilisce, nell'ambito dei regolamenti di cui all'art. 4, le modalità e le regole tecniche con le quali i gestori dell'identità digitale e i gestori degli attributi qualificati curano e rendono disponibile la verifica degli attributi stessi ai fornitori di servizi. Gli attributi qualificati sono verificati dal fornitore di servizi presso il gestore di attributi qualificati.

Art. 6

Livelli di sicurezza delle identità digitali

1. Lo SPID è basato su tre livelli di sicurezza di autenticazione informatica:
a) nel primo livello, corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a un fattore,

quale la password, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'art. 4;
b) nel secondo livello, corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'art. 4;
c) nel terzo livello, corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo, secondo quanto previsto dal presente decreto e dai regolamenti di cui all'art. 4.
2. L'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello, nonché i criteri per la valutazione dei sistemi di autenticazione informatica e la loro assegnazione al relativo livello di sicurezza. In tale ambito, i gestori dell'identità digitale rendono pubbliche le decisioni dell'Agenzia con le modalità indicate dalla stessa.
3. I gestori dell'identità digitale garantiscono che l'autenticazione informatica avvenga attraverso software e soluzioni tecniche che non richiedono ai fornitori di servizi di dotarsi di dispositivi, fissi o mobili, proprietari. Sono consentite soluzioni tecniche che prevedono il caricamento del software necessario per effettuare l'autenticazione informatica.
4. I fornitori di servizi non possono discriminare l'accesso ai propri servizi sulla base del gestore di identità che l'ha fornita.
5. I fornitori di servizi scelgono il livello di sicurezza necessario per accedere ai propri servizi.

Art. 7

Rilascio delle identità digitali

1. Le identità digitali sono rilasciate, a domanda dell'interessato, dal gestore dell'identità digitale, previa verifica dell'identità del soggetto richiedente e mediante consegna in modalità sicura delle credenziali di accesso. Nell'ambito della propria struttura organizzativa, i gestori delle identità digitali individuano il responsabile delle attività di verifica dell'identità del soggetto richiedente.
2. La verifica dell'identità del soggetto richiedente e la richiesta di adesione avvengono in uno dei seguenti modi:
a) identificazione del soggetto richiedente che sottoscrive il modulo di adesione allo SPID, tramite esibizione a vista di un valido documento d'identità e, nel caso di persone giuridiche, della procura attestante i poteri di rappresentanza;
b) identificazione informatica tramite documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi;
c) identificazione informatica tramite altra identità digitale SPID di livello di sicurezza pari o superiore a quella oggetto della richiesta;
d) acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale;
e) identificazione informatica fornita da sistemi informatici preesistenti all'introduzione dello SPID che risultino aver adottato, a seguito di apposita istruttoria dell'Agenzia, regole di identificazione informatica caratterizzate da livelli di sicurezza uguali o superiori a quelli definiti nel presente decreto.
3. Con i regolamenti di cui all'art. 4, l'Agenzia definisce le modalità con le quali la verifica dell'identità di cui al comma 2 è effettuata secondo i più alti livelli di controllo disponibili, anche in relazione ai livelli di sicurezza di cui all'art. 6.
4. Nei casi di cui alle lettere b), c) ed e) del comma 2 i dati di adesione vengono forniti direttamente, utilizzando i moduli informatici posti a disposizione in rete dal gestore dell'identità digitale.
5. I gestori dell'identità digitale, al fine di poter documentare la corretta attribuzione della stessa, conservano per il periodo prescritto dal comma 8, in relazione alle modalità di identificazione di cui

al comma 2, copia per immagine del documento di identità esibito e del modulo di cui alla lettera a), copia del log della transazione di cui alle lettere b), c) ed e) o il modulo firmato digitalmente di cui alla lettera d), nonché i documenti e i dati utilizzati per l'associazione e la verifica degli attributi.
6. I gestori dell'identità digitale, ricevuta la richiesta di adesione, effettuano la verifica degli attributi identificativi del richiedente utilizzando prioritariamente i servizi convenzionali di cui all'art. 4, comma 1, lettera c).
7. Nei casi in cui le informazioni necessarie per la verifica degli attributi identificativi non siano accessibili tramite i servizi convenzionali di cui al comma 6, i gestori dell'identità digitale effettuano tali verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, secondo i criteri e le modalità stabilite dall'Agenzia con i regolamenti di cui all'art. 4, fatto salvo il caso di cui al comma 2, lettera e).
8. I gestori dell'identità digitale conservano la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.
Alla scadenza del predetto termine, i gestori cancellano la suddetta documentazione. Salvo il subentro ai sensi dell'art. 12, il gestore che cessa l'attività prima della scadenza del termine di cui al presente comma trasmette la medesima documentazione all'Agenzia, che la conserva fino alla scadenza del suddetto periodo.
9. I dati personali raccolti ai sensi del presente decreto sono trattati e conservati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
Art. 8
Gestione delle identità digitali
1. Fatto salvo il caso in cui l'aggiornamento degli attributi identificativi avvenga in modalità automatica tramite le convenzioni previste all'art. 4, comma 1, lettera c), gli utenti sono obbligati a informare tempestivamente il gestore dell'identità digitale di ogni variazione degli attributi previamente comunicati. Il gestore dell'identità digitale provvede tempestivamente ai necessari aggiornamenti, avendo verificato le informazioni fornite secondo le modalità di cui all'art. 7, comma 7.
2. Fatti salvi i casi previsti dall'art. 9, l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o revoca della propria identità digitale ovvero la modifica dei propri attributi secondari e delle proprie credenziali di accesso. A tali richieste il gestore dell'identità digitale provvede tempestivamente. L'Agenzia, con i regolamenti di cui all'art. 4, stabilisce le procedure per consentire agli utenti la rimozione dei dati contenuti nell'identità digitale.
3. Il gestore dell'identità digitale revoca l'identità digitale se riscontra l'inattività della stessa per un periodo superiore a ventiquattro mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica, utilizzando i servizi messi a disposizione dalle convenzioni di cui all'art. 4, comma 1, lettera c), ovvero, laddove l'informazione non sia disponibile in tali ambiti, attivando opportune e documentate verifiche delle informazioni ricevute.
4. Il gestore dell'identità digitale, su richiesta dell'utente, gli segnala ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari a tale scopo indicato dall'utente stesso, secondo le regole tecniche definite con i regolamenti di cui all'art. 4.
5. I gestori di identità SPID possono stipulare accordi con pubbliche amministrazioni al fine di importare nel sistema SPID identità digitali rilasciate dalle pubbliche amministrazioni conformemente a quanto previsto dall'art. 7.
Art. 9
Uso illecito delle identità digitali
1. Nel caso in cui l'utente ritenga, anche a seguito della segnalazione di cui all'art. 8, comma 4, che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, può chiedere, con le modalità indicate nei regolamenti di cui all'art. 4, la sospensione immediata dell'identità digitale al gestore della stessa e, se conosciuto, al fornitore di servizi presso il quale

essa risulta essere stata utilizzata. Salvo il caso in cui la richiesta sia inviata tramite posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identità digitale e il fornitore di servizi eventualmente contattato verificano, anche attraverso uno o più attributi secondari, la provenienza della richiesta di sospensione da parte del soggetto titolare dell'identità digitale e forniscono la conferma della ricezione della medesima richiesta.
2. Nel caso previsto dal comma 1, il gestore dell'identità digitale sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Scaduto tale periodo, l'identità digitale è ripristinata o revocata ai sensi del comma 3.
3. Il gestore revoca l'identità digitale se, nei termini previsti dal comma 2, riceve dall'interessato copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione.

Art. 10

Accreditamento dei gestori dell'identità digitale

1. Le modalità di richiesta di accreditamento sono definite nei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4, che possono contenere ulteriori criteri per l'accreditamento delle pubbliche amministrazioni.
2. A seguito dell'accoglimento della richiesta, l'Agenzia stipula apposita convenzione secondo lo schema definito nell'ambito dei regolamenti di cui all'art. 4 e dispone l'iscrizione del richiedente nel registro SPID, consultabile in via telematica.
3. Al fine di ottenere l'accreditamento gli interessati devono:
a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a cinque milioni di euro;
b) garantire il possesso, da parte dei rappresentanti legali, dei soggetti preposti all'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'art. 26 del decreto legislativo 1° settembre 1993, n. 385;
c) dimostrare la capacità organizzativa e tecnica necessaria per svolgere l'attività di gestione dell'identità digitale;
d) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi da fornire. In particolare, il personale addetto alla realizzazione e gestione del sistema informatico deve possedere, in relazione alle attività da svolgere, la competenza gestionale, l'appropriata conoscenza e padronanza delle procedure operative e di sicurezza, nonché delle regole tecniche da applicare. Il gestore provvede al periodico aggiornamento professionale del personale;
e) comunicare all'Agenzia i nominativi e il profilo professionale dei soggetti responsabili delle specifiche funzioni individuate nei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4;
f) essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative, alla norma ISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia;
g) trattare i dati personali nel rispetto del decreto legislativo 30 giugno 2003, n. 196;
h) essere in possesso della certificazione di qualità ISO 9001, successive modifiche o norme equivalenti.
4. Le lettere a) e b) del comma 3 non si applicano alle pubbliche amministrazioni che chiedono l'accreditamento al fine di svolgere l'attività di gestore dell'identità digitale.
5. L'Agenzia procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la permanenza della sussistenza dei requisiti previsti dal presente decreto. Se, all'esito dei controlli, accerta la mancanza dei requisiti richiesti per l'iscrizione nel registro SPID, decorso il termine fissato per consentire il ripristino degli stessi, l'Agenzia, con provvedimento motivato notificato all'interessato, può adottare le azioni previste dall'art. 12.

Art. 11

Obblighi dei gestori dell'identità digitale

1. I gestori dell'identità digitale, nel rispetto dei regolamenti di cui all'art. 4:
a) utilizzano sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;
b) adottano adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;
c) effettuano un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta;
d) effettuano, con cadenza almeno annuale, un'analisi dei rischi;
e) definiscono il piano per la sicurezza dei servizi SPID, da trasmettere all'Agenzia, e ne garantiscono l'aggiornamento;
f) allineano le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;
g) conducono, con cadenza almeno semestrale, il «Penetration Test»;
h) garantiscono la continuità operativa dei servizi afferenti allo SPID;
i) effettuano ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;
l) garantiscono la gestione sicura delle componenti riservate delle identità digitali degli utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata;
m) garantiscono la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dal presente decreto e dai regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4;
n) si sottopongono, con cadenza almeno biennale, ad una verifica di conformità alle disposizioni vigenti da parte di un organismo di valutazione accreditato ai sensi del Regolamento CE 765/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008. Inviano all'Agenzia l'esito della verifica, redatto dall'organismo di valutazione in lingua inglese, entro tre giorni lavorativi dalla sua ricezione;
o) informano tempestivamente l'Agenzia e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali, secondo le modalità individuate nei regolamenti adottati ai sensi dell'art. 4;
p) adeguano i propri sistemi a seguito degli aggiornamenti emanati dall'Agenzia;
q) inviano all'Agenzia, in forma aggregata, i dati da questa richiesti a fini statistici, che potranno essere resi pubblici.

Art. 12

Cessazione, subentro, sospensione e revoca dell'attività dei gestori dell'identità digitale

1. Il gestore dell'identità digitale comunica all'Agenzia e agli utenti a cui ha attribuito l'identità digitale l'intenzione di cessare la propria attività almeno trenta giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali dallo stesso rilasciate.
2. Il gestore sostitutivo, previo invio all'Agenzia della dichiarazione di accettazione e previa acquisizione del consenso degli utenti, subentra nella gestione delle identità digitali rilasciate dal gestore cessato e nella conservazione delle informazioni di cui all'art. 7, comma 8.
3. Salvo quanto disposto al comma 2, il gestore dell'identità digitale che cessa la propria attività, scaduto il termine del periodo previsto al comma 1, revoca le identità digitali rilasciate.
4. L'Agenzia, previo accertamento della violazione delle disposizioni di cui al presente decreto e dei regolamenti attuativi adottati ai sensi dell'art. 4, può disporre la sospensione dell'attività di attribuzione di identità digitali per un periodo minimo di un mese e massimo di un anno o, nei casi più gravi, la revoca dell'accreditamento del gestore dell'identità digitale.
5. In caso di revoca dell'accreditamento del gestore dell'identità digitale si applicano le disposizioni relative alle cessazioni di cui al presente articolo.

Art. 13

Adesione ed obblighi dei fornitori di servizi
1. I fornitori di servizi possono aderire allo SPID stipulando apposita convenzione con l'Agenzia il cui schema è definito nell'ambito dei regolamenti attuativi di cui all'art. 4.
2. I fornitori di servizi conservano per ventiquattro mesi le informazioni necessarie a imputare, alle singole identità digitali, le operazioni effettuate sui propri sistemi tramite SPID.
3. Nel caso in cui i fornitori di servizi rilevino un uso anomalo di un'identità digitale, informano immediatamente l'Agenzia e il gestore dell'identità digitale che l'ha rilasciata.
4. I fornitori di servizi trattano i dati personali nel rispetto del decreto legislativo 30 giugno 2003, n. 196. Nell'ambito dell'informativa di cui all'art. 13 del decreto legislativo n. 196 del 2003, i fornitori di servizi informano l'utente che l'identità digitale e gli eventuali attributi qualificati saranno verificati, rispettivamente, presso i gestori dell'identità digitale e i gestori degli attributi qualificati.
5. I fornitori di servizi, fatto salvo quanto previsto dall'art. 14 per le pubbliche amministrazioni, possono affidare la gestione delle interfacce di autenticazione informatica ai propri servizi in rete ai gestori di identità SPID.
Art. 14
Adesione allo SPID da parte delle pubbliche amministrazioni in qualità di fornitori di servizi
1. Nel rispetto dell'art. 64, comma 2, del CAD, le pubbliche amministrazioni che erogano in rete servizi qualificati, direttamente o tramite altro fornitore di servizi, consentono l'identificazione informatica degli utenti attraverso l'uso dello SPID.
2. Ai fini del comma 1, le pubbliche amministrazioni di cui all'art. 2, comma 2, del CAD aderiscono allo SPID, secondo le modalità stabilite dall'Agenzia ai sensi dell'art. 4, entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale.
3. Le pubbliche amministrazioni possono affidare ai gestori di identità dello SPID le funzioni di autenticazione informatica previste dalla normativa vigente in materia.
4. Le pubbliche amministrazioni possono affidare ai gestori di identità SPID le funzioni di autenticazione informatica basate sugli strumenti per i quali il diritto dell'Unione europea prevede il mutuo riconoscimento.
5. Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati. Per l'adeguamento allo SPID dei propri sistemi informatici, le amministrazioni utilizzano le risorse finanziarie disponibili a legislazione vigente, senza nuovi e maggiori oneri a carico della finanza pubblica.
Art. 15
Adesione allo SPID da parte di soggetti privati fornitori di servizi
1. Non possono aderire allo SPID i soggetti privati fornitori di servizi il cui rappresentante legale, soggetto preposto all'amministrazione o componente di organo preposto al controllo risulta condannato con sentenza passata in giudicato per reati commessi a mezzo di sistemi informatici.
2. Ai sensi dell'art. 64, comma 2-quinquies, del CAD, i soggetti privati che aderiscono allo SPID per la verifica dell'accesso ai servizi erogati in rete, nel rispetto del presente decreto e dei regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4, soddisfano gli obblighi di cui all'art. 17, comma 2, del decreto legislativo 9 aprile 2003, n. 70 con la comunicazione del codice identificativo dell'identità digitale utilizzata dall'utente.
3. Nella convenzione che i fornitori di servizi privati stipulano con l'Agenzia, nell'ambito dei regolamenti attuativi di cui all'art.
4, possono essere regolati i corrispettivi dovuti dai fornitori di servizi ai gestori dell'identità digitale e ai gestori degli attributi qualificati per i servizi di verifica.

Art. 16
Accreditamento dei gestori di attributi qualificati
1. I soggetti che hanno il potere, in base alle norme vigenti, di attestare gli attributi qualificati si accreditano indicando i dati che intendono rendere disponibili nello SPID, nel rispetto del presente

decreto e secondo le modalità indicate nei regolamenti attuativi adottati ai sensi dell'art. 4.
2. L'Agenzia inserisce in un apposito registro, accessibile a parte dei fornitori di servizi, le tipologie di dati resi disponibili da ciascun gestore di attributi qualificati.
3. Su richiesta degli interessati, sono accreditati di diritto i seguenti gestori di attributi qualificati:
a) il Ministero dello sviluppo economico in relazione ai dati contenuti nell'indice nazionale degli indirizzi PEC delle imprese e dei professionisti di cui all'art. 6-bis del CAD;
b) i consigli, gli ordini e i collegi delle professioni regolamentate relativamente all'attestazione dell'iscrizione agli albi professionali;
c) le camere di commercio, industria, artigianato e agricoltura per l'attestazione delle cariche e degli incarichi societari iscritti nel registro delle imprese;
d) l'Agenzia in relazione ai dati contenuti nell'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi di cui all'art. 57-bis del CAD.
Art. 17
Disposizione finale
1. I soggetti interessati a ottenere l'accreditamento allo SPID possono presentare domanda all'Agenzia successivamente all'emanazione dei regolamenti attuativi di cui all'art. 4.
Il presente decreto è inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.
Roma, 24 ottobre 2014
p. Il Presidente del Consiglio dei ministri
Il Ministro per la semplificazione e la pubblica amministrazione
Madia
Il Ministro dell'economia e delle finanze
Padoan

Registrato alla Corte dei conti il 24 novembre 2014
Ufficio controllo atti P.C.M. Ministeri giustizia e affari esteri
Reg.ne – Prev. n. 3020

DM 21/02/2011, n. 44 – Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-

legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24

20 Maggio 2019

DM 21/02/2011, n. 44

DECRETO MINISTERIALE 21 febbraio 2011, n. 44[(1)].

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*.[(2)]

[(1)]Pubblicato nella Gazz. Uff. 18 aprile 2011, n. 89.

[(2)]Emanato dal Ministero della giustizia.

IL MINISTRO DELLA GIUSTIZIA

di concerto con

IL MINISTRO PER LA PUBBLICA

AMMINISTRAZIONE E L'INNOVAZIONE

Visto l'*articolo 17, comma 3, della legge 23 agosto 1988, n. 400*;

Visto l'*articolo 4 del decreto-legge 29 dicembre 2009, n. 193*, recante «Interventi urgenti in materia di funzionalità del sistema giudiziario», convertito in legge, con modificazioni, dalla *legge 22 febbraio 2010 n. 24*;

Visto il *decreto legislativo 7 marzo 2005, n. 82*, recante "Codice dell'amministrazione digitale" e successive modificazioni;

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

Visti gli *articoli 16* e *16-bis del decreto-legge 29 novembre 2008, n. 185*, recante «Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale», convertito in legge, con modificazioni, dalla *legge 28 gennaio 2009, n. 2*»;

Visto il *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*, recante «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»;

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 legge 16 gennaio 2003, n. 3*»;

Visto il *decreto del Ministro della giustizia 17 luglio 2008*, recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile»;

Visto il *decreto ministeriale 27 aprile 2009*, recante «Nuove regole procedurali relative alla tenuta

dei registri informatizzati dell'amministrazione della giustizia»;

Visto il *decreto del Presidente del Consiglio dei Ministri 6 maggio 2009*, recante «Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini»;

Rilevata la necessità di adottare le regole tecniche previste dall'articolo 4, comma 1, del citato decreto, in sostituzione delle regole tecniche adottate con il *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123* e con il decreto del Ministro della giustizia 17 luglio 2008;

Acquisito il parere espresso in data 15 luglio 2010 dal Garante per la protezione dei dati personali;

Acquisito il parere espresso in data 20 luglio 2010 da DigitPA;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 25 novembre 2010 e quello espresso nell'adunanza del 20 dicembre 2010;

Vista la comunicazione al Presidente del Consiglio dei Ministri in data 18 gennaio 2011;

Adotta

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.

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*.

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.

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.

4. Il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dalla vigente normativa processuale.[(3)]

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.

[(3)] Comma così modificato dall'*art. 1, comma 1, lett. a), b) e c), D.M. 15 ottobre 2012, n. 209*.

Art. 14 *Documenti probatori e allegati non informatici*

1. I documenti probatori e gli allegati depositati in formato non elettronico sono identificati e descritti in una apposita sezione delle informazioni strutturate di cui all'*articolo 11*, secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34*.

2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare copia informatica dei documenti probatori e degli allegati su supporto cartaceo e ad inserirla nel fascicolo informatico, apponendo la firma digitale ai sensi e per gli effetti di cui all'*articolo 22*, comma 3 del codice dell'amministrazione digitale.

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.[4]

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.[5]

[4]Comma così sostituito dall' *art. 2, comma 1, lett. a), D.M. 15 ottobre 2012, n. 209*.

[5]Comma così modificato dall' *art. 2, comma 1, lett. b), D.M. 15 ottobre 2012, n. 209*.

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.[6]

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 3 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.[7]

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.[6]

8. Si applica, in ogni caso, il disposto dell'*articolo 49 del codice dell'amministrazione digitale*.

[6] Comma così modificato dall' *art. 3, comma 1, lett. a), D.M. 15 ottobre 2012, n. 209*.

[7] Comma così sostituito dall' *art. 3, comma 1, lett. b), D.M. 15 ottobre 2012, n. 209*.

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.[8]

[8] Comma così modificato dall' *art. 4, comma 1, D.M. 15 ottobre 2012, n. 209*.

Art. 18 *Notificazioni per via telematica eseguite dagli avvocati* [9]

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*.

[9] Articolo modificato dall'*art. 5, comma 1, lett. a) e b), D.M. 15 ottobre 2012, n. 209* e, successivamente, così sostituito dall'*art. 1, comma 1, D.M. 3 aprile 2013, n. 48*.

Art. 19 *Disposizioni particolari per la fase delle indagini preliminari*

1. Nelle indagini preliminari le comunicazioni tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria avvengono su canale sicuro protetto da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34*.

2. Le specifiche tecniche assicurano l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività, anche mediante l'utilizzo di misure di sicurezza ulteriori rispetto a quelle previste dal disciplinare tecnico di cui all'*allegato B del codice in materia di protezione dei dati personali*.

3. Per le comunicazioni di atti e documenti del procedimento di cui al comma 1 sono utilizzati i gestori di posta elettronica certificata delle forze di polizia. Gli indirizzi di posta elettronica certificata sono resi disponibili unicamente agli utenti abilitati sulla base delle specifiche stabilite ai sensi dell'*articolo 34*.

4. Alle comunicazioni previste dal presente articolo si applicano, in quanto compatibili, le disposizioni dell'*articolo 16*, commi 1, 2, 3, 4 e 5, e dell'*articolo 20*.

5. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto dalle forze di polizia nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'*articolo 34*; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34*. L'atto del processo, protetto da meccanismi di crittografia, è sottoscritto con firma digitale. Si applicano, in quanto compatibili, l'*articolo 14* del presente decreto, nonché gli *articoli 20* e *21 del codice dell'amministrazione digitale*.

6. La comunicazione degli atti del processo alle forze di polizia, successivamente al deposito previsto dall'*articolo 15*, è effettuata per estratto con contestuale messa a disposizione dell'atto integrale, protetto da meccanismo di crittografia, in apposita area riservata all'interno del dominio giustizia, accessibile solo dagli appartenenti alle forze di polizia legittimati, secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34* e nel rispetto dei requisiti di sicurezza di cui all'*articolo 26*.

7. Per la gestione del fascicolo informatico si applicano, in quanto compatibili, le disposizioni di cui all'*articolo 9*, commi da 1 a 5. Agli atti contenuti nel fascicolo informatico, custodito in una sezione distinta del sistema documentale di cui all'*articolo 9*, protetta da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34*, hanno accesso unicamente i soggetti abilitati interni appositamente abilitati. Alla conclusione delle indagini preliminari, e in ogni altro caso in cui il fascicolo o parte di esso deve essere consultato da soggetti abilitati esterni o da utenti privati, questi accedono alla copia resa disponibile mediante il punto di accesso e il portale dei servizi telematici, secondo quanto previsto al capo IV.

8. Per la trasmissione telematica dei flussi informativi sintetici delle notizie di reato e dei relativi esiti tra il Centro Elaborazione Dati del Servizio per il Sistema Informativo Interforze, di cui all'*articolo 8, della legge 1° aprile 1981, n. 121* e successive modifiche ed integrazioni, e il sistema dei registri delle notizie di reato delle Procure della Repubblica sono utilizzate le infrastrutture di connettività delle pubbliche amministrazioni che consentono una interconnessione tra le Amministrazioni, secondo le specifiche tecniche stabilite ai sensi dell'*articolo 34*. Il canale di comunicazione è protetto con le modalità di cui al comma 1.

9. Per assicurare la massima riservatezza della fase delle indagini preliminari la base di dati dei registri di cui al comma 8 è custodita, con le speciali misure di cui al comma 2, separatamente rispetto a quella relativa ai procedimenti per i quali è stato emesso uno degli atti di cui all'articolo 60, del codice di procedura penale, in infrastrutture informatiche di livello distrettuale o interdistrettuale individuate dal responsabile per i sistemi informativi automatizzati. I compiti di vigilanza sulle procedure di sicurezza adottate sulla base dati prevista dal presente comma sono svolti dal Procuratore della Repubblica presso il Tribunale e dal Procuratore generale della Repubblica presso la Corte di appello competenti in relazione all'ufficio giudiziario titolare dei dati, avvalendosi del personale tecnico individuato dal responsabile per i sistemi informativi automatizzati.

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 l'effettiva disponibilità dello spazio disco a disposizione.

6. La modifica dell'indirizzo elettronico può avvenire dal 1° al 31 gennaio e dal 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*[(10)(11)]

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.

(10) Articolo così sostituito dall'*art. 6, comma 1, D.M. 15 ottobre 2012, n. 209*.

(11) Vedi, anche, l'*art. 6, comma 2, D.M. 15 ottobre 2012, n. 209*.

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 l'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.

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.

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.[(12)]

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.

[(12)] Per le specifiche tecniche previste dal presente comma vedi il *Provvedimento 18 luglio 2011* e il *Provvedimento 16 aprile 2014*.

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.[(13)]

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.

[(13)] Comma così modificato dall'*art. 7, comma 1, D.M. 15 ottobre 2012, n. 209*.

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.

Agenzia per l'Italia Digitale: Circolare 66 del 4 settembre 2014

20 Maggio 2019

circolare_n._66_del_4_settembre_2014

D.L. 163-2013 Regolamento Processo Tributario Telematico

20 Maggio 2019

Pubblicato, il 14 febbraio 2014, nella Gazzetta Ufficiale il regolamento del Ministro dell'Economia e delle Finanze (decreto 23 dicembre 2013), che disciplina il processo tributario telematico.
Il regolamento disciplina l'uso degli strumenti informatici e telematici nell'ambito del processo

tributario, che contribuiranno, attraverso la dematerializzazione dei flussi documentali, al miglioramento del servizio di giustizia tributaria nel suo complesso, con una notevole riduzione dei costi diretti e indiretti per tutti gli operatori di settore (giudici, difensori, enti impositori, contribuenti, uffici di segreteria delle commissioni tributarie).

Leggi: DL 163-2013 Regolamento Processo Tributario Telematico

---

Decreto Presidente del Consiglio Dei Ministri 23 agosto 2013, n. 109 (1)

20 Maggio 2019

Regolamento recante disposizioni per la prima attuazione dell'articolo 62 del decreto legislativo 7 marzo 2005, n. 82, come modificato dall'articolo 2, comma 1, del decreto-legge 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221, che istituisce l'Anagrafe Nazionale della Popolazione Residente (ANPR).

(1)Pubblicato nella Gazz. Uff. 1 ottobre 2013, n. 230.

Entrata in vigore del provvedimento: 16/10/2013

Leggi: DPCONS 23-08-2013, n. 109 Costituzione ANPR