



Specifiche tecniche previste dall'articolo 34, comma 1, del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel 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 dalla legge 22 febbraio 2010, n. 24



MINISTERO DELLA GIUSTIZIA

Dipartimento per l'innovazione tecnologica

Direzione generale per i sistemi informativi automatizzati

IL DIRETTORE GENERALE

Visto il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, recante “Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24”, come modificato dal decreto del Ministro della giustizia 15 ottobre 2012, n. 209, dal decreto del Ministro della giustizia 3 aprile 2013, n. 48 e dal decreto del Ministro della giustizia 29 dicembre 2023, n. 217;

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

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Visto il Decreto legislativo 18 maggio 2018, n. 51, recante “Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”;

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

Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge n. 16 gennaio 2003, n. 3”;

Visto il decreto del Ministro della giustizia 27 aprile 2009 recante “Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia”;

Visto il decreto-legge 18 ottobre 2012, n. 179, recante “Ulteriori misure urgenti per la crescita del Paese”, convertito con modificazioni dalla legge 17 dicembre 2012, n. 22;

Visto il decreto legislativo 10 ottobre 2022, n. 149, recante “Attuazione della legge 26 novembre 2021, n. 206, recante delega al Governo per l'efficienza del processo civile e per la revisione della disciplina degli strumenti di risoluzione alternativa delle controversie e misure urgenti di razionalizzazione dei procedimenti in materia di diritti delle persone e delle famiglie nonché in materia di esecuzione forzata”;

Visto il decreto legislativo 10 ottobre 2022, n. 150, recante “Attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari”;

Visto l'articolo 36 del decreto-legge 24 febbraio 2023, n. 13, recante “Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e del Piano nazionale degli investimenti complementari al PNRR (PNC), nonché per l'attuazione delle politiche di coesione e della politica agricola comune”, convertito con modificazioni dalla legge 21 aprile 2023, n. 41;

Rilevata la necessità di adottare nuove specifiche tecniche previste dall'articolo 34, comma 1, del decreto del Ministro della giustizia 21 febbraio 2011, n. 44, come da ultimo novellato dal decreto del Ministro della giustizia 29 dicembre 2023, n. 217;

Acquisito il parere espresso in data 1° marzo 2024 dall'Agenzia per l'Italia Digitale;

Acquisito il parere espresso in data 6 giugno 2024 dal Garante per la protezione dei dati personali.

EMANA

IL SEGUENTE PROVVEDIMENTO

CAPO I

PRINCIPI GENERALI

Articolo 1

(Ambito di applicazione)

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

Articolo 2

(Definizioni)

1. Ai fini del presente provvedimento, oltre alle definizioni contenute nell'articolo 2 del Regolamento, si intende:

- a) Annotazioni Preliminari dal Portale: area di transito del Re.Ge.WEB nella quale sono effettuati i controlli preliminari sulle comunicazioni di cui all'articolo 18 dal personale di segreteria degli uffici del pubblico ministero;
- b) Area Riservata: sezione del sito alla quale si può accedere previa identificazione informatica, come disciplinata dall'articolo 6;
- c) Atto Abilitante: atto da cui risulti la conoscenza dell'esistenza in una procura della Repubblica di un procedimento relativo al proprio assistito e il relativo numero di registro;
- d) Autenticazione a due fattori: metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia che combina un'informazione nota (ad esempio un nome utente e una password) con un oggetto a disposizione (ad esempio, una carta di credito, token o telefono cellulare).
- e) PDF: Portable Document Format;
- f) PDP: Portale Deposito atti Penali di cui all'articolo 7-bis, comma 1, del Regolamento;
- g) PNR: Portale delle notizie di reato di cui all'articolo 7-bis, comma 2, del Regolamento;
- h) PST: Portale Servizi Telematici di cui all'articolo 6 del Regolamento;
- i) CAD: decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;
- j) CAeS (CMS Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 103 173 v.2.2.1 e basata a sua volta sulle specifiche RFC 5652 e RFC 2634 e successive modificazioni;
- k) Certificato: documento digitale generato da EJBCA, dietro specifica approvazione da parte di personale autorizzato;
- l) CNS: Carta Nazionale dei Servizi come definita nel CAD ossia il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;
- m) Codice IPA: identificativo univoco assegnato al termine di un processo di accreditamento, a ciascun soggetto tenuto all'iscrizione nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA), di cui all'articolo 6-ter del CAD;
- n) CSV: Comma-separated values;
- o) DTD: Document Type Definition;
- p) DGSIA: Direzione generale per i sistemi informativi automatizzati del Dipartimento per l'innovazione tecnologica;
- q) EJBCA: software di Certification Authority;
- r) Funzione di hash: una funzione matematica che genera, a partire da un documento informatico, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire il documento informatico originario e generare impronte uguali a partire da documenti informatici differenti;
- s) HSM: Hardware Security Module;
- t) HTTPS: HyperText Transfer Protocol over Secure Socket Layer di cui alle specifiche RFC 2818 e successive modifiche;
- u) IMAP: Internet Message Access Protocol;

- v) Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash.
- w) OID (Object Identifier): codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale;
- x) PAdES (PDF Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;
- y) pagoPA: il sistema dei pagamenti a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi, che si avvale della piattaforma tecnologica di cui all'articolo 5, comma 2, del CAD;
- z) PdA: Punto di accesso, come definito all'articolo 23 del Regolamento;
- aa) PEC: Posta Elettronica Certificata;
- bb) PKCS#11: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite apposita sequenza di chiamate al token per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di identificazione;
- cc) POP3: Post Office Protocol di cui alle specifiche RFC 1939;
- dd) RAFe (Registration Authority Front End): software in uso al personale autorizzato per la gestione dei certificati. Si connette a EJBCA per la generazione e la revoca dei certificati;
- ee) Regolamento: il decreto del Ministro della giustizia 21 febbraio 2011, n. 44, recante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24" e successive modificazioni;
- ff) Re.Ge.WEB: modulo del sistema SICP per la gestione dei registri di cancelleria;
- gg) ReGIndE: Registro Generale degli Indirizzi Elettronici, come definito all'articolo 7 del Regolamento;
- hh) SICP: Sistema Informativo della Cognizione Penale;
- ii) SMTP: Simple Mail Transfer Protocol di cui alle specifiche RFC 5321 e successive modifiche;
- jj) SPC: Sistema Pubblico di Connettività;
- kk) SPID: sistema pubblico di identità digitale;
- ll) Token crittografico: dispositivo (smart card, chiavetta USB o altro dispositivo sicuro) che contiene un certificato di autenticazione CNS
- mm) Ufficio Fonte: struttura organizzativa nella quale sono inseriti dipendenti con le qualifiche di Ufficiali o Agenti di Polizia Giudiziaria, ovvero altri soggetti tenuti per legge alla trasmissione della notizia di reato;
- nn) UNEP: Ufficio Notificazioni, Esecuzioni e Protesti;
- oo) WSDL: Web Services Definition Language;
- pp) XML; eXtensible Markup Language;
- qq) XSD: XML Schema Definition.

CAPO II

SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Articolo 3

(Infrastrutture informatiche)

1. Il sistema informatico del Ministero della giustizia è articolato, salvo le infrastrutture unitarie e comuni, a livello nazionale, interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale (di circondario).
2. Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.
3. Il sistema di posta elettronica certificata è gestito dal fornitore presso la propria sala server, oppure presso una sala server del Ministero della giustizia, secondo le linee guida su interoperabilità e sicurezza.
4. Il dispiegamento di detti sistemi rispetta le disposizioni di cui al decreto del Ministro della giustizia in data 27 aprile 2009, recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".
5. Il Direttore generale DGSIA emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico, sentito il Garante per la protezione dei dati personali. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul sito internet dell'Amministrazione.
6. Le strutture elaborative serventi ed i dati sono allocati in corrispondenza delle componenti di cui ai commi precedenti.

Articolo 4

(Gestore della posta elettronica certificata del Ministero della giustizia)

1. Il Ministero della giustizia si avvale del proprio gestore di posta elettronica certificata, che rilascia e gestisce apposite caselle di PEC degli uffici giudiziari e degli UNEP da utilizzare esclusivamente per i servizi previsti dal Regolamento, nel rispetto delle specifiche tecniche riportate nel presente provvedimento.
2. Le caselle appartengono ad apposito sottodominio (civile.ptel.giustiziacert.it e penale.ptel.giustiziacert.it) e possono ricevere unicamente messaggi di posta elettronica certificata. I messaggi di posta elettronica ordinaria vengono automaticamente scartati.
3. Il gestore dei servizi telematici utilizza i protocolli POP3S, IMAPS e SMTPS per collegarsi al gestore di posta elettronica certificata del Ministero.
4. La codifica dei singoli uffici, comprensiva del relativo indirizzo di PEC, è contenuta nel catalogo dei servizi telematici di cui all'articolo 5, comma 3.
5. Non possono essere utilizzate caselle di PEC diverse da quelle di cui ai commi precedenti per la trasmissione e il deposito di atti processuali.

procedimento, con indicazione delle date di udienza ed annotazione dell'evento, senza riferimenti in chiaro ai nomi o ai dati personali delle parti e tali per cui non sia possibile risalire all'identità dell'interessato. Il canale di comunicazione per l'accesso a tali informazioni è cifrato (HTTPS).

3. Il catalogo dei servizi telematici è consultabile nella sezione "Servizi" dell'Area Pubblica, nonché mediante appositi web services, documentati nella sezione "Documentazione" nella voce "Altro".

4. Nell'area riservata sono disponibili informazioni, dati e provvedimenti giudiziari in formato elettronico, secondo quanto previsto all'articolo 27 del Regolamento, nonché i servizi di pagamento telematico e di richiesta copie.

Articolo 6

(Identificazione informatica)

1. L'identificazione informatica per i soggetti abilitati esterni e gli utenti privati avviene sul PST mediante carta nazionale dei servizi o SPID con livello di sicurezza almeno pari a 2 e sul punto di accesso mediante autenticazione a due fattori oppure tramite token crittografico (smart card, chiavetta USB o altro dispositivo sicuro) o SPID con livello di sicurezza almeno pari a 2, in conformità all'articolo 64 del CAD; in caso si utilizzi il token crittografico, l'identificazione avviene nel rispetto dei seguenti requisiti:

a) Il certificato deve essere rilasciato da un certificatore accreditato dall'Agenzia per l'Italia Digitale ai sensi dell'art 29 del CAD, che si fa garante dell'identità del soggetto;

b) Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all'Appendice 1 del documento rilasciato dal CNIPA: "Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi". L'estensione Certificate Policy (2.5.29.32) può essere valorizzata con un Object Identifier (OID) definito dalla CA;

c) In termini di sicurezza, i dispositivi ammessi sono i dispositivi personali consentiti per la firma elettronica qualificata e quindi smart card e token USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criteria EAL4+ con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie;

d) In termini d'interoperabilità, sono ammissibili dispositivi che consentano la disponibilità di entrambe le interfacce PKCS#11 e CSP; in particolare, entrambe le interfacce devono consentire l'accesso alla procedura d'identificazione forte mediante digitazione del PIN da parte dell'utente; il dispositivo deve inoltre rispettare la strutturazione del file system come da specifiche CNS.

2. In fase di identificazione tramite token crittografico, il punto di accesso o il PST verifica la validità del certificato presente nel token crittografico utilizzato dall'utente che accede; prima di consentire qualunque operazione, inoltre, il punto di accesso verifica che il token crittografico sia collegato alla postazione; in caso contrario, invalida e termina la sessione.

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

4. La violazione delle regole di sicurezza di cui ai precedenti commi comporta per il punto di accesso la sospensione dell'autorizzazione a erogare i servizi, fino al definitivo adeguamento ai suddetti requisiti.

5. L'identificazione informatica per i soggetti abilitati interni avviene ai sensi dell'articolo 12.

Articolo 7

(Registro generale degli indirizzi elettronici)

1. Il ReGIndE è gestito dal Ministero della giustizia e contiene i dati identificativi nonché l'indirizzo di PEC dei soggetti abilitati esterni.
2. Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al Regolamento.
3. I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l'inserimento manuale dei dati.
4. Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:
 - a) soggetti rappresentanti un ente pubblico o privato, chiamati a svolgere una specifica attività processuale nell'ambito di procedimenti civili o penali, escluse le parti private;
 - b) professionisti iscritti in albi ed elenchi istituiti con legge;
 - c) professionisti non iscritti ad alcun albo: tutti i soggetti nominati dal giudice come consulenti tecnici d'ufficio, periti o più in generale ausiliari del giudice, non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (ad eccezione degli avvocati).
5. Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.
6. Il ReGIndE è consultabile dai soggetti abilitati esterni tramite il proprio punto di accesso o tramite il PST, su connessioni sicure, attraverso un apposito web service; i relativi WSDL sono pubblicati nell'area pubblica del PST.

Articolo 8

(Alimentazione del registro generale degli indirizzi elettronici)

1. L'alimentazione del ReGIndE avviene previo invio al responsabile per i sistemi informativi automatizzati di un documento di censimento contenente le informazioni necessarie ad identificare:
 - a) l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;
 - b) il nominativo e il codice fiscale del delegato all'invio dell'albo, che dovrà sottoscrivere con firma digitale o firma elettronica qualificata l'albo in trasmissione;
 - c) la casella di PEC utilizzata per l'invio dell'albo.
2. Il documento di censimento di cui al comma precedente aderisce al modello reperibile nell'area pubblica del portale e viene inviato all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.ddsc@giustiziacert.it.
3. Terminate le operazioni di censimento da parte del responsabile per i sistemi informativi automatizzati, l'ente mittente del documento di censimento riceve una risposta; in caso di esito positivo, l'ente può procedere all'invio dell'albo secondo le seguenti specifiche:

- a) il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;
 - b) non vi sono vincoli sull'oggetto né sul corpo del messaggio;
 - c) l'indirizzo di PEC mittente deve essere censito tra quelli delegati all'invio e riportati nel documento di censimento;
 - d) deve essere allegato un solo file (ComunicazioniSoggetti.xml sottoscritto con firma digitale o firma elettronica qualificata);
 - e) la firma digitale o firma elettronica qualificata deve appartenere al soggetto delegato di cui al comma 1, lettera b, sulla base del codice fiscale censito;
 - f) il file ComunicazioniSoggetti.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;
 - g) il codice ente specificato nel file deve essere tra quelli censiti.
4. Il mancato rispetto di uno o più dei vincoli di cui all'articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l'allegato ComunicazioniSoggetti.xml viene scartato.
5. A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso “– Esito” e riporta in allegato l'esito dell'elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell'Allegato 3.
6. L'esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come, ad esempio, codice fiscale inesistente), sia ad errori legati a vincoli e prerequisiti che presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richiedente e dei soggetti abilitati all'invio dell'albo).
7. Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell'inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di PEC di cortesia in cui si attesta l'avvenuta registrazione.

Articolo 9

(Professionisti non iscritti in albi)

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

Articolo 10

(Indirizzi PEC delle pubbliche amministrazioni e degli enti privati)

1. La pubblica amministrazione o l'ente privato che deve comunicare il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni, ai sensi dell'articolo 16, comma 12, primo periodo, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, procede inserendo tale indirizzo sul PST.

2. Ai fini di cui al comma precedente, l'amministrazione pubblica o l'ente privato invia all'indirizzo di posta elettronica certificata della DGSIA (prot.dgsia.ddsc@giustiziacert.it) un documento aderente allo specifico modello disponibile nell'area pubblica del PST, contenente le seguenti informazioni:

- a) denominazione e codice fiscale della amministrazione pubblica o dell'ente privato;
- b) nominativo e codice fiscale del soggetto incaricato di inserire o modificare l'indirizzo di PEC dell'amministrazione pubblica sul PST;
- c) denominazione e codice fiscale o, in mancanza, in caso di amministrazione pubblica, il codice IPA dei propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni e notificazioni per via telematica nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale; in mancanza di codice fiscale o di codice IPA si provvederà ai sensi dell'articolo 11, comma 2, lettera a);
- d) denominazione e codice fiscale o, in mancanza, in caso di amministrazione pubblica, il codice IPA delle specifiche aree organizzative omogenee presso cui l'amministrazione pubblica elegge domicilio ai fini del giudizio; in mancanza di codice fiscale o di codice IPA si provvederà ai sensi dell'articolo 11, comma 2, lettera a).

3. Il soggetto incaricato di cui alla lettera b) del comma precedente accede ad un'apposita area riservata del PST, previa identificazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica:

- a) l'indirizzo di PEC della pubblica amministrazione o dell'ente privato;
- b) il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti o rappresentanti, tramite i quali la pubblica amministrazione o l'ente privato stanno in giudizio personalmente o svolgono attività processuale consentita; tali soggetti alimentano il ReGIndE.

4. Inserito o modificato l'indirizzo di PEC di cui al comma precedente, il soggetto incaricato inserisce o modifica il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti o rappresentanti tramite i quali la pubblica amministrazione o l'ente privato sta in giudizio personalmente o svolge attività processuale consentita; tali soggetti alimentano il ReGIndE.

5. Per le amministrazioni pubbliche il cui indirizzo di PEC sia già censito ai sensi dell'articolo 16, comma 12, primo periodo, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, la comunicazione dei dati di cui alle lettere c) e d) del comma 2 e delle loro successive modificazioni avviene mediante l'invio di un documento, aderente allo specifico modello reperibile sull'area pubblica del PST, al medesimo indirizzo di posta elettronica certificata della DGSIA indicato al comma 2.

6. L'elenco degli indirizzi di PEC delle pubbliche amministrazioni e degli enti privati è consultabile dagli uffici giudiziari e dagli UNEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni.

7. L'elenco degli indirizzi di PEC di cui al comma 3, è consultabile dagli avvocati tramite il proprio punto di accesso o tramite il PST (area riservata), su connessioni sicure, attraverso un apposito web service, che verifica la presenza dell'avvocato sul ReGIndE; i relativi WSDL sono pubblicati nell'area pubblica del PST. L'accesso è tracciato in appositi log, che il Ministero della giustizia conserva per cinque anni, recanti: il punto di accesso attraverso cui è stato effettuato l'accesso, la data e l'ora dell'accesso.

Articolo 11

(Indirizzi PEC degli organi, articolazioni e aree organizzative omogenee delle pubbliche amministrazioni)

1. Effettuate dall'incaricato dell'amministrazione pubblica le attività previste dal comma 3 dell'articolo 10, gli organi, le articolazioni, anche territoriali, e le aree organizzative omogenee (AOO), indicate nel documento di cui al comma 2 dell'articolo 10, comunicano il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni.

2. Ai fini del comma precedente, ciascun organo, articolazione, anche territoriale, o area organizzativa omogenea (AOO) invia all'indirizzo di posta elettronica certificata della DGSIA (prot.dgsia.ddsc@giustiziacert.it) un documento di censimento, aderente al modello reperibile nell'area pubblica del PST, contenente le seguenti informazioni:

a) denominazione e codice fiscale dell'amministrazione pubblica di cui al comma 1 ed il codice fiscale dell'organo, dell'articolazione, anche territoriale, o dell'area organizzativa omogenea stessa o, in mancanza, il relativo codice IPA. In difetto di codice fiscale o di codice IPA, la DGSIA assegnerà un codice identificativo univoco che sarà reso noto nella comunicazione di avvenuto censimento e che, unitamente al codice fiscale dell'amministrazione pubblica di cui al comma 1, dovrà essere indicato per la costituzione in giudizio e per i depositi telematici;

b) nominativo e codice fiscale del soggetto incaricato di inserire o modificare gli indirizzi di PEC dell'organo, dell'articolazione o della AOO sul PST.

3. Il soggetto incaricato di cui alla lettera b) del comma precedente accede ad un'apposita area riservata del PST, previa identificazione autenticazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica l'indirizzo di PEC dell'organo, dell'articolazione, anche territoriale, o della AOO.

4. Effettuate le attività di cui al comma che precede, il soggetto incaricato inserisce o modifica il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti tramite i quali l'organo, l'articolazione, anche territoriale, o l'area organizzativa omogenea sta in giudizio personalmente; tali soggetti alimentano il ReGIndE.

5. L'elenco degli indirizzi di PEC degli organi e delle articolazioni, anche territoriali, nonché la speciale sezione dell'elenco contenente gli indirizzi PEC delle aree organizzative omogenee (AOO) delle amministrazioni pubbliche sono consultabili dagli uffici giudiziari e dagli UNEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni e dagli avvocati secondo le medesime modalità previste dal comma 5 dell'articolo 10.

Articolo 12

(Sistemi informatici per i soggetti abilitati interni)

1. I sistemi informatici a disposizione dei soggetti abilitati interni sono conformi alle regole di cui al decreto del Ministro della giustizia 27 aprile 2009 e mettono a disposizione le funzioni relative a:
 - a) ricezione, accettazione e trasmissione dei dati e dei documenti informatici;
 - b) consultazione e gestione del fascicolo informatico.
2. Per l'accesso ai sistemi di cui al comma precedente dall'interno degli uffici giudiziari, l'identificazione è effettuata mediante coppia di credenziali "nome utente/password" oppure mediante autenticazione a due fattori.
3. Per l'accesso ai sistemi di cui al comma 1 dall'esterno della Rete Giustizia, l'identificazione è effettuata dal PST sulla base del sistema "Active Directory Nazionale" (ADN) tramite autenticazione a due fattori; ai soli fini del recupero dall'esterno delle informazioni di registro da parte dei sistemi a disposizione dei magistrati in ambito civile, è sufficiente l'identificazione sulla base del sistema ADN purché l'interrogazione dei dati finalizzati al recupero preveda l'indicazione del numero di ruolo generale nonché del codice fiscale dell'attore principale e del convenuto principale del procedimento.

Articolo 13

(Trattamento dei dati personali)

1. Nell'ambito dei sistemi informatici del processo civile e penale telematico, il Ministero della giustizia è responsabile della gestione e organizzazione del portale dei servizi telematici, curando lo sviluppo, il funzionamento e la manutenzione delle componenti informatiche.
2. Nell'ambito del processo civile e penale telematico, sono coinvolti, per le finalità rispettivamente perseguite e nei limiti delle proprie funzioni istituzionali, il Ministero della giustizia e gli organi giudiziari.
3. Gli organi giudiziari, quali Titolari del trattamento nell'ambito dell'esercizio delle proprie funzioni giurisdizionali, si avvalgono dei servizi telematici resi disponibili dal Ministero della giustizia e forniscono a tal fine ai soggetti operanti sotto la propria autorità ed abilitati ad accedere ai dati apposite istruzioni sul trattamento. Rispetto ai predetti trattamenti, il Ministero agisce quale Responsabile del trattamento per conto degli organi giudiziari, per le finalità di gestione e organizzazione anche strumentale dei servizi telematici a livello centrale.
4. I gestori dei punti di accesso forniscono ai soggetti abilitati esterni al dominio giustizia i servizi di connessione al portale dei servizi telematici, secondo le regole tecnico-operative di cui al DM 44/2011 e trattano i dati personali quali Titolari del trattamento nel caso in cui accedano per proprio conto ai servizi telematici o quali Responsabili del trattamento nel caso in cui agiscano per conto di soggetti abilitati esterni.
5. Il Ministero della giustizia si avvale di soggetti fornitori di tecnologie e servizi professionali funzionali all'erogazione dei servizi telematici, tra cui la gestione del sistema di posta elettronica certificata, quali Responsabili del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo 18 maggio 2018, n. 51, che assicurino, in particolare, misure tecniche e organizzative adeguate a garantire la protezione dei dati personali e la tutela dei diritti degli interessati.
6. Il Ministero della giustizia assicura adeguati livelli di sicurezza, aggiornamento tecnologico, economicità ed efficienza dei sistemi informatici utilizzati nell'ambito del processo civile e penale telematico, al fine di conseguire un miglioramento dell'organizzazione dei servizi di cancelleria e di

raggiungere una maggiore trasparenza delle informazioni relative ai procedimenti giurisdizionali.

7. I Titolari del trattamento sono tenuti a segnalare tempestivamente al Ministero della giustizia qualsiasi incidente di sicurezza, del quale siano venuti a conoscenza, suscettibile di configurare una violazione dei dati personali di cui all'articolo 4, punto 12), del Regolamento (UE) 2016/679 o all'articolo 2, comma 1, lettera m), del decreto legislativo 18 maggio 2018, n. 51. Il Ministero informa, senza ingiustificato ritardo, gli ulteriori Titolari del trattamento per i quali l'incidente di sicurezza possa produrre effetti in relazione alle attività di trattamento da questi effettuate, in modo da consentire loro di stabilire se si è verificata una violazione dei dati personali, di valutare i rischi per i diritti e le libertà delle persone fisiche che ne derivano, di adottare misure per porvi rimedio e per attenuare i possibili effetti negativi, nonché di verificare la sussistenza dei presupposti per la notifica al Garante, ai sensi dell'articolo 33 del Regolamento (UE) 2016/679 o dell'articolo 26 del decreto legislativo 18 maggio 2018, n. 51, e, se del caso, per la comunicazione agli interessati, ai sensi dell'articolo 34 del Regolamento (UE) 2016/679 o dell'articolo 27 del decreto legislativo 18 maggio 2018, n. 51. Le modalità operative di condivisione delle informazioni di cui al presente comma sono definite in un disciplinare adottato dal Ministero della Giustizia, sentiti gli organi giudiziari.

8. Il Ministero della Giustizia, quale Responsabile del trattamento per conto degli organi giudiziari, gestisce le violazioni dei dati personali, di cui viene a conoscenza, secondo la procedura indicata nell'atto di designazione adottato ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 e dell'articolo 18 del decreto legislativo 18 maggio 2018, n. 51. Tale atto prevede, in particolare, che il Responsabile assista i Titolari nel garantire l'adempimento degli obblighi di cui agli articoli 33 e 34 del Regolamento (UE) 2016/679 e agli articoli 26 e 27 del decreto legislativo 18 maggio 2018, n. 51, e metta a disposizione degli stessi Titolari tutti gli elementi necessari a dimostrarne il rispetto. Fermo quanto previsto nell'atto di designazione, il Ministero, sentiti gli organi giudiziari, può definire le modalità di gestione delle violazioni dei dati personali mediante l'adozione di specifici protocolli operativi.

Articolo 14

(Fascicolo informatico)

1. Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.

2. Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutti i metodi – esposti attraverso appositi web service – necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione.

3. Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:

- a) il codice fiscale del soggetto che ha effettuato l'accesso;
- b) il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);
- c) la data e l'ora dell'accesso.

4. Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni dalla data di esecuzione di ciascun accesso e sarà oggetto di allarmi volti a rilevare eventuali comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti abilitati. Inoltre, a fronte di tali allarmi o di verifiche a campione, tali log potranno essere soggetti ad attività di controllo interno.

CAPO III

TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Articolo 15

(Formato dell'atto del procedimento in forma di documento informatico)

1. L'atto del procedimento civile o penale in forma di documento informatico, da depositare telematicamente nell'ufficio giudiziario, deve rispettare i seguenti requisiti:

- a) è in formato PDF o PDF/A;
- b) è privo di elementi attivi;
- c) è ottenuto dalla trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
- d) è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;
- e) è privo di protezione di password;
- f) nel procedimento civile è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata.
- g) nel procedimento penale per gli atti che le parti formano personalmente, se depositati come atto principale, è consentita la scansione di documento analogico purché in bianco e nero e con una risoluzione pari a 200 dpi.

2. La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CAdES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo "firme multiple indipendenti" o parallele, e prevede che uno o più soggetti firmino, ognuno con la propria chiave privata, lo stesso documento (o contenuto della busta). L'ordine di apposizione delle firme dei firmatari non è significativo e un'alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica; nel caso del formato CAdES il file generato si presenta con un'unica estensione p7m. Il meccanismo qui descritto è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

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

Articolo 16

(Formato dei documenti informatici allegati)

1. I documenti informatici allegati, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:
 - a) documenti impaginati - PDF o PDF/A (.pdf), Rich-Text Format (.rtf).
 - b) Immagini raster - JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), GIF (.gif), DICOM (.dcm).
 - c) Video - formati video delle famiglie MPEG2 e MPEG4 (.mp4, .m4v, .mov, .mpg, .mpeg), AVI (.avi).
 - d) Audio: MP3 (.mp3), FLAC (.flac), audio RAW (.raw), Waveform Audio File Format (.wav), AIFF (.aiff, .aif).
 - e) Testo - TXT (.txt).
 - f) Ipertesto – XML Extended markup language (.xml), HTML (.html, .htm).
 - g) Posta elettronica - eml (.eml), purché contenenti file nei formati di cui alle lettere precedenti (a-f)
 - h) Posta elettronica - .msg, anche se contenenti file nei formati di cui alle lettere da a) a g).
 - i) Formato compresso: è consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti alle lettere precedenti: .zip, .rar, .arj
2. Gli allegati sono sottoscritti con firma digitale o firma elettronica qualificata nei casi previsti dalla legge. Nel caso di formati compressi la firma digitale, se presente, deve essere applicata dopo la compressione.
3. La procura alle liti, sia come originale informatico sottoscritto digitalmente, sia come copia informatica per immagine di documento analogico, deve essere prodotta in formato PDF o PDF/A, priva di elementi attivi, tra cui macro e campi variabili e deve essere firmata digitalmente dal difensore.

Articolo 17

(Trasmissione di atti da parte dei soggetti abilitati esterni nel procedimento civile)

1. Nel procedimento civile l'atto in forma di documento informatico e gli allegati di cui all'articolo 16, sono trasmessi dai soggetti abilitati esterni mediante la posta elettronica certificata di cui al d.p.r. 11 febbraio 2005, n. 68.
2. L'atto e gli allegati sono contenuti nella cosiddetta "busta telematica", ossia un file in formato MIME che riporta tutti i dati necessari per l'elaborazione da parte del sistema ricevente (gestore dei servizi telematici); in particolare la busta contiene il file Atto.enc, ottenuto dalla cifratura del file Atto.msg, il quale contiene a sua volta:
 - a) IndiceBusta.xml: il DTD è riportato nell'Allegato 4. Tale file deve essere omissivo qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b).;
 - b) DatiAtto.xml: gli XSD sono riportati nell'Allegato 5;

c) <nome file (libero)>: atto vero e proprio, in formato PDF o PDF/A, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 15 comma 2;

d) AllegatoX.xxx: uno o più allegati nei formati di file di cui all'articolo 16, eventualmente sottoscritti con firma digitale o firma elettronica qualificata; il nome del file può essere scelto liberamente.

3. La cifratura di Atto.msg è eseguita con la chiave di sessione (ChiaveSessione) cifrata con il certificato del destinatario; IssuerDname è il Distinguished Name della CA che ha emesso il certificato dell'ufficio giudiziario o dell'UNEP destinatario, SerialNumber è il numero seriale del certificato dell'ufficio giudiziario o dell'UNEP destinatario; l'operazione di cifratura simmetrica del file è effettuato con algoritmo di cifratura dedicato e le chiavi simmetriche di sessione sono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario; le chiavi di cifratura degli uffici giudiziari sono disponibili nell'area pubblica del PST (il relativo percorso e nome file è indicato nel catalogo dei servizi telematici).

4. La dimensione massima consentita per la busta telematica è pari a 60 Megabyte.

5. La busta telematica viene trasmessa all'ufficio giudiziario destinatario in allegato ad un messaggio di posta elettronica certificata che rispetta le specifiche su mittente, destinatario, oggetto, corpo e allegati come riportate nell'Allegato 6.

6. Il gestore dei servizi telematici scarica il messaggio dal gestore della posta elettronica certificata del Ministero della giustizia ed effettua le verifiche formali sul messaggio; le eccezioni gestite sono le seguenti:

a) T001: l'indirizzo del mittente non è censito in ReGIndE;

b) T002: Il formato del messaggio non è aderente alle specifiche;

c) T003: la dimensione del messaggio eccede la dimensione massima consentita.

7. Il gestore dei servizi telematici, nel caso in cui il mittente sia un avvocato, effettua l'operazione di certificazione, ossia recupera lo status del difensore da ReGIndE; nel caso in cui lo status non sia "attivo", viene segnalato alla cancelleria.

8. Il gestore dei servizi telematici effettua i controlli automatici sulla busta telematica; le possibili anomalie all'esito dell'elaborazione della busta telematica sono codificate secondo le seguenti tipologie:

a) WARN (WARNING): anomalia non bloccante; si tratta in sostanza di segnalazioni, tipicamente di carattere giuridico (ad esempio manca la procura alle liti allegata all'atto introduttivo certificato di firma non valido o mittente non firmatario dell'atto);

b) ERROR: anomalia bloccante che si verifica in tutti i casi nei quali è necessario un intervento della cancelleria al fine di consentire l'accettazione dell'atto;

c) FATAL: anomalia bloccante, eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fondamentali per l'elaborazione).

9. A seguito dell'invio dell'atto processuale i sistemi informativi ministeriali procedono alla verifica e alla accettazione automatica del deposito degli atti inviati, salvi i casi di anomalia ovvero quelli in cui è necessario l'intervento degli operatori di cancelleria.

10. In caso di anomalia bloccante (FATAL) il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata, contenente la comunicazione del rifiuto dell'accettazione dell'atto.

11. In caso di accettazione dell'atto, anche dopo l'intervento degli operatori di cancelleria, il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata, contenente la comunicazione dell'avvenuto deposito dell'atto, con effetto a decorrere dal momento in cui è stata generata la ricevuta di accettazione da parte del gestore di posta elettronica certificata del depositante, ai sensi dell'articolo 6, comma 1, del d.p.r. 11 febbraio 2005, n. 68.

12. La busta telematica è conservata nel sistema documentale di cui all'articolo 14, comma 2.

Articolo 18

(Trasmissione di atti attraverso il portale delle notizie di reato)

1. La trasmissione di atti e di documenti in modalità telematica agli uffici del pubblico ministero presso i tribunali ordinari, da parte degli ufficiali e degli agenti di polizia giudiziaria e di ogni altro pubblico ufficiale od incaricato di pubblico servizio tenuto per legge alla trasmissione della notizia di reato, avviene attraverso il PNR, accessibile all'indirizzo: <https://portalendr.giustizia.it/NdrWEB/home.do>.

2. L'abilitazione dei referenti interni agli uffici del pubblico ministero avviene tramite la procedura di seguito descritta:

- a) il procuratore della Repubblica nomina uno o più referenti interni per il PNR e ne comunica le generalità alla DGSIA a mezzo protocollo;
- b) il referente dell'ufficio del pubblico ministero si accredita tramite l'applicativo RA.FE. richiedendo il certificato alla DGSIA;
- c) attraverso lo stesso applicativo la DGSIA verifica e approva la richiesta, inviando al referente una comunicazione di posta elettronica che contiene il Certificato per l'accesso a RA.FE.;
- d) il referente dell'ufficio del pubblico ministero, con l'applicativo RA.FE., gestisce la distribuzione dei Certificati ai referenti degli uffici fonte.

3. L'abilitazione dei referenti del PNR degli uffici fonte avviene tramite la procedura di seguito descritta:

- a) l'Ufficio Fonte individua uno o più referenti e ne comunica le generalità all'ufficio del pubblico ministero del circondario di riferimento;
- b) il referente dell'Ufficio Fonte, tramite l'applicativo RA.FE., richiede il certificato all'ufficio del pubblico ministero a cui sono state inviate le proprie generalità;
- c) con lo stesso applicativo il referente dell'ufficio del pubblico ministero destinatario della richiesta la approva e la invia al richiedente una comunicazione di posta elettronica contenente il Certificato di accesso a RA.FE.

4. L'abilitazione degli operatori degli uffici fonte avviene tramite la procedura di seguito descritta:

- a) il referente dell'Ufficio Fonte, con l'applicativo RA.FE., gestisce la distribuzione dei Certificati agli operatori del proprio ufficio;
- b) il referente dell'Ufficio Fonte, con l'applicativo RA.FE., genera un Certificato per ogni operatore del proprio ufficio ed invia loro una comunicazione di posta elettronica contenente il predetto Certificato;
- c) l'operatore accede al PNR col proprio certificato ed è abilitato all'invio delle comunicazioni di atti e di documenti in modalità telematica agli uffici del pubblico ministero.

5. Il Certificato emesso è nominativo e consente l'accesso all'applicativo per cui è stato generato. Il Certificato deve essere installato sulla postazione di lavoro ed ha una validità di due anni dal momento della emissione. Il Certificato può essere revocato, impedendo all'utente titolare di accedere

all'applicativo. Il referente dell'ufficio fonte è tenuto con cadenza periodica, almeno trimestrale, a verificare e eventualmente disabilitare gli utenti non più autorizzati ad accedere al portale, mediante le funzionalità messe a disposizione dall'applicativo RAFF.

6. L'atto in forma di documento informatico contenente la comunicazione della notizia di reato e gli atti contenenti le note informative successive, rispettano i requisiti di cui all'articolo 15.

7. Gli allegati, in forma di documento informatico, rispettano i requisiti di cui all'articolo 16.

8. Gli atti e gli allegati di cui ai commi 6 e 7 possono avere una dimensione massima complessiva di 60 Megabyte.

9. Le tipologie di firma ammesse sono CADES e PAdES.

10. Gli atti e gli allegati sono trasmessi secondo la procedura del PNR che consiste:

- a) nell'inserimento dei dati richiesti dal sistema;
- b) nel caricamento dell'atto contenente la notizia di reato o la nota informativa successiva ed i relativi allegati;
- c) nell'esecuzione del comando di invio.

11. Il PNR consente di salvare i dati ed i documenti caricati per un successivo invio. I dati ed i documenti restano disponibili per un successivo invio per quindici giorni dal primo salvataggio in bozza, decorsi i quali verranno automaticamente cancellati. Il PNR dà evidenza all'operatore dell'ufficio fonte del decorso dei primi cinque giorni. All'atto del salvataggio in bozza, l'operatore dell'ufficio fonte indica l'ufficio del pubblico ministero destinatario. La predetta indicazione può essere modificata dall'operatore sino al momento dell'invio della notizia di reato.

12. Il PNR genera la ricevuta di accettazione nel momento in cui la comunicazione diviene disponibile nelle "Annotazioni Preliminari dal Portale". La ricevuta di accettazione, che è scaricabile e resta a disposizione dell'operatore dell'ufficio fonte sul PNR, contiene:

- a) data e orario in cui la comunicazione diviene disponibile nelle "Annotazioni Preliminari dal Portale";
- b) tipologia notizia di reato;
- c) ufficio Fonte;
- d) ufficio del pubblico ministero destinatario;
- e) numero protocollo PNR;
- f) numero protocollo "Annotazioni Preliminari dal Portale".

13. Il PNR consente, in caso di urgenza, la comunicazione di notizie di reato selezionando l'apposita funzione. Una notizia di reato urgente viene selezionata con priorità maggiore per l'invio rispetto ad una ordinaria.

14. L'operatore dell'ufficio fonte può visualizzare lo stato della comunicazione, così come definito di seguito:

- a) **ATTESA DI INVIO:** presa in carico dal sistema;
- b) **INVIATA:** In transito;
- c) **ACQUISITA:** Comunicazione nella disponibilità dell'ufficio del pubblico ministero destinatario nelle "Annotazioni preliminari da Portale" (primo invio);
- d) **RIGETTATA:** La segreteria dell'ufficio del pubblico ministero non ha convalidato i dati e/o gli allegati della notizia di reato;
- e) **RIACQUISITA:** Comunicazione nuovamente nella disponibilità dell'ufficio del pubblico

ministero destinatario nelle “Annotazioni preliminari da Portale” (dopo un rigetto da parte dell’ufficio del pubblico ministero);

f) **PROTOCOLLATA**: Iscritta nel registro/inserita nel fascicolo come nota informativa successiva.
15. Gli atti e i documenti, nonché gli allegati, correttamente acquisiti da Re.Ge.WEB sono visibili unicamente dal personale di segreteria abilitato dal procuratore della Repubblica all’accesso alle “Annotazioni Preliminari dal Portale”, secondo gli stati delle comunicazioni individuati di seguito:

- a) **ACQUISITA**: Nella disponibilità dell’ufficio del pubblico ministero destinatario (primo invio);
- b) **RIGETTATA**: L’ufficio del pubblico ministero non ha convalidato i dati e/o gli allegati della notizia di reato;
- c) **RIACQUISITA**: Nuovamente nella disponibilità dell’ufficio del pubblico ministero (dopo un rigetto).

16. Le trasmissioni utilizzano algoritmi di cifratura asimmetrica e chiavi di sessione con le seguenti caratteristiche:

- a) chiave di sessione a 256 bit per cifrare gli atti, i documenti e gli allegati con AES;
- b) la chiave di sessione viene cifrata con una chiave asimmetrica RSA a 2048 bit.

17. I dati personali, una volta che la comunicazione assume lo stato “Acquisita” di cui al comma 14 non sono più presenti sul PNR.

Articolo 19

(Trasmissione di atti da parte dei soggetti abilitati esterni nel procedimento penale)

1. Nel procedimento penale l’atto in forma di documento informatico di cui all’articolo 15, e gli allegati di cui all’articolo 16, sono trasmessi dai soggetti abilitati esterni mediante il PDP, accessibile dal PST all’indirizzo <https://pst.giustizia.it>, tramite l’area riservata di cui all’articolo 5“, con le modalità di identificazione informatica di cui all’articolo 6.

2. L’accesso al PDP è consentito unicamente ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all’Avvocatura dello Stato.

3. Le trasmissioni utilizzano algoritmi di cifratura asimmetrica e chiavi di sessione conformi a quanto previsto dall’articolo 17, comma 3.

4. Alla trasmissione dell’atto di nomina nella procura della Repubblica deve essere allegato un atto abilitante, quando il procedimento sia in fase di indagine preliminare e non sia stato ancora emesso o non sia previsto uno degli avvisi di cui agli articoli 408, 411 o 415 bis codice di procedura penale.

5. La preventiva annotazione nel ReGeWEB, a cura delle cancellerie e segreterie degli uffici giudiziari, del codice fiscale dei soggetti abilitati esterni è requisito indispensabile per ottenere la visibilità dei procedimenti autorizzati.

6. La procedura di trasmissione tramite il PDP consiste:

- a) nell’inserimento dei dati richiesti dal sistema;
- b) nel caricamento dell’atto del procedimento e dei documenti allegati;
- c) nell’esecuzione del comando di invio.

7. Il PDP, al termine della procedura di cui ai commi precedenti genera la ricevuta di accettazione del deposito (articolo 172 c.p.p.) che contiene:

- a) un identificativo unico nazionale nella forma anno/numero;
- b) i dati inseriti dal depositante;
- c) la data e l'orario dell'operazione di invio rilevati dai sistemi del Ministero di giustizia.

8. La ricevuta è scaricabile in formato PDF e resta, comunque, a disposizione del difensore sul PDP.

9. A seguito dell'invio dell'atto processuale i sistemi informativi ministeriali procedono alla verifica ed accettazione automatica del deposito degli atti inviati dai difensori rispetto ai quali vi è corrispondenza tra i dati inseriti sul PDP ed i dati di registro del procedimento penale, senza intervento degli operatori di segreteria e di cancelleria.

10. Il difensore può verificare lo stato del deposito accedendo al PDP nella sezione "Consultazione - Depositi"

11. Il personale amministrativo degli uffici giudiziari ha a disposizione apposite funzionalità per la gestione dei depositi pervenuti tramite il PDP e si avvale dell'ausilio dell'esito dei preventivi controlli automatici eseguiti dai sistemi.

12. All'accettazione o al rigetto del deposito gli atti del procedimento ed i documenti allegati in forma di documento informatico sono conservati nel sistema documentale di cui all'articolo 14, comma 2.

13. I possibili valori di stato del deposito sul PDP sono:

- a) INVIATO: eseguita con successo l'operazione di "Invio";
- b) IN TRANSITO: in attesa di smistamento al sistema informativo dell'ufficio giudiziario destinatario; nel momento in cui il deposito assume lo stato "in transito", il PDP cancella tutti i dati personali;
- c) ACCETTATO (automaticamente o a seguito di verifiche ove previste): intervenuta associazione dell'atto inviato al procedimento di riferimento. L'associazione è automatica nel caso di coincidenza tra i dati inseriti sul PDP ed i dati di registro del procedimento penale e, quando previsto, in presenza dell'atto abilitante di cui all'articolo 19, comma 5. L'associazione è ad opera del cancelliere o del segretario qualora, dopo le verifiche, sia stato individuato univocamente il procedimento di riferimento. Nel caso di denuncia, di querela e di istanza di procedimento, l'accoglimento equivale al ricevimento ed iscrizione del procedimento nel ReGeWEB da parte della procura della Repubblica;
- d) IN VERIFICA: anomalia bloccante, il deposito è pervenuto nel sistema dell'ufficio giudiziario destinatario ma non essendoci coincidenza di dati non è stato automaticamente associato ad un procedimento ed è sottoposto a verifiche da parte del personale dell'ufficio;
- e) RIFIUTATO: anomalia bloccante; rifiuto del deposito successivo alle verifiche automatiche e ad opera del personale dell'ufficio; la motivazione è riportata sul PDP;
- f) ERRORE TECNICO: anomalia bloccante; si è verificato un problema in fase di trasmissione; il difensore è invitato dal messaggio di stato del PDP ad effettuare nuovamente il deposito.

14. Il difensore può consultare tutti gli stati del deposito accedendo alla relativa sezione del PDP, e scaricare un documento che attesta gli esiti: accolto, rigettato ed errore tecnico. Tali esiti sono altresì comunicati a mezzo mail ordinaria, previa configurazione della stessa da parte del difensore nella sezione "Preferenze" del PDP.

15. La dimensione massima consentita per ciascun deposito di atti ed eventuali allegati è pari a 60 Megabyte per singolo file, fino ad un massimo di 600 Megabyte per l'intero deposito.

Articolo 20

(Trasmissione di atti da parte dei soggetti abilitati interni)

1. Nei procedimenti civili e nei procedimenti penali i soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro trasmissione alla cancelleria o alla segreteria dell'ufficio giudiziario.
2. Nel procedimento civile l'atto è inserito nella medesima busta telematica di cui all'articolo 17 e viene trasmesso su canale sicuro (al gestore dei servizi telematici, tramite collegamento sincrono (http/SOAP); si applicano le disposizioni di cui all'articolo 12, comma 2.
3. Se il provvedimento del magistrato è redatto in forma di documento analogico, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia in formato PDF, nel rispetto di quanto previsto dall'articolo 22 del CAD, e lo inserisce immediatamente nel fascicolo informatico.

Articolo 21

(Comunicazioni e notificazioni per via telematica)

1. Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall'ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell'utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi di cui agli articoli 6-bis, 6-ter e 6-quater del CAD; il formato del messaggio è riportato nell'Allegato 8; la comunicazione o notificazione è riportata nel corpo del messaggio nonché nel file allegato Comunicazione.xml (il relativo DTD è riportato nell'Allegato 4).
2. La cancelleria o la segreteria dell'ufficio giudiziario, attraverso apposite funzioni messe a disposizione dai sistemi informatici di cui all'articolo 12, provvede ad effettuare una copia per immagine in formato PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.
3. Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni.

Articolo 22

(Comunicazioni e notificazioni contenenti categorie particolari di dati personali)

1. La comunicazione o la notificazione che contiene categorie particolari di dati personali è effettuata per estratto; in questo caso al destinatario viene recapitato l'avviso di disponibilità, secondo il formato riportato nell'Allegato 8; il destinatario effettua il prelievo dell'atto integrale accedendo all'indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso.
2. Il prelievo di cui al comma precedente avviene attraverso l'apposito servizio proxy del PST, su canale sicuro; tale servizio effettua l'identificazione informatica dell'utente, ai sensi dell'articolo 6; il prelievo è consentito unicamente se l'utente è registrato nel ReGIndE.

3. Il prelievo di cui al comma precedente avviene da un'apposita area di download del gestore dei servizi telematici, dove viene gestita e mantenuta un'apposita tabella recante le seguenti informazioni:

- a) il codice fiscale del soggetto che ha effettuato il prelievo o la consultazione;
- b) il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 5);
- c) la data e l'ora di invio dell'avviso;
- d) la data e l'ora del prelievo o della consultazione.

4. Le informazioni di cui al comma precedente vengono conservate per cinque anni.

5. Nel caso in cui il destinatario sia un'impresa iscritta nel relativo registro o una Pubblica Amministrazione, la comunicazione o la notificazione che contiene categorie particolari di dati personali è effettuata ai sensi del comma 1; l'utente che accede all'indirizzo (URL) contenuto nel messaggio di PEC di avviso, su canale sicuro, viene identificato ai sensi dell'art 6 ed è abilitato ad accedere all'atto integrale solo se appartiene all'impresa destinataria come risultante dal registro delle imprese o se è un dipendente della Pubblica Amministrazione autorizzato.

Articolo 23

(Notificazioni per via telematica a cura degli UNEP)

1. Le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP in formato XML, attraverso un colloquio diretto, via web service, tra i rispettivi gestori dei servizi telematici, su canale sicuro, oppure tramite posta elettronica certificata.

2. Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tecnici di cui agli articoli 17, 18 e 19; all'interno della busta telematica è inserito il file RichiestaParte.xml, il cui XML-Schema è riportato nell'Allegato 5.

3. All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.

4. Alla notificazione per via telematica da parte dell'UNEP si applicano le specifiche della comunicazione per via telematica di cui all'articolo 21; il formato del messaggio di posta elettronica certificata è riportato nell'Allegato 7.

5. Ai fini della notificazione per via telematica, il sistema informatico dell'UNEP recupera l'indirizzo di posta elettronica del destinatario a seconda della sua tipologia:

- a) soggetti abilitati esterni e professionisti iscritti in albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con legge del 28 gennaio 2009, n. 2: dal ReGIndE, ai sensi dell'articolo 7, comma 6, nonché dall'indice nazionale delle imprese e dei professionisti (INI-PEC), sezione professionisti, costituito ai sensi dell'articolo 6-bis del CAD;
- b) imprese: dall'indice nazionale delle imprese e dei professionisti (INI-PEC), sezione imprese, costituito ai sensi dell'articolo 6-bis del CAD;

c) cittadini, professionisti che svolgono una professione non organizzata in ordini, albi o collegi ai sensi della legge n. 4/2013, enti di diritto privato non tenuti all'iscrizione nell'INI-PEC: dall'indice nazionale dei domicili digitali (INAD), costituito ai sensi dell'articolo 6-quater del CAD.

6. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette - per via telematica a chi ha richiesto il servizio - il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale o firma elettronica qualificata e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata. La relazione di notificazione è in formato XML e rispetta l'XML-Schema riportato nell'Allegato 5; se il richiedente è un soggetto abilitato esterno, la trasmissione avviene via posta elettronica certificata; il formato del messaggio è riportato nell'Allegato 7.

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

Articolo 24

(Richiesta di copie di atti e documenti nel procedimento civile)

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

2. Il soggetto che ne ha diritto può richiedere alla cancelleria:

- a) copia semplice in formato digitale;
- b) copia semplice per l'avvocato non costituito in formato digitale;
- c) copia autentica in formato digitale;
- d) copia esecutiva in formato digitale;
- e) copia semplice in formato cartaceo;
- f) copia autentica in formato cartaceo;
- g) copia esecutiva in formato cartaceo.

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

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

Articolo 25

(Rilascio delle copie di atti e documenti)

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

2. Nel caso di copia di documenti contenenti categorie particolari di dati personali o nel caso di copia di documenti che eccedono il massimo consentito dalla posta elettronica certificata, il messaggio di cui al comma precedente contiene l'avviso di disponibilità della copia, secondo il formato riportato nell'Allegato 9; il prelievo avviene mediante l'utilizzo dei servizi previsti dall'articolo 28, commi 2, 3 e 4.

Articolo 26

(Notificazioni per via telematica eseguite dagli avvocati)

1. Qualora l'atto da notificarsi sia un documento originale informatico, esso deve essere in formato PDF o PDF/A e ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è ammessa la scansione di immagini. Il documento informatico così ottenuto è allegato al messaggio di posta elettronica certificata.
2. Nei casi diversi dal comma 1, i documenti informatici o copie informatiche, anche per immagine, di documenti analogici, allegati al messaggio di posta elettronica certificata, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti in formato PDF o PDF/A.
3. Nei casi in cui l'atto da notificarsi sia l'atto del processo da trasmettere telematicamente all'ufficio giudiziario (esempio: atto di citazione), si procede ai sensi del precedente comma 1.
4. Qualora il documento informatico, di cui ai commi precedenti, sia sottoscritto con firma digitale o firma elettronica qualificata, si applica quanto previsto all'articolo 16, comma 2.
5. La trasmissione in via telematica all'ufficio giudiziario delle ricevute previste dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53, nonché della copia dell'atto notificato ai sensi dell'articolo 9, comma 1, della medesima legge, è effettuata inserendo l'atto notificato all'interno della busta telematica di cui all'articolo 17 e, come allegati, la ricevuta di accettazione e la ricevuta di avvenuta consegna relativa ad ogni destinatario della notificazione; i dati identificativi relativi alle ricevute sono inseriti nel file DatiAtto.xml di cui all'articolo 15, comma 1, lettera f).

Articolo 27

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

1. Quando si deve procedere ad attestare la conformità di una copia informatica, anche per immagine, ai sensi del terzo comma dell'articolo 16-undecies del decreto-legge 18 ottobre 2012, n.179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 212, l'attestazione è inserita in un documento informatico in formato PDF e contiene una sintetica descrizione del documento di cui si sta attestando la conformità nonché il relativo nome del file. Il documento informatico contenente l'attestazione è sottoscritto dal soggetto che compie l'attestazione con firma digitale o firma elettronica qualificata secondo quanto previsto all'articolo 15, comma 2.
2. Se la copia informatica è destinata ad essere depositata secondo le regole tecniche previste dall'articolo 4 del decreto legge 29 dicembre 2009, n.193, convertito con modificazioni dalla legge 22 febbraio 2010, n. 24, il documento informatico contenente l'attestazione è inserito come allegato nella busta telematica di cui all'articolo 17; i dati identificativi del documento informatico contenente l'attestazione, nonché del documento cui essa si riferisce, sono anche inseriti nel file DatiAtto.xml di cui all'articolo 15, comma 1, lettera f).

3. Se la copia informatica è destinata ad essere notificata ai sensi dell'articolo 3-bis della legge 21 gennaio 1994, n. 53, gli elementi indicati al primo comma, sono inseriti nella relazione di notificazione.

4. Nelle ipotesi diverse dai commi 2 e 3, se la copia informatica è destinata ad essere trasmessa tramite posta elettronica certificata, l'attestazione di cui al primo comma è inserita come allegato al messaggio di posta elettronica certificata.

5. In ogni altra ipotesi, l'attestazione di conformità è inserita in un documento informatico in formato PDF contenente i medesimi elementi di cui al primo comma, l'impronta del documento informatico di cui si sta attestando la conformità e il riferimento temporale di cui ai capitoli 2.2, comma quarto e 2.3, comma sesto delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici del 2021. Il documento informatico contenente l'attestazione è sottoscritto dal soggetto che compie l'attestazione con firma digitale o firma elettronica qualificata. L'impronta del documento può essere omessa in tutte le ipotesi in cui il documento informatico contenente l'attestazione di conformità è inserito, unitamente alla copia informatica del documento, in una struttura informatica idonea a garantire l'immodificabilità del suo contenuto.

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

CAPO IV

CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Articolo 28

(Requisiti di sicurezza)

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

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

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

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

5. Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.

6. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del PST.

7. L'accesso ai servizi di consultazione avviene su canale sicuro previa identificazione informatica su di un PdA o sul PST, secondo le specifiche di cui all'articolo 6; a seguito di tale identificazione, il PdA o il PST attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice

fiscale del soggetto che effettua l'accesso (nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy trasmette la richiesta al web service del gestore dei servizi telematici.

8. In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal Regolamento.

9. In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche dell'Agenzia per l'Italia Digitale; in questo caso, il Direttore generale DGSIA, valutata la soluzione proposta e opportunamente descritta nel piano della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.

10. Il punto di accesso può consentire l'accesso a soggetti delegati da un utente registrato (soggetto delegante), con le stesse modalità di cui ai commi 7, 8 e 9, purché il soggetto delegante abbia predisposto un atto di delega, sottoscritto con firma digitale, che il punto di accesso conserva unitamente alla tracciatura di ogni accesso effettuato su delega; gli atti di conferimento e di revoca della delega sono conservati per tre anni dalla data di cessazione della delega; le informazioni relative agli accessi effettuati su delega sono conservate per cinque anni dalla data di esecuzione di ciascun accesso; le informazioni e gli atti di cui sopra sono forniti su richiesta al Ministero della giustizia.

11. Fuori dai casi previsti ai commi 1 e 10, l'architettura dei servizi di consultazione prevede in via residuale che il PdA o il PST effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che rende disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati identificativi del soggetto vengono inseriti nell'header HTTP della richiesta.

12. I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 3.

13. L'elenco dei PdA autorizzati è pubblicato nell'area pubblica del PST e nel catalogo dei servizi telematici, di cui all'articolo 5, comma 3

14. Il PdA si dota di un piano della sicurezza, depositato al responsabile per i sistemi informativi automatizzati unitamente all'istanza di iscrizione all'elenco pubblico dei punti di accesso, che prevede la trattazione, esaustiva e dettagliata, dei seguenti argomenti:

- a) struttura logistica e operativa dell'organizzazione;
- b) ripartizione e definizione delle responsabilità del personale addetto;
- c) descrizione dei dispositivi installati;
- d) descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);
- e) descrizione delle procedure di registrazione delle utenze e delle procedure di conferimento e revoca delle deleghe;
- f) descrizione relativa all'implementazione dei meccanismi di identificazione informatica;
- g) qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;
- h) procedura di gestione delle copie di sicurezza dei dati;
- i) procedura di gestione dei disastri;

- j) analisi dei rischi e contromisure previste;
 - k) descrizione dell'eventuale processo di delega di cui al comma 10 nonché delle modalità di conservazione dell'elenco dei soggetti delegati e delle eventuali revoche delle deleghe;
 - l) descrizione della modalità di verifica dell'effettiva funzionalità e adeguatezza del sistema di sicurezza del punto di accesso.
15. Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi informativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.
16. Il punto di accesso abilita i propri iscritti unicamente a usufruire dei servizi esplicitamente autorizzati dal responsabile per i sistemi informativi automatizzati e riportati nel catalogo dei servizi telematici.
17. Il PdA si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della giustizia.
18. Il PdA fornisce al Ministero della giustizia, su richiesta, i dati di censimento sul ReGIndE di cui articolo 8 comma 1 per i casi di iscrizione dei professionisti non iscritti in albi di cui articolo 9 comma 1.
19. Il PdA verifica l'effettiva funzionalità e adeguatezza del sistema di sicurezza almeno una volta l'anno e provvede ad inviare l'esito delle stesse, unitamente ad eventuali variazioni nei contenuti del piano, all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.ddsc@giustiziacert.it.

Articolo 29

(Registrazione dei soggetti abilitati esterni e degli utenti privati)

1. L'utente accede ai servizi di consultazione previa registrazione presso un PdA autorizzato o presso il PST tramite le modalità di autenticazione riportate nell'art.6 comma 1.
2. Il PdA o il PST effettuano la registrazione del soggetto abilitato esterno o dell'utente privato, acquisendo il codice fiscale, il nome e il cognome nell'ambito della procedura di identificazione informatica di cui all'articolo 6; attraverso un'apposita maschera web, il soggetto abilitato esterno completa i propri dati, inserendo almeno le seguenti informazioni:
 - a) residenza
 - b) domicilio
 - c) ruolo
 - d) consiglio dell'ordine o ente di appartenenza.
3. Gli esperti e gli ausiliari del giudice, non iscritti ad alcun albo professionale o per i quali il proprio ordine non abbia provveduto all'invio dell'albo, presentano, all'atto della registrazione, copia elettronica in formato PDF dell'incarico di nomina da parte del giudice; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
4. Qualora il professionista sia iscritto ad un albo dei consulenti tecnici, istituito presso un tribunale, lo stesso professionista presenta copia elettronica in formato PDF del provvedimento di

iscrizione all'albo da parte del comitato per la formazione dell'albo dei consulenti tecnici; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che si iscrive.

5. Il Ministero della giustizia e il PdA conservano i dati di cui al comma 2, unitamente alla data in cui è avvenuta la registrazione, e i documenti informatici di cui ai commi 3 e 4 per cinque anni dalla data di cessazione di ogni utenza. Il PdA rende disponibili tali dati e documenti, su richiesta, al Ministero della giustizia.

6. I PdA trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all'allegato 11.

CAPO V

PAGAMENTI TELEMATICI

Articolo 30

(Requisiti relativi al processo di pagamento telematico)

1. Il PST espone ai punti di accesso servizi web per l'esecuzione dei pagamenti telematici utilizzando esclusivamente le funzionalità messe a disposizione da pagoPA, accedendo al portale dei servizi telematici.

2. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del PST

CAPO VI

DISPOSIZIONI TRANSITORIE

Articolo 31

(Entrata in vigore)

1. Il presente provvedimento sarà pubblicato sul PST ed acquista efficacia a decorrere dal 30 settembre 2024.

2. Dalla data di efficacia del presente provvedimento cessano di trovare applicazione le specifiche tecniche adottate con provvedimento del Direttore generale DGSIA del 16 aprile 2014 e successive modifiche.

De Lisi
Vincenzo
MINISTERO
DELLA
GIUSTIZIA
02.08.2024
08:55:43
GMT+00:00

