Consiglio dell'Ordine degli Avvocati di Catania

Il Consiglio dell'Ordine degli Avvocati di Catania ha predisposto il presente *Vademecum* per il deposito degli atti penali, dopo l'entrata in vigore del D.M. 27 dicembre 2024 n. 206.
Il *Vademecum* è frutto di una primissima lettura delle nuove norme e vuole essere un ausilio ragionato all'applicazione delle stesse.
Non ha, ovviamente, alcun valore vincolante né deroga alla disciplina di riferimento.
Si invitano, inoltre, gli Avvocati ad una attenta lettura delle norme e, in particolare, dei commi 5, 6 e 7 dell'articolo 1 del predetto D.M.

LA NUOVA DISCIPLINA DEL DEPOSITO DEGLI ATTI PENALI

DOPO IL D.M. 27.12.2024 N. 206

a cura dell'Avv. Mattia Serpotta

componente della Commissione informatica del Consiglio dell'Ordine degli Avvocati di Catania

1. Premessa

In data 30.12.2024, è entrato in vigore il D.M. 27 dicembre 2024, n. 206 (allegato *sub* 1), rubricato "*Regolamento concernente modifiche al decreto 29 dicembre 2023, n. 217 in materia di processo penale telematico*"[1].

L'articolo 1 ha riscritto e sostituito integralmente l'art. 3 del D.M. 217 del 2023, provvedimento che era stato emanato in attuazione dell'articolo 87, comma 3, del D. Lgs. 150 del 2022 (c.d. Riforma Cartabia), al fine di individuare gli "**uffici giudiziari e le tipologie di atti**" per cui possono essere adottate anche "**modalità non telematiche**" di deposito, nonché i "**termini di transizione**" al "**nuovo**" regime di deposito telematico **obbligatorio** previsto dall'art. 111 *bis* c.p.p.

2. L'art. 111 *bis* c.p.p.

La norma è stata introdotta dal D. Lgs. 150 del 2022 e prevede appunto, in "**ogni stato e grado del procedimento**", la "**esclusività**" della "**modalità telematica**" per il deposito di "**atti, documenti, richieste, memorie**", salve le eccezioni di cui ai commi 3 e 4:

*1. In ogni stato e grado del procedimento, il deposito di atti, documenti, richieste, memorie ha luogo **esclusivamente** con modalità telematiche, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione degli atti e dei documenti informatici.*

*3. La disposizione di cui al comma 1 non si applica agli atti e ai documenti che, **per loro natura o per specifiche esigenze processuali**[2], non possono essere acquisiti in copia informatica.*

*4. Gli atti che le **parti** e la **persona offesa** dal reato compiono **personalmente** possono essere depositati anche con **modalità non telematiche**.*

[1] Pubblicato in Gazzetta Ufficiale, *Serie generale* n. 304 del 30.12.2024.

[2] Così, la relazione illustrativa: "*si pensi a tutti i documenti che vengono versati in originale nel corso di un procedimento, quali, ad esempio, una scrittura privata o un testamento olografo dei quali si contesti l'autenticità, ovvero ancora planimetrie, estratti di mappa, fotografie aeree e satellitari, per i quali appare indispensabile il deposito in forma di documento analogico poste che l'acquisizione in forma di documento informatico priverebbe di nitidezza e precisione i relativi dati, incidendo sul loro valore dimostrativo in sede processuale".*

Dovendo in questa sede semplificare, in base alla disciplina transitoria introdotta dall'art. 87, comma 5, del D. Lgs. 150 del 2022, l'art. 111 *bis* c.p.p., al pari di altre norme ivi richiamate, deve oggi certamente ritenersi entrato in vigore **limitatamente** agli uffici giudiziari e alle categorie di atti per i quali il D.M. 217 del 2023, prima, e il D.M. 206 del 2024, adesso, hanno previsto quella telematica come modalità di deposito **esclusiva e obbligatoria**[3].

3. La definizione di "modalità telematica" e di portale.

L'art. 111 *bis* c.p.p. e tutte le altre norme introdotte dalla Riforma Cartabia non forniscono una definizione di "modalità telematica", non individuano cioè quale sia **il "mezzo**" attraverso il quale avviene la **trasmissione e il deposito** del documento informatico.
Il D.M. 29.12.23 ha sul punto modificato il Regolamento n. 44 del 2011[4] (allegato *sub* 2), introducendo l'art. 13 *bis*:

«*Art. 13 bis (Trasmissione dei documenti da parte dei soggetti abilitati esterni nel procedimento penale).*
— 1. ***Nel procedimento penale, gli atti e i documenti in forma di documento informatico di cui agli articoli 11 e 12 sono trasmessi da parte dei soggetti abilitati esterni attraverso la procedura prevista dal portale dei depositi telematici*** *[...] previa autenticazione del soggetto depositante, secondo le specifiche tecniche previste dall'articolo 34.*
2. Gli atti e i documenti di cui al comma 1, ***si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di accettazione*** *da parte del portale dei depositi telematici, che*

[3] Così, l'art. 87 del D. Lgs. 150 del 2022:
"*4. Sino al quindicesimo giorno successivo alla pubblicazione dei regolamenti di cui ai commi 1 e 3, ovvero* ***sino al diverso termine di transizione previsto dal regolamento di cui al comma 3 per gli uffici giudiziari e per le tipologie di atti in esso indicati****, continuano ad applicarsi, nel testo vigente al momento dell'entrata in vigore del presente decreto, le disposizioni di cui agli articoli 110, 111, comma 1, 116, comma 3-bis, 125, comma 5, 134, comma 2, 135, comma 2, 162, comma 1, 311, comma 3, 391-octies, comma 3, 419, comma 5, primo periodo, 447, comma 1, primo periodo, 461, comma 1, 462, comma 1, 582, comma 1, 585, comma 4, del codice di procedura penale, nonché' le disposizioni di cui l'articolo 154, commi 2, 3 e 4 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271.*
5. Le disposizioni di cui agli articoli 111, commi 2-bis, 2-ter e 2-quater, ***111 bis****, 111-ter, 122, comma 2-bis, 172, commi 6-bis e 6-ter, 175-bis, 386, comma 1-ter, 483, comma 1-bis, 582, comma 1-bis, del codice di procedura penale, cosi' come introdotte dal presente decreto, si applicano a partire* ***dal quindicesimo giorno successivo alla pubblicazione dei regolamenti di cui ai commi 1 e 3****, ovvero* ***a partire dal diverso termine previsto dal regolamento di cui al comma 3 per gli uffici giudiziari e per le tipologie di atti in esso indicati***."

[4] Rubricato "*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*."

attesta il deposito dell'atto o del documento presso l'ufficio giudiziario competente, ***senza l'intervento degli operatori della cancelleria o della segreteria****, salvo il caso di anomalie bloccanti*».

Lo stesso D.M. ha poi introdotto l'art. 7 *bis*, con il quale è stata data una definizione del "portale dei depositi telematici":
«*Art. 7 -bis (Portale dei depositi telematici e delle notizie di reato).*
— 1. Il portale dei depositi telematici consente la trasmissione in via telematica da parte dei soggetti abilitati esterni degli atti e dei documenti del procedimento […].
3. L'accesso ai portali di cui ai commi 1 […] avviene a norma dell'articolo 64 del codice dell'amministrazione digitale e secondo le specifiche stabilite ai sensi dell'articolo 34».

Il portale deve dunque intendersi oggi quale **unico mezzo di trasmissione e di deposito telematico** degli atti del procedimento penale.
L'art. 3 del D.M. 217 del 2023, prima, e l'art. 1 del D.M. 206 del 2024, adesso, equiparano invece il deposito mediante **posta elettronica certificata**, così come disciplinato dall'art. 87 *bis* del D. Lgs. 150 del 2022, al "***deposito non telematico***", cioè con modalità cartacea.

4. La nuova disciplina introdotta dall'art 1 del D.M. 206 del 2024

4.1. Premessa

Come si vedrà adesso nel dettaglio, il D.M. 206 del 2024 ha riprodotto, seppur con delle sostanziali novità, lo schema già previsto dal D.M. 217 del 2023, distinguendo:

- **ipotesi di deposito telematico (portale) obbligatorio**, in cui è cioè **precluso** l'uso della modalità cartacea e della PEC;
- **ipotesi di deposito telematico (portale) non obbligatorio**, in cui è quindi **facoltativo** l'uso del portale, della PEC o della modalità cartacea;
- **ipotesi in cui il deposito telematico (portale) non è allo stato consentito**, nelle quali è quindi possibile **soltanto** l'uso della modalità cartacea o della PEC.

4.2. Ipotesi di deposito telematico (portale) obbligatorio

Il comma 1 dell'art. 3 del D.M. 206 del 2024 individua con maggiore chiarezza rispetto al passato i casi di deposito obbligatorio al portale, identificandoli, non più per fasi o atti, ma per **destinazione**.
A partire dall'1.1.2025, **salve le eccezioni di cui al paragrafo successivo e quelle generali previste dai commi 3 dell'art. 111 *bis* c.p.p.**, il deposito di "*atti, documenti, richieste e memorie*" provenienti dai "***soggetti abilitati esterni***", tra i quali rientrano anche i "***difensori delle parti private***"[5], ha luogo "***esclusivamente con modalità telematiche, ai sensi dell'articolo 111 bis del codice di procedura penale***", dunque al portale, purchè destinato ai seguenti Uffici:
– Procura della Repubblica presso il Tribunale ordinario (compresa la Procura europea);
– Tribunale ordinario (compreso il G.I.P. e il G.U.P.);
– Procura generale presso la Corte di Appello, limitatamente al procedimento di avocazione.
La norma è di chiara interpretazione. La novità a cui bisogna prestare però particolare attenzione rispetto al passato è che tra gli atti di maggior interesse che devono adesso essere obbligatoriamente depositati al portale rientrano certamente, oltre alla **lista testi ex art. 468 c.p.p.**, anche **tutte le impugnazioni** – appello, ricorso per Cassazione, opposizione al D.P., reclamo – avverso i provvedimenti emessi dal Giudice di primo grado (Tribunale, anche in funzione di Giudice d'Appello, G.I.P., G.U.P.). L'art. 582 c.p.p., comma 1[6], prevede infatti che l'atto di impugnazione è presentato mediante deposito con le modalità previste dall'art. 111 *bis* c.p.p. nella "**cancelleria del Giudice che ha emesso il provvedimento impugnato"**[7].
La norma non contiene più una previsione espressa in ordine al deposito obbligatorio al portale della nomina del difensore e della rinuncia o revoca del mandato, prima prevista dall'art. 3 del D.M. 217 del 2023, in qualsiasi fase processuale, se tali atti erano destinati ai seguenti Uffici giudiziari:
– Corte di appello;
– Tribunale ordinario (compreso G.I.P. e G.U.P);
– Giudice di pace;
– Procura generale presso la Corte di Appello;

[5] Ai sensi dell'art. 2 del Regolamento n. 44 del 2011, lett. m, n. 3, sono da considerare "***soggetti abilitati esterni***" anche i "***difensori delle parti private***".
[6] Ai sensi dell'art. 87, comma 4 del D. Lgs. 150 del 2022, l'art. 582 comma 1 c.p.p. deve ritenersi certamente entrato in vigore nella nuova formulazione introdotta dalla Riforma Cartabia, per tutte le impugnazioni proposte avverso i provvedimenti emessi dal Giudice di primo grado (Tribunale, G.I.P., G.U.P.). Rispetto a tale Ufficio, infatti, è **definitivamente cessato in data 30.12.2024 il regime di transizione previsto dal D.M. 217 del 2023**.
[7] Si segnala che l'art. 461 c.p.p., in tema di opposizione a decreto penale di condanna, continua a prevedere la possibilità della impugnazione fuori sede: "*Nel termine di quindici giorni dalla notificazione del decreto, l'imputato e la persona civilmente obbligata per la pena pecuniaria, personalmente o a mezzo del difensore eventualmente nominato, possono proporre opposizione con le forme previste dall'articolo 582 nella cancelleria del giudice per le indagini preliminari che ha emesso il decreto* ***ovvero nella cancelleria del tribunale o del giudice di pace del luogo in cui si trova l'opponente***".

– Procura della Repubblica presso il Tribunale;

– Procura europea.

Secondo la regola generale introdotta dall'art. 1 del D.M. 206 del 2024, deve oggi ritenersi che il deposito della nomina del difensore, della rinuncia o revoca del mandato rimanga obbligatorio al portale solo se diretto a:

– Procura della Repubblica presso il Tribunale ordinario, compresa la Procura europea;

– Tribunale ordinario, compreso il G.I.P. e il G.U.P.;

– Procura generale presso la Corte di Appello, limitatamente al procedimento di avocazione.

Analoga ipotesi di deposito telematico obbligatorio sembra oggi prevista dall'art. 122 comma 2 *bis*, norma entrata in vigore in forza della disciplina transitoria di cui all'art. 87 del D. Lgs. 150 del 2022, sopra richiamata, a mente del quale "*la procura speciale è depositata,* ***in copia informatica autenticata con firma digitale o altra firma elettronica qualificata***[8]*, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici, con le modalità previste dall'articolo 111 bis, salvo l'obbligo di conservare l'originale analogico da esibire a richiesta dell'autorità giudiziaria*».

4.3 Eccezioni alla regola generale di deposito obbligatorio al portale

Prima eccezione. L'art. 1, comma 3, del D.M. 206 del 2024, prevede una prima eccezione – **sino al 31.12.2025** – al deposito obbligatorio al portale previsto nel paragrafo precedente, laddove gli atti, documenti, richieste e memorie siano **depositati al Tribunale**, **compreso il G.I.P. e il G.U.P.**, e riguardino:

– i "***procedimenti regolati dal libro IV del codice di procedura penale***" in materia di misure cautelari personali e reali. Rientrano in questa eccezione, dunque, le richieste ex art. 299 c.p.p. e, più in generale, le impugnazioni in materia cautelare;

– i "***procedimenti relativi alle impugnazioni in materia di sequestro probatorio***"[9].

In entrambi i casi, il deposito potrà avvenire in alternativa attraverso il portale o con "*modalità non telematiche*", cioè in cartaceo o mediante la PEC, secondo la disciplina di cui all'art. 87 *bis* del D. Lgs. 150 del 2022, così come espressamente previsto dal comma 9 dell'art. 1 del D.M. 206 del 2024.

[8] La lettera della norma sembra consentire l'autenticazione della firma dell'assistito, non soltanto apponendo graficamente la propria firma, ma anche applicando quella digitale. Sul punto, si segnala ad esempio Cassazione penale, Sezione VI, 26 settembre 2024, n. 42391, che ha ritenuto perfettamente valida l'autentica tramite "*firma digitale del difensore di fiducia apposta sotto la firma*" dell'assistito.

[9] La previsione di una norma *ad hoc* deriva dalla collocazione sistematica – Libro III – delle disposizioni in materia di sequestro.

Attenzione: questa eccezione riguarda solo gli atti destinati al Tribunale (compreso il G.I.P. e il G.U.P), ma **non anche quelli depositati in Procura, per i quali il portale deve intendersi sempre obbligatorio**.

Seconda eccezione. Il comma 4 dell'art. 1 del D.M. 206 del 2024 prevede una seconda eccezione – questa volta **sino al 31.3.2025** – al deposito obbligatorio al portale previsto nel paragrafo precedente, laddove gli atti, documenti, richieste e memorie siano relativi "*al procedimento*" di cui al libro VI, titoli I (**giudizio abbreviato**), III (**giudizio direttissimo**) e IV (**giudizio immediato**).
In questi casi, il deposito potrà avvenire sempre attraverso il portale o con "*modalità non telematiche*", cioè in cartaceo, o mediante la PEC, secondo la disciplina di cui all'art. 87 *bis* del D. Lgs. 150 del 2022, così come espressamente previsto dal comma 9 dell'art. 1 del D.M. 206 del 2024.
Si segnalano, tuttavia, due problemi interpretativi.
Il primo: a differenza del comma 3, il comma 4 dell'art. 1 del D.M. 206 del 2024 non specifica se l'eccezione riguardi solo gli atti destinati al Tribunale/G.I.P./G.U.P., come forse potrebbe lasciare intendere l'espressione "*fermo quanto previsto dal comma 3*", o anche quelli destinati alla Procura. Nel dubbio, in quest'ultimo caso, tenuto anche della scarsa finestra temporale di validità dell'eccezione, si suggerisce il deposito al portale e non con modalità alternative.
Il secondo: non è chiaro se tra gli "atti del procedimento" relativi ai predetti riti alternativi possano rientrare anche quelli di impugnazione, i quali invece, secondo la regola generale indicata nel paragrafo precedente, devono essere sempre depositati obbligatoriamente al portale. Si pensi, ad esempio, all'impugnazione avverso una sentenza emessa all'esito di giudizio abbreviato. Anche in questo caso, appare sempre più prudente il deposito al portale e non con modalità alternative.

4.4. Ulteriori ipotesi di deposito telematico (portale) non obbligatorio

Il comma 5 dell'art. 1 del D.M. 206 del 2024 individua **l'1.1.2027** quale data a partire dalla quale diventerà obbligatorio e quindi esclusivo il deposito al portale degli atti destinati ai seguenti uffici:
– Ufficio del Giudice di Pace;
– Corte d'Appello;
– Procura generale presso la Corte d'Appello.
– Procura presso il Tribunale per i Minorenni;
– Tribunale per i Minorenni;
– Tribunale di sorveglianza/Magistrato di sorveglianza;
– Corte di Cassazione;

– Procura Generale presso la Corte di Cassazione;

L'unica certezza sul piano interpretativo è che, **fino all'31.12.2026**, **tutti gli atti destinati a questi uffici potranno essere depositati con modalità cartacea o a mezzo PEC**.

La lettura congiunta dei commi 5, 6 e 7 pone invece una questione interpretativa in ordine alla possibilità di ricorrere nei medesimi casi anche all'uso del portale.

Ai sensi del comma 7, infatti, negli uffici menzionati al comma 5[10], tra i quali il D.M. 206 del 2024 menziona testualmente anche il "**Giudice di Pace, la Corte d'Appello e la Procura generale presso la Corte d'Appello"**, il deposito al portale è consentito a **condizione** che venga emanato e pubblicato un **provvedimento del D.G.S.I.A. che attesti la funzionalità dei sistemi informatici**.

Ad oggi, per nessuno di questi uffici tale provvedimento è stato emanato e dunque l'uso del portale **sembra espressamente precluso** anche per il deposito destinato al Giudice di Pace, alla Corte d'Appello e alla Procura generale presso la Corte d'Appello.

Alcuni commentatori superano il dato testuale del comma 7, privilegiando esclusivamente il contenuto del comma 6, il quale invece, a onor del vero in continuità con quanto previsto già dal D.M. 217 del 2023 e con la struttura della piattaforma stessa che di fatto individua tali uffici tra i "destinatari", consente il deposito al portale degli atti, documenti, richieste e memorie destinate a:

– Ufficio del Giudice di Pace;

– Corte d'Appello;

– Procura generale presso la Corte d'Appello.

Si invita a prestare particolare attenzione a tale questione, affatto teorica, atteso che, su tutti, espone a un rischio di inammissibilità in caso di deposito al portale dei ricorsi per Cassazione avverso i provvedimenti emessi dalla Corte d'Appello e, più in generale, delle impugnazioni avverso le sentenze emesse dai Giudici di pace.

In attesa di un intervento chiarificatore, in questi casi, si suggerisce pertanto in via prudenziale l'uso della modalità cartacea o della PEC.

[10] E cioè:
– Ufficio del Giudice di Pace;
– Corte d'Appello;
– Procura generale presso la Corte d'Appello.
– Procura presso il Tribunale per i Minorenni;
– Tribunale per i Minorenni;
– Tribunale di sorveglianza/Magistrato di sorveglianza;
– Corte di Cassazione;
– Procura Generale presso la Corte di Cassazione.

4.5. Ipotesi in cui è certamente precluso il deposito al portale

Sino al 31.12.2026, l'uso del portale è certamente **precluso** in caso di deposito relativo:
– ai "*procedimenti in materia di misure di prevenzione*";
– alle fasi disciplinate dai libri X (esecuzione) e XI (rapporti con le autorità straniere) del codice di procedura penale.
Ciò significa che **per tutti gli atti relativi a tali procedimenti e fasi il deposito potrà avvenire soltanto con modalità cartacea o a mezzo PEC**.

5. Ulteriori problemi e questioni

5.1 Il deposito in udienza

Deve sempre ritenersi consentito il deposito **in udienza** di un atto che rientra tra quelli per i quali in astratto sia previsto l'uso obbligatorio del portale: si pensi, ad esempio, alla nomina del difensore, alla costituzione di parte civile, alla comparsa conclusionale.
L'ipotesi rientra infatti nella previsione di cui al comma 3 dell'art. 111 *bis* c.p.p., trattandosi di atti che per la loro "*natura o per specifiche esigenze processuali*" non possono essere acquisiti in copia informatica.

5.2. Le specifiche tecniche degli atti

L'art. 13 *bis* del Regolamento n. 44 del 2011 prevede che il deposito telematico avvenga secondo le specifiche tecniche indicate dall'art. 34 dello stesso Regolamento. Tali specifiche tecniche sono state adottate e sono entrate in vigore il 30.9.2024 (allegato *sub* 3).
Si ricorda che, in forza dell'art. 15, "*l'atto del procedimento penale in forma di documento informatico, da depositare telematicamente nell'ufficio giudiziario*" dovrà 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.
Ai sensi dell'art. 16, gli "*allegati*" 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.

Gli allegati sono sottoscritti con firma digitale o firma elettronica qualificata **soltanto nei casi previsti dalla legge.** La disposizione riproduce quella già prevista dal provvedimento del D.G.S.I.A. dell'11.7.2023 e in particolare il principio per cui, **in assenza di previsioni normative espresse, da ritenersi pertanto tassative, i documenti allegati al portale non dovranno essere firmati digitalmente.**

Il comma 3 prevede poi che "*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***".

5.3 Il perfezionamento del deposito

L'art. 172 c.p.p., comma 6 *bis*, prevede che "*il termine per depositare documenti in un ufficio giudiziario **con modalità telematiche** si considera rispettato se **l'accettazione da parte del sistema informatico** avviene **entro le ore 24 dell'ultimo giorno utile**".*

Ai sensi dell'art. 13 *bis* del regolamento n. 44 del 2011, gli atti e i documenti "*si intendono ricevuti dal dominio giustizia nel momento in cui viene **generata la ricevuta di accettazione** da parte del portale dei depositi telematici, che **attesta il deposito** dell'atto o del documento presso l'ufficio giudiziario competente, **senza l'intervento degli operatori della cancelleria o della segreteria**, salvo il caso di anomalie bloccanti*".

Ai sensi dell'art. 19 del regolamento sulle specifiche tecniche entrato in vigore il 30.9.2024, sopra citato e allegato *sub* 3, 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.

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

È dunque la ricevuta generata a seguito del mero invio che consente di ritenere perfezionato il deposito agli effetti di legge e ciò indipendentemente dagli eventi successivi.

Prosegue poi il comma 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*.

[…] 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;

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".

Per un approfondimento del tema, si allegano *sub* 4 la circolare esplicativa a firma del D.G.S.I.A. e i successivi chiarimenti del 12.11.2024.

5.4 L'atto abilitante

Ai sensi dell'art. 2, lettera c), del regolamento sulle specifiche tecniche entrato in vigore il 30.9.2024, si definisce atto abilitante quello "*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*".
Si ricorda che **non è necessario allegare l'atto abilitante** al deposito della dichiarazione di nomina, se non nei casi previsti. L'art. 19, comma 4, dello stesso regolamento prevede infatti sul punto che: "*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***".
L'atto abilitante non è dunque necessario quando il procedimento si trovi in una fase successiva all'emissione degli avvisi di cui agli articoli 408, 411 o 415 *bis* codice di procedura penale. Ogni prassi diversa e, soprattutto, il rigetto del deposito di una dichiarazione di nomina in assenza di atto abilitante, quando questo non è dovuto, è **illegittimo**.

5.5. L'autorizzazione del procedimento

È frequente il caso dei procedimenti che non "compaiono" tra quelli autorizzati e ciò nonostante la propria nomina risulti certamente in atti o, addirittura, sia indicata all'interno di atti notificati al difensore.
Anche in questi casi, è necessario ottenere l'autorizzazione:
a) utilizzando la procedura di "sollecito" all'interno del portale;
b) depositando nuovamente la nomina o comunque un qualsiasi atto da cui questa risulti (es. verbale di identificazione, avviso ex art. 415 *bis* c.p.p., decreto di citazione, sentenza etc.).
Capita altrettanto di frequente che, nonostante il procedimento risulti autorizzato, il sistema non consenta il deposito di alcuni **atti successivi**, i quali non appaiono tra quelli in elenco. Il caso tipico è quello della lista testimoniale, nonostante il procedimento sia autorizzato già in fase di indagini. In questo caso, l'unica possibilità per ovviare al problema è quella di depositare nuovamente la nomina – nel caso di specie in Tribunale, indicando il numero di N.R. – e scegliere tra gli atti contestuali quello di interesse (nel caso di specie, comparirà la lista testi).

5.6. La denuncia e la querela depositate dall'avvocato

Nell'ipotesi in cui la denuncia e la querela siano depositati in Procura, l'uso del portale è oggi inequivocabilmente obbligatorio, ciò **sia nell'ipotesi in cui il difensore sia nominato procuratore speciale, ex art. 122 e 336 c.p.p., sia nel caso in cui sia meramente incaricato al deposito ex art. 337 c.p.p.**: l'art. 1 del D.M. 206 del 2024 parla infatti di **deposito "da parte" dei difensori**, senza distinguere l'ipotesi in cui l'atto sia compiuto personalmente dall'avvocato da quella in cui egli sia un mero delegato dell'assistito.
Il difensore potrà invece sempre depositare l'atto in formato cartaceo, secondo la regola generale di cui agli art. 333 e 336 c.p.p., a qualsiasi Ufficiale di Polizia Giudiziaria. Gli artt. 111 *bis* c.p.p. e 1 del D.M. 206 del 2024 disciplinano infatti soltanto il deposito telematico del difensore diretto all'Ufficio della Procura della Repubblica.

5.7 Il deposito da parte dei privati

Alla luce della recente modifica dell'art. 111 *bis* comma 4, le parti e la persona offesa possono depositare gli atti che compiono personalmente anche con modalità non telematiche.
In particolare, la denuncia e la querela possono essere depositate con modalità cartacea **sia all'ufficiale di Polizia Giudiziaria, sia presso l'ufficio ricezione atti della Procura.**
Analogamente, possono essere depositate personalmente le memorie, l'opposizione alla richiesta di archiviazione e l'atto di impugnazione.

5.8 Il regime delle impugnazioni

Riassumendo quanto già detto più sopra, il regime di deposito delle impugnazioni è il seguente:
– tutte le impugnazioni (appello, ricorso per Cassazione, opposizione al D.P., reclamo, etc.) avverso i provvedimenti emessi dal Tribunale/G.I.P./G.U.P., comprese le sentenze emesse dal Tribunale in funzione di Giudice di Appello (**deposito obbligatorio al portale, esclusa la modalità cartacea e la PEC**. Fino al 31.3.2025, **anche la PEC e il cartaceo**, limitatamente alle censure avverso i provvedimenti emessi in sede di rito abbreviato, direttissimo e immediato, **se si ritiene che tra gli "atti del procedimento" rientri anche l'impugnazione**);
– impugnazioni in materia cautelare (**portale, cartaceo e PEC, fino al 31.12.2025**);

– impugnazioni avverso i provvedimenti emessi dal Giudice di Pace e dalla Corte d'Appello (**deposito cartaceo e PEC fino al 31.12.2026** Il portale è **consentito** solo aderendo a una interpretazione restrittiva del comma 7 dell'art. 1 del D.M. 206 del 2024);
– impugnazioni avverso i provvedimenti emessi dal Tribunale per i Minorenni e dal Tribunale di sorveglianza/Magistrato di sorveglianza (**deposito cartaceo e PEC fino al 31.12.2026**).
Si segnala infine, invitando i difensori a far rispettare la decisione, che, con parere reso in data 12.11.24, il Ministero ha chiarito che, in caso di impugnazione, le copie o i relativi diritti sono:
– dovuti, se è proposta con modalità cartacea o a mezzo PEC;
– **non dovuti, se è depositata attraverso il portale**.

5.9 Il malfunzionamento del portale

L'art. 175 *bis* c.p.p. distingue:
a) il malfunzionamento certificato dal D.G.S.I.A.;
b) il malfunzionamento attestato dal Dirigente dell'ufficio giudiziario.
In entrambi i casi, "*a decorrere dall'inizio e sino alla fine del malfunzionamento dei sistemi informatici, atti e documenti* ***sono redatti in forma di documento analogico e depositati con modalità non telematiche***".
Applicando estensivamente il comma 9 dell'art. 1 del D.M. 206 del 2024 anche al caso di malfunzionamento del portale, il deposito potrà quindi avvenire con modalità cartacea o a mezzo PEC.
L'art. 175 *bis* c.p.p. **non è invece certamente applicabile nel caso di malfunzionamento non attestato e comunicato per tempo dal D.G.S.I.A. o dal Dirigente dell'ufficio**. Ciò si segnala, al fine di rappresentare i rischi di iniziative personali dei difensori, i quali procedessero al deposito con modalità alternative al portale, laddove ovviamente quest'ultimo sia obbligatorio, allegando la prova del malfunzionamento (es. screenshot dello schermo).
Tali iniziative, quandanche avallate oralmente dai funzionari di cancelleria, sono sprovviste di copertura normativa, salvo a ritenere in questo applicabile il comma 3 dell'art. 111 *bis* c.p.p. e dunque ricorrenti "*specifiche esigenze processuali*".
In alternativa, potrebbe invece invocarsi il comma 6 *quater* dell'articolo 87, norma **mai abrogata** e la cui vigenza sopravvive certamente al D.M. 217 del 2023, prima, e al D.M. 206 del 2024, poi, non essendo testualmente ancorata alla pubblicazione di alcun regolamento.
L'ultimo periodo della norma legittima infatti l'Autorità giudiziaria ad "autorizzare" il deposito dell'atto in formato cartaceo, se ricorrono "**ragioni specifiche**": tra queste, potrebbe includersi anche

il malfunzionamento non certificato. La disposizione sembra quindi attribuire ampi margini ai Dirigenti degli Uffici giudiziari, affinchè adottino provvedimenti, anche di carattere generale e preventivo, che autorizzino il deposito cartaceo, e di conseguenza a mezzo PEC, anche nel caso di malfunzionamento improvviso del portale, dunque non attestato e comunicato preventivamente ai sensi dell'art. 175 *bis* c.p.p.

5.10 Il deposito a mezzo PEC

Nei casi in cui è consentito il deposito a mezzo PEC, l'art. 1 comma 9 del D.M. 206 del 2024 richiama espressamente la disciplina dell'art. 87 *bis* del D. Lgs. 150 del 2022.
Si riporta qui il testo integrale della norma, anche al fine di ricordare le cause espresse di inammissibilità in tema di impugnazioni e, soprattutto, le **deroghe in materia cautelare**:

"[…] è consentito il deposito con valore legale mediante invio dall'indirizzo di posta elettronica certificata inserito nel registro generale degli indirizzi elettronici di cui all'articolo 7 del regolamento di cui al decreto del Ministro della giustizia 21 febbraio 2011, n. 44. Il deposito con le modalità di cui al periodo precedente ***deve essere effettuato presso gli indirizzi di posta elettronica certificata degli uffici giudiziari destinatari, indicati in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati****, pubblicato nel portale dei servizi telematici del Ministero della giustizia. Con il medesimo provvedimento sono indicate le specifiche tecniche relative ai formati degli atti e alla sottoscrizione digitale e le ulteriori modalità di invio. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nel provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al presente comma, il deposito può essere eseguito mediante l'invio di più messaggi di posta elettronica certificata. Il deposito è* ***tempestivo quando è eseguito entro le ore 24 del giorno di scadenza****.*
[…] 3. Quando il deposito di cui al comma 1 ha ad oggetto ***un'impugnazione****, l'atto in forma di documento informatico è sottoscritto digitalmente secondo le modalità indicate con il provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al comma 1 e* ***contiene la specifica indicazione degli allegati, che sono trasmessi in copia informatica per immagine, sottoscritta digitalmente dal difensore per conformità all'originale****.*
4. L'atto di impugnazione è trasmesso tramite posta elettronica certificata dall'indirizzo di posta elettronica certificata del difensore a quello dell'ufficio che ha emesso il provvedimento impugnato, individuato ai sensi del comma 1, con le modalità e nel rispetto delle specifiche tecniche ivi indicate.

*5. I **motivi nuovi e le memorie sono proposti**, nei termini rispettivamente previsti, secondo le modalità indicate nei commi 3 e 4, con atto in formato elettronico trasmesso tramite posta elettronica certificata dall'indirizzo di posta elettronica certificata del difensore a quello dell'ufficio del giudice dell'impugnazione, individuato ai sensi del comma 1.*

*6. Le disposizioni di cui ai commi 3, 4 e 5 si applicano a tutti gli atti di impugnazione comunque denominati e, in quanto compatibili, alle opposizioni di cui agli articoli 461 e 667, comma 4, del codice di procedura penale e ai reclami giurisdizionali previsti dalla legge 26 luglio 1975, n. 354. Nel caso di **richiesta di riesame o di appello** contro ordinanze in materia di misure cautelari, personali o reali, l'atto di impugnazione, in deroga a quanto disposto dal comma 3, **è trasmesso all'indirizzo di posta elettronica certificata del tribunale di cui all'articolo 309, comma 7, del codice di procedura penale.***

7. Fermo restando quanto previsto dall'articolo 591 del codice di procedura penale, nel caso di proposizione dell'atto ai sensi del comma 3 del presente articolo l'impugnazione è altresì inammissibile:

a) quando l'atto di impugnazione non è sottoscritto digitalmente dal difensore;

b) quando l'atto è trasmesso da un indirizzo di posta elettronica certificata che non è presente nel registro generale degli indirizzi elettronici di cui al comma 1;

c) quando l'atto è trasmesso a un indirizzo di posta elettronica certificata non riferibile, secondo quanto indicato dal provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al comma 1, all'ufficio che ha emesso il provvedimento impugnato o, nel caso di richiesta di riesame o di appello contro provvedimenti resi in materia di misure cautelari, personali o reali, a un indirizzo di posta elettronica certificata non riferibile, secondo quanto indicato dal provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al comma 1, all'ufficio competente a decidere il riesame o l'appello.

8. Nei casi previsti dal comma 7, il giudice che ha emesso il provvedimento impugnato dichiara, anche d'ufficio, con ordinanza l'inammissibilità dell'impugnazione e dispone l'esecuzione del provvedimento impugnato».

Si invitano poi i difensori a fare particolare attenzione alla esatta individuazione dell'indirizzo di destinazione dell'atto di impugnazione e, in particolare, alla **ripartizione adottata all'interno dei singoli uffici delle caselle *depositoattipenali* assegnate dal D.G.S.I.A**. A tal proposito, si segnala infatti una recente sentenza della Cassazione[11] che, ponendosi in realtà in contrasto con altre pronunce di segno contrario, ha ritenuto inammissibile il ricorso in Cassazione depositato dal difensore, poiché

[11] Cassazione penale, I Sezione, 29 novembre 2024, n. 3848.

inviato all'indirizzo "*depositoattipenali*" assegnato alla Sezione della Corte di Appello che aveva emesso la decisione impugnata, anziché al diverso indirizzo assegnato dal Dirigente all'ufficio impugnazioni.

5.11 I diritti di copia

Con la legge di bilancio 2025, è stato introdotto l'art. 269 *bis* del D.P.R. 115/2002, rubricato "*Diritto per la trasmissione con modalità telematica di duplicati e copie informatiche nel procedimento penale*" e sostituito l'allegato 8. La norma prevede ora che per la trasmissione da parte della segreteria o della cancelleria del "*duplicato o della copia informatica di atti e documenti del procedimento penale*", è dovuto un "**diritto forfettizzato**" nella misura di:

– **€ 25,00, per "ogni" riversamento degli atti su un supporto dati** (chiavette USB, CD, DVD);

– **€ 8,00 per "ogni" trasmissione degli atti con modalità telematica** (posta elettronica, posta elettronica certificata o portali).

La norma appare applicabile, e soprattutto conveniente, solo a fronte della necessità di estrarre un quantitativo di copie il cui costo con la modalità cartacea sarebbe superiore a quello forfettizzato. Negli altri casi, rimane in ogni caso salva la possibilità di rilascio di copia cartacea secondo il tradizionale sistema di calcolo dei diritti da corrispondere.

Avv. Mattia Serpotta
Foro di Catania

SCHEMA RIEPILOGATIVO DELLE MODALITA' DI DEPOSITO DEGLI ATTI PENALI DOPO IL D.M. 27.12.2024 N. 206

a cura dell'Avv. Mattia Serpotta

componente della Commissione informatica del Consiglio dell'Ordine degli Avvocati di Catania

ATTI E UFFICI DI DESTINAZIONE	**MODALITA' DI DEPOSITO**	**NOTE**
1. Tutti gli atti, documenti, richieste e memorie destinati a: – **Procura** della Repubblica presso il Tribunale ordinario (compresa la Procura europea); – **Tribunale** ordinario (compreso il **G.I.P.** e il **G.U.P.**); – Procura generale presso la Corte di Appello, **limitatamente al procedimento di avocazione**.	a partire dall'**1.1.2025,** portale **obbligatorio ed esclusivo** **non ammessa** la modalità cartacea e la PEC, fatte **salve** le due **eccezioni** seguenti	Sono quindi compresi: – tutte le **impugnazioni** (appello, ricorso per Cassazione, reclamo, opposizione a D.P.) avverso i provvedimenti emessi dal Tribunale/G.I.P./G.U.P., – la **dichiarazione di nomina** del difensore, la rinuncia o revoca del mandato; – la **procura speciale**, ex art. 122, comma 2 *bis*; – la **denuncia – querela;** – l'**opposizione alla richiesta di archiviazione;**
PRIMA ECCEZIONE Tutti gli atti, documenti, richieste e memorie destinati a: – **Tribunale/G.I.P./G.U.P.** e relativi a: – procedimenti regolati dal libro IV del codice di procedura penale (**misure cautelari**); – procedimenti relativi alle **impugnazioni in materia di sequestro probatorio**;	a partire dall'1.1.2025, ma **fino al 31.12.2025** deposito **alternativo portale, modalità cartacea e PEC**	Questa eccezione riguarda solo gli atti destinati al Tribunale/G.I.P./G.U.P., ma non anche quelli depositati in Procura, per i quali il portale **deve intendersi sempre obbligatorio, secondo la regola generale di cui sopra.**
SECONDA ECCEZIONE Tutti gli atti, documenti, richieste e memorie destinati a: – **Procura**; – **Tribunale/G.I.P./G.U.P.** e relativi a: – giudizio **abbreviato**; – giudizio **direttissimo**; – giudizio **immediato**.	a partire dall'1.1.2025, ma **fino al 31.3.2025** deposito **alternativo portale, modalità cartacea e PEC**	**Due dubbi interpretativi:** a) se rientrano nell'eccezione anche gli atti destinati alla Procura; b) se rientrano nell'eccezione anche gli atti di impugnazione. Nel dubbio, si suggerisce in entrambi i casi solo l'uso del portale.

ATTI E UFFICI DI DESTINAZIONE	MODALITA' DI DEPOSITO	NOTE
Tutti gli atti, documenti, richieste e memorie destinati a – Ufficio del Giudice di Pace; – Corte d'Appello; – Procura generale presso la Corte d'Appello; – Procura presso il Tribunale per i Minorenni; – Tribunale per i Minorenni; – Tribunale di sorveglianza – Magistrato di sorveglianza; – Corte di Cassazione; – Procura Generale presso la Corte di Cassazione.	A partire dall'1.1.2025 e **fino al 31.12.2026** **deposito alternativo modalità cartacea e PEC** **deposito al portale** solo se interverrà il provvedimento del D.G.S.I.A. che ne attesti la funzionalità, ai sensi del comma 7 dell'art. 1 del D.M. 204 del 2024.	Secondo alcuni commentatori, il comma 6 dell'art. 1 del D.M. 206 del 2024 legittimerebbe il deposito al portale, **anche in assenza del provvedimento del D.G.S.I.A. di cui al comma 7**, degli atti destinati a: – Ufficio del Giudice di Pace; – Corte d'Appello; – Procura generale presso la Corte d'Appello. Nell'incertezza, specie in caso di impugnazioni dei provvedimenti del Giudice di Pace e della Corte d'Appello, si suggerisce il deposito in forma cartacea o a mezzo PEC.
Tutti gli atti, documenti, richieste e memorie relativi a: – procedimenti in materia di **misure di prevenzione**; – fasi disciplinate dai libri X (**esecuzione**) e XI (**rapporti con le autorità straniere**) del codice di procedura penale. **RIEPILOGO IMPUGNAZIONI**	A partire dall'1.1.2025 e **fino al 31.12.2026** **deposito alternativo modalità cartacea e PEC. Escluso il portale.**	
– tutte le impugnazioni (appello, ricorso per Cassazione, opposizione a D.P., reclamo) avverso i provvedimenti emessi da Tribunale, G.I.P., G.U.P.;	deposito obbligatorio al **portale** (escluso cartaceo e PEC)	fino al 31.3.2025, in sede di rito abbreviato, direttissimo e immediato, **anche la PEC e il cartaceo**, **se si ritiene che tra gli atti del procedimento rientri anche l'impugnazione**
– impugnazioni in materia cautelare;	fino al 31.12.2025 **portale, cartaceo e PEC**	
– impugnazioni avverso i provvedimenti emessi dal Giudice di Pace e dalla Corte d'Appello; – impugnazioni avverso i provvedimenti emessi da a) Tribunale per i Minorenni b) Tribunale di sorveglianza c) Magistrato di sorveglianza	fino al 31.12.2026 **deposito cartaceo e PEC**	allo stato, **portale consentito anche per i provvedimenti emessi dal G.D.P. e dalla Corte d'Appello**, solo aderendo a una interpretazione restrittiva del comma 7 dell'art. 1 del D.M. 206 del 2024

	INDICE	

MINISTERO DELLA GIUSTIZIA

DECRETO 27 dicembre 2024, n. 206

Regolamento concernente modifiche al decreto 29 dicembre 2023, n. 217 in materia di processo penale telematico. (24G00226)

(GU n.304 del 30-12-2024)

Vigente al: 30-12-2024

IL MINISTRO DELLA GIUSTIZIA

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

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 nonche' 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, nonche' in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari»;

Visti il regio decreto 19 ottobre 1930, n. 1398, recante approvazione del testo definitivo del codice penale e il decreto del Presidente della Repubblica 22 settembre 1988, n. 447, recante approvazione del codice di procedura penale;

Visto il decreto legislativo 28 luglio 1989, n. 271, recante norme di attuazione, di coordinamento e transitorie del codice di procedura penale;

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 16 gennaio 2003, n. 3»;

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 ministeriale 27 aprile 2009 recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati

dell'amministrazione della giustizia»;

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

Visto l'articolo 87, commi 1 e 3 del decreto legislativo 10 ottobre 2022, n. 150;

Visto il regolamento 29 dicembre 2023, n. 217 recante: «Decreto ai sensi dell'articolo 87, commi 1 e 3 del decreto legislativo 10 ottobre 2022, n. 150 e dell'articolo 4, comma 1 del decreto-legge 29 dicembre 2009, n. 193, convertito con modificazioni dalla legge 22 febbraio 2010, n. 24, recante modifiche al decreto del Ministro della giustizia di concerto con il Ministro per la pubblica amministrazione e l'innovazione 21 febbraio 2011, n. 44» che, all'articolo 3, detta le disposizioni in materia di individuazione degli uffici giudiziari penali e delle tipologie di atti del procedimento penale per cui possono essere adottate anche modalita' non telematiche di deposito nonche' i termini di transizione al nuovo regime, consentendo il deposito di atti, documenti, richieste e memorie anche con modalita' non telematiche durante la fase delle indagini preliminari sino alla data del 31 dicembre 2024, ferme le eccezioni individuate dal medesimo articolo 3, commi 7 e 8, e indicando i successivi tempi di transizione al nuovo regime per gli uffici giudiziari e le fasi del procedimento diversi da quelli indicati dal comma 1 del medesimo articolo 3;

Rilevata la necessita' di ridefinire tanto l'individuazione degli uffici giudiziari e delle tipologie di atti per cui possono essere adottate anche modalita' non telematiche di deposito, comunicazione o notificazione, quanto i termini di transizione al nuovo regime di deposito, comunicazione e notificazione degli atti del procedimento penale mediante la rimodulazione dei termini medesimi che, nel testo vigente, inizierebbero ad operare sin dal primo gennaio 2025;

Visti gli articoli 10 delle preleggi in tema di deroga alla vacatio legis ordinaria dei regolamenti e 87, commi da 4 a 6-bis, del decreto legislativo 10 ottobre 2022, n. 150 che attribuisce al regolamento di cui al comma 3 del medesimo articolo il potere della individuazione dei termini di transizione al nuovo regime anche in deroga al termine del quindicesimo giorno successivo alla pubblicazione del regolamento medesimo;

Sentiti il Consiglio superiore della magistratura, che si e' espresso nella seduta dell'11 dicembre 2024, e il Consiglio nazionale forense, in data 22 novembre 2024;

Udito il parere del Consiglio di Stato espresso dalla Sezione Consultiva per gli Atti Normativi nell'adunanza del 23 dicembre 2024;

Vista la comunicazione al Presidente del Consiglio dei Ministri in data 23 dicembre 2024;

Adotta
il seguente regolamento:

Art. 1

Modifiche all'articolo 3
del decreto 29 dicembre 2023, n. 217

1. L'articolo 3 del decreto 29 dicembre 2023, n. 217 e' sostituito dal seguente:

«Art. 3 (Disposizioni in materia di individuazione degli uffici giudiziari penali e delle tipologie di atti del procedimento penale per cui possono essere adottate anche modalita' non telematiche di deposito. Termini di transizione al nuovo regime). - 1. Salvo quanto disposto dai commi 2, 3 e 4, a decorrere dal 1° gennaio 2025, il deposito di atti, documenti, richieste e memorie da parte dei soggetti abilitati interni ed esterni ha luogo esclusivamente con modalita' telematiche, ai sensi dell'articolo 111-bis del codice di procedura penale, nei seguenti uffici giudiziari penali:

a) procura della Repubblica presso il tribunale ordinario;

b) Procura europea;

c) sezione del giudice per le indagini preliminari del tribunale ordinario;

d) tribunale ordinario;

e) procura generale presso la corte di appello, limitatamente al procedimento di avocazione.

2. Sino al 31 dicembre 2025, negli uffici giudiziari penali indicati dal comma 1, lettere a), b) e c), il deposito da parte dei soggetti abilitati interni di atti, documenti, richieste e memorie, diversi da quelli relativi ai procedimenti di cui al libro V, titolo IX, e di cui al libro VI, titoli II, V e V-bis del codice di procedura penale, a quelli di archiviazione di cui agli articoli 408, 409, 410, 411 e 415 del codice di procedura penale, nonche' alla riapertura delle indagini di cui all'articolo 414 del codice di procedura penale, puo' avere luogo anche con modalita' non telematiche.

3. Sino al 31 dicembre 2025, negli uffici giudiziari penali indicati dal comma 1, lettere c) e d), il deposito da parte dei soggetti abilitati interni ed esterni di atti, documenti, richieste e memorie, nei procedimenti regolati dal libro IV del codice di procedura penale e in quelli relativi alle impugnazioni in materia di sequestro probatorio, puo' avere luogo anche con modalita' non telematiche.

4. Fermo quanto previsto dai commi 1, 2 e 3, sino al 31 marzo 2025 puo' avere, altresi', luogo anche con modalita' non telematiche l'iscrizione da parte dei soggetti abilitati interni delle notizie di reato di cui all'articolo 335 del codice di procedura penale nonche' il deposito di atti, documenti, richieste e memorie da parte dei soggetti abilitati interni ed esterni relativi al procedimento di cui al libro VI, titoli I, III e IV del codice di procedura penale.

5. A decorrere dal 1° gennaio 2027, il deposito di atti, documenti, richieste e memorie da parte dei soggetti abilitati interni ed esterni ha luogo esclusivamente con modalita' telematiche, ai sensi dell'articolo 111-bis del codice di procedura penale, anche nei seguenti uffici giudiziari penali:

a) Ufficio del giudice di pace;

b) procura della Repubblica presso il tribunale per i

minorenni;
c) tribunale per i minorenni;
d) tribunale di sorveglianza;
e) corte di appello;
f) procura generale presso la corte di appello;
g) Corte di cassazione;
h) Procura generale presso la Corte di cassazione.

6. Sino al 31 dicembre 2026, negli uffici indicati dal comma 5, lettere a), e) ed f) il deposito da parte dei soggetti abilitati esterni di atti, documenti, richieste e memorie puo' avere luogo anche con modalita' telematiche.

7. Sino alla medesima data di cui al comma 6, negli uffici giudiziari penali indicati dal comma 5 il deposito da parte dei soggetti abilitati interni ed esterni di atti, documenti, richieste e memorie puo' avere luogo anche con modalita' telematiche, previo provvedimento che attesti la funzionalita' dei sistemi informatici adottato dal Capo del Dipartimento dell'innovazione tecnologica della giustizia del Ministero della giustizia e pubblicato sul suo Portale dei servizi telematici.

8. Le disposizioni di cui al comma 5 si applicano anche ai procedimenti in materia di misure di prevenzione ed alle fasi disciplinate dai libri X e XI del codice di procedura penale.

9. Rimane consentito ai difensori il deposito mediante posta elettronica certificata come disciplinato dall'articolo 87-bis del decreto legislativo 10 ottobre 2022, n. 150 per tutti i casi in cui il deposito puo' avere luogo anche con modalita' non telematiche.».

Art. 2

Clausola di invarianza finanziaria

1. Dall'attuazione del presente regolamento non devono derivare nuovi o maggiori oneri per la finanza pubblica. Le amministrazioni interessate provvedono ai relativi adempimenti nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Il presente decreto, munito del sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana ed entra in vigore il giorno della sua pubblicazione. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 27 dicembre 2024

Il Ministro: Nordio

Visto, il Guardasigilli: Nordio

Registrato alla Corte dei conti il 30 dicembre 2024
Ufficio di controllo sugli atti della Presidenza del Consiglio dei ministri, del Ministero della giustizia e del Ministero degli affari esteri e della cooperazione internazionale, n. 3277

DECRETO 21 febbraio 2011 , n. 44

Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24. (11G0087)

Capo I

PRINCIPI GENERALI

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 n. 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:

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: **piattaforma informatica** che fornisce l'accesso **o il collegamento** ai servizi telematici resi disponibili dal dominio giustizia, secondo le regole tecnico operative riportate nel presente decreto;

b-bis) portale dei depositi telematici: piattaforma informatica che consente il deposito di atti e documenti in formato digitale da parte dei soggetti abilitati esterni e degli utenti privati; b-ter): portale delle notizie di reato: piattaforma informatica che consente il deposito di atti e documenti in formato digitale riservata agli ufficiali e agenti di polizia giudiziaria ed a ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato;

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;

e-bis) servizio elettronico di recapito certificato qualificato: il servizio elettronico di recapito certificato qualificato come definito dal Regolamento (UE) n. 910/2014 (eIDAS);

f) identificazione informatica: processo di identificazione dell'utente abilitato interno o esterno per l'accesso ai servizi, alle piattaforme e alle risorse del dominio giustizia, mediante autenticazione

elettronica, in conformità alle disposizioni dettate in materia di identificazione e autenticazione elettronica dal decreto legislativo 7 marzo 2005, n. 82 e dal Regolamento (UE) n. 910/2014 (eIDAS);

g) firma digitale: firma elettronica **qualificata**, di cui al decreto legislativo 7 marzo 2005, n. 82;

g-bis) firma elettronica qualificata: firma elettronica avanzata, creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche, di cui al Regolamento (UE) n. 910/2014 (eIDAS);

h) fascicolo informatico: fascicolo contenente gli atti e i documenti redatti in forma di documento informatico nonché le copie informatiche di atti e documenti redatti in forma di documento analogico, nel rispetto di quanto stabilito dal codice dell'amministrazione digitale e dalla disciplina processuale vigente;

h-bis) applicativo informatico: insieme di programmi messi a disposizione dal Ministero della giustizia ai soggetti abilitati interni;

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**, nonché le persone fisiche che possono stare in giudizio personalmente e quelle che rappresentano un ente privato**;

4) soggetti abilitati esterni pubblici: l'Avvocatura generale dello Stato, le avvocature distrettuali dello Stato, gli avvocati e i procuratori dello Stato, gli altri dipendenti di amministrazioni statali, regionali, metropolitane, provinciali e comunali nonché il personale di polizia giudiziaria ed ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato e delle comunicazioni successive;

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, **sentita l'Agenzia per l'Italia Digitale** 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) 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;

v) Identificativo unico di versamento: codice numerico conforme agli standard stabiliti da pagoPA, che costituisce elemento identificativo delle operazioni che transitano su pagoPA.

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) 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.

2) 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 **mediante i dati contenuti nell'indice di cui all'articolo 6-quater del CAD, ove disponibili, e** 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. 7-bis

Portale dei depositi telematici e delle notizie di reato

1) Il portale dei depositi telematici consente la trasmissione in via telematica da parte dei soggetti abilitati esterni degli atti e dei documenti del procedimento.

2) Il portale delle notizie di reato consente la trasmissione in via telematica da parte del personale di polizia giudiziaria e di ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato di atti e documenti su canale sicuro protetto da un meccanismo di crittografia, in modo da assicurare l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività.

3) L'accesso ai portali di cui ai commi 1 e 2 avviene a norma dell'articolo 64 del codice dell'amministrazione digitale e secondo le specifiche stabilite ai sensi dell'articolo 34. 4. 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.

Art. 8

Sistemi informatici per i soggetti abilitati interni

1) I sistemi informatici del dominio giustizia **consentono ai** 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

Fascicolo informatico

1) Il fascicolo informatico contiene gli atti, i documenti, gli allegati, le ricevute di posta elettronica certificata, le ricevute di pagamento e i dati del procedimento medesimo da chiunque formati, ovvero le copie informatiche dei medesimi atti quando siano stati depositati in forma di documento analogico.

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) Restano fermi gli obblighi di conservazione dei documenti originali unici su supporto cartaceo previsti dal codice dell'amministrazione digitale o di atti e documenti depositati o comunque acquisiti in forma di documento analogico in conformità alla disciplina processuale vigente.

4) Il fascicolo informatico reca l'indicazione:

a) dell'ufficio titolare del procedimento, che cura **la formazione** e la gestione del fascicolo medesimo;

b) dell'oggetto del procedimento **e di ogni altro specifico contenuto previsto dalla normativa**

processuale e regolamentare;

c) dell'elenco dettagliato degli atti e dei documenti depositati o comunque acquisiti, compresi quelli in forma di documento analogico;

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 procedimento in forma di documento informatico.

1) L'atto del procedimento in forma di documento informatico è privo di elementi attivi ed è redatto nei formati previsti dalle specifiche tecniche di cui all'articolo 34, che stabiliscono altresì le informazioni strutturate destinate ad essere inserite nei registri informatici.

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) E' 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 nel procedimento civile

1) Nel procedimento civile, gli atti e i documenti in forma di documento informatico di cui agli articoli 11 e 12 possono essere trasmessi da parte dei soggetti abilitati esterni, con modalità telematiche, secondo le specifiche tecniche stabilite dall'articolo 34.

2) I documenti informatici di cui al comma 1 si intendono ricevuti dal dominio giustizia nel momento in cui viene **generata la conferma della trasmissione, secondo le specifiche tecniche stabilite dall'articolo 34, senza l'intervento degli operatori della cancelleria, salvo il caso di anomalie bloccanti.**

3) Nel caso previsto dal comma 2 **la conferma** attesta l'avvenuto deposito dell'atto o del documento presso l'ufficio giudiziario competente.

4) Nei procedimenti civili di volontaria giurisdizione si osservano le apposite specifiche tecniche previste dall'articolo 36, comma 1, del decreto-legge 24 febbraio 2023, n. 13, convertito con modificazioni dalla legge 21 aprile 2023, n. 41.

5) La certificazione dei soggetti abilitati esterni 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, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

7) 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.

8) I soggetti abilitati esterni possono avvalersi dei servizi del punto di accesso, di cui all'articolo 23, per la trasmissione dei documenti; in tale caso il punto di accesso si attiene alle modalità di trasmissione dei documenti di cui al presente articolo.

Art. 13-bis

Trasmissione dei documenti da parte dei soggetti abilitati esterni nel procedimento penale

1) Nel procedimento penale, gli atti e i documenti in forma di documento informatico di cui agli articoli 11 e 12 sono trasmessi da parte dei soggetti abilitati esterni attraverso la procedura prevista dal portale dei depositi telematici o dal portale delle notizie di reato previa autenticazione del soggetto depositante, secondo le specifiche tecniche previste dall'articolo 34.

2) Gli atti e i documenti di cui al comma 1, si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di accettazione da parte del portale dei depositi telematici, che attesta il deposito dell'atto o del documento presso l'ufficio giudiziario competente, senza l'intervento degli operatori della cancelleria o della segreteria, salvo il caso di anomalie bloccanti.

3) Al fine di garantire la riservatezza degli atti e dei documenti da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

Art. 14

Documenti e allegati in forma di documento analogico

1) I documenti e gli allegati depositati in forma di documento analogico sono identificati e descritti nel fascicolo informatico, 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 e degli allegati di cui al comma 1, e ad inserirla nel fascicolo informatico.

Art. 15

Deposito dell'atto del procedimento da parte dei soggetti abilitati interni

1) L'atto del procedimento, redatto in forma di documento informatico da un soggetto abilitato interno e sottoscritto con firma digitale o altra firma elettronica qualificata, è depositato nel fascicolo tramite l'applicativo l'informatico, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2) Se il provvedimento del magistrato è in forma di documento analogico, la cancelleria o la segreteria 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.

Art. 16

Comunicazioni o notificazioni per via telematica dall'ufficio giudiziario

1) Salvo che non sia diversamente stabilito dalla legge, la comunicazione o la notificazione per via telematica da un soggetto abilitato interno 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 negli altri pubblici elenchi previsti dalle legge, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2) La comunicazione o la notificazione per via telematica tra soggetti abilitati interni avviene in interoperabilità ai sensi del codice dell'amministrazione digitale, secondo le specifiche tecniche stabilite dall'articolo 34.

3) La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare una copia informatica degli atti e dei documenti formati e depositati in forma di documento analogico da comunicare o da notificare nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34, che conserva nel fascicolo informatico.

4) Le ricevute di avvenuta consegna e gli avvisi di mancata consegna sono conservati nel fascicolo informatico.

5) La comunicazione o la notificazione che contiene dati sensibili di cui all'articolo 9 del Regolamento (UE) 2016/679 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.

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

Art. 17

Notificazioni per via telematica tramite UNEP

1) Le richieste di notifica per posta elettronica certificata sono inoltrate dai soggetti abilitati interni ed esterni all'UNEP tramite posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2) Il sistema informatico dell'UNEP individua l'indirizzo di posta elettronica del destinatario dal registro generale degli indirizzi elettronici, ovvero da uno degli altri pubblici elenchi previsti dalla legge.

3) 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.

Art. 18

Notificazioni per via telematica eseguite dagli avvocati

1) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217, COME MODIFICATO DALL'AVVISO DI RETTIFICA IN G.U. 15/01/2024, N. 11.

2) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217, COME MODIFICATO DALL'AVVISO DI RETTIFICA IN G.U. 15/01/2024, N. 11.

3) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217, COME MODIFICATO DALL'AVVISO DI RETTIFICA IN G.U. 15/01/2024, N. 11.

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.

Art. 19

ARTICOLO ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

Art. 20

Requisiti della casella di PEC del soggetto abilitato esterno

1) Il **gestore di posta elettronica certificata del** soggetto abilitato esterno **deve dotarsi di una casella di posta elettronica conforme agli** 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», **o di un recapito certificato ai sensi del Regolamento (UE) n. 910/2014 (eIDAS) che disponga di soluzioni idonee** a prevenire la trasmissione di messaggi indesiderati.

2) Il soggetto abilitato esterno è tenuto a dotare il terminale informatico utilizzato di software idoneo a verificare l'assenza di virus informatici per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.

3) Il soggetto abilitato esterno è tenuto a conservare, con ogni mezzo idoneo, le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia.

4) La casella di posta elettronica certificata deve disporre di uno spazio disco minimo definito nelle specifiche tecniche di cui all'articolo 34.

5) Il soggetto abilitato esterno è tenuto a dotarsi di servizio automatico di avviso dell'imminente saturazione della propria casella di posta elettronica certificata e a verificare la effettiva disponibilità dello spazio disco a disposizione.

6) La modifica dell'indirizzo elettronico può avvenire dall'1 al 31 gennaio e dall'1 al 31 luglio.

7) La disposizione di cui al comma 6 non si applica qualora la modifica dell'indirizzo si renda necessaria per cessazione dell'attività da parte del gestore di posta elettronica certificata.

Art. 21

Estrazione e rilascio di copie di atti e documenti

1) I soggetti abilitati esterni estraggono con modalità telematiche duplicati di atti e documenti dai fascicoli informatici cui possono accedere per legge, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2) Il rilascio di copia di atti e documenti depositati nel fascicolo informatico avviene, previa verifica del regolare pagamento dei diritti, ove previsti, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

3) L'atto o il documento che contiene dati di cui all'articolo 9 del Regolamento (UE) 2016/679 o dati 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.

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:

e) nome, cognome, codice fiscale, indirizzo di posta elettronica certificata, numero di telefono e di fax; 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 puo' 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) Nei casi previsti dalla legge, il dominio giustizia consente al soggetto abilitato esterno l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui **esercita la difesa** o svolge attività di esperto o ausiliario. **Nei casi previsti dalla legge, l'utente** privato accede alle informazioni contenute nei fascicoli dei procedimenti 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) E' 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 **sostituzione del difensore, ai sensi dell'articolo 14 della legge 31 dicembre 2012, n. 147**, 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) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

5) Gli esperti e gli ausiliari del giudice accedono ai servizi di consultazione nel limite dell'incarico ricevuto e della autorizzazione concessa dal giudice.

6) Salvo quanto previsto dal comma 2, gli avvocati e i procuratori dello Stato accedono alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione la cui difesa in giudizio è stata assunta dal soggetto che effettua l'accesso.

Art. 28

Registrazione dei soggetti abilitati esterni e degli utenti privati

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

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

Art. 29

Orario di disponibilità dei servizi di consultazione

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

Capo V

PAGAMENTI TELEMATICI

Art. 30

Pagamenti

1) Il pagamento del contributo unificato e degli altri diritti e spese è effettuato **esclusivamente tramite pagoPA, accedendo al portale dei servizi telematici))**. **((La ricevuta di pagamento può essere acquisita automaticamente dai sistemi oppure trasmessa dall'interessato all'ufficio, secondo le modalità previste dall'articolo 5 del CAD.**

2) I sistemi del dominio giustizia verificano la regolarità delle ricevute di pagamento telematico.

3) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

4) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

5) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

6) COMMA ABROGATO DAL DECRETO 29 DICEMBRE 2023, N. 217

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, **sentita l'Agenzia per l'Italia Digitale** e, limitatamente ai profili inerenti alla protezione dei dati personali, sentito il Garante per la protezione dei dati personali.

2) Le specifiche di cui al comma precedente vengono rese disponibili mediante pubblicazione nell'area pubblica del portale dei servizi telematici.

3) (Fino all'emanazione delle nuove specifiche tecniche, continuano ad applicarsi, in quanto compatibili, le specifiche tecniche vigenti, già adottate dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia.

Art. 35

Disposizioni finali e transitorie

1) L'attivazione della trasmissione dei documenti informatici **da parte dei soggetti abilitati esterni** è preceduta da un decreto dirigenziale che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.

2) L'indirizzo elettronico già previsto dal decreto del Ministro della Giustizia, 17 luglio 2008 recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile» è utilizzabile per un periodo transitorio non superiore a sei mesi dalla data di entrata in vigore del presente decreto.

3) La data di attivazione dell'indirizzo di posta elettronica certificata di cui all'articolo 4, comma 2, è stabilita, per ciascun ufficio giudiziario, con apposito decreto dirigenziale del responsabile per i sistemi informativi automatizzati del Ministero della giustizia che attesta la funzionalità del sistema di posta elettronica certificata del Ministero della giustizia.

4) Le caratteristiche specifiche della strutturazione dei modelli informatici sono definite con decreto del responsabile per i sistemi informativi automatizzati del Ministero della giustizia e pubblicate nell'area pubblica del portale dei servizi telematici.

5) Fino all'emanazione dei provvedimenti di cui al comma 4, conservano efficacia le caratteristiche di strutturazione dei modelli informatici di cui al decreto del Ministro della giustizia 10 luglio 2009, recante "Nuova strutturazione dei modelli informatici relativa all'uso di strumenti informatici e telematici nel processo civile e introduzione dei modelli informatici per l'uso di strumenti informatici e telematici nelle procedure esecutive individuali e concorsuali", pubblicato nella Gazzetta Ufficiale n. 165 del 18 luglio 2009 - s.o. n. 120.

Art. 36

Adeguamento delle regole tecnico-operative

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

Art. 37

Efficacia

1) Il presente decreto acquista efficacia il trentesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana

2) Dalla data di cui al comma 1, cessano di avere efficacia nel processo civile le disposizioni del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e del decreto del Ministro della giustizia 17 luglio 2008.

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

Roma, 21 febbraio 2011

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. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 21 febbraio 2011 Il Ministro della giustizia: Alfano Il Ministro per la pubblica amministrazione e l'innovazione: Brunetta

Visto, il Guardasigilli: Alfano Registrato alla Corte dei conti l'11 aprile 2011

Ministeri istituzionali, registro n. 8, foglio n. 84

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, nonchè 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) CAdES (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.

6. Il Ministero della giustizia conserva il log dei messaggi, pervenuti e transitati attraverso il proprio gestore di posta elettronica certificata, per cinque anni. A tal fine, il gestore di PEC del Ministero invia giornalmente, a una casella di posta di sistema, il log in formato CSV. Il file contenente il log è protetto mediante tecniche crittografiche in grado di garantire la lettura del file al solo Ministero della giustizia. Il log, sottoscritto con firma digitale o firma elettronica qualificata, è relativo a tutti gli indirizzi del sottodominio delle caselle del processo telematico e contiene tutti gli eventi relativi ai messaggi pervenuti e transitati, conservando le seguenti informazioni:

a) il codice identificativo univoco assegnato al messaggio originale;

b) la data e l'ora dell'evento;

c) il mittente del messaggio originale;

d) i destinatari del messaggio originale;

e) l'oggetto del messaggio originale;

f) il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);

g) il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);

h) il gestore mittente.

7. Un apposito modulo nell'ambito del PST comprende i componenti funzionali necessari per l'acquisizione, il salvataggio e l'interrogazione dei log prodotti dal servizio di PEC.

8. I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.

9. Le comunicazioni di atti e documenti tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria nella fase delle indagini preliminari, avvengono anche mediante i gestori di posta elettronica certificata delle forze di polizia; in questo caso il gestore dei servizi telematici utilizza un canale sicuro protetto da un meccanismo di crittografia mediante i protocolli POP3S o HTTPS, al fine di evitare la trasmissione in chiaro delle credenziali di accesso e dei messaggi.

Articolo 5

(Portale dei servizi telematici)

1. Il PST è accessibile all'indirizzo https://pst.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".

2. L'area pubblica, denominata "Servizi online Uffici Giudiziari", è composta da tutte le pagine web e i servizi del portale disponibili ad accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione; in essa sono disponibili le seguenti tipologie d'informazione:

a) Informazioni e documentazione sui servizi telematici del dominio giustizia;

b) Raccolte giurisprudenziali;

c) Informazioni essenziali sullo stato dei procedimenti pendenti, rese disponibili in forma anonima; in questo caso, i parametri e i risultati di ricerca riportano i dati identificativi dei procedimenti limitatamente a: numero di ruolo generale, tipo di registro, ufficio giudiziario procedente, ritualità, oggetto del fascicolo, nome del magistrato, sezione, , data dell'atto introduttivo, data della prossima udienza, numero ed anno del provvedimento, stato del fascicolo, storico del

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'iscriva ad un albo, oppure pervenga copia dell'albo da parte dell'ordine di appartenenza, prevalgono i dati trasmessi dall'ordine stesso; in questo caso il sistema cancella la prima iscrizione e invia un messaggio PEC di cortesia al professionista.

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 omogene (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 abitati 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 omesso 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 RAFE 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 RAFE;
d) il referente dell'ufficio del pubblico ministero, con l'applicativo RAFE, 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 RAFE, 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 RAFE.

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 RAFE.

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 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 reat0.

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 sevizi 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.

Ministero della Giustizia

Dipartimento per l'innovazione tecnologica della giustizia

Direzione generale per i sistemi informativi automatizzati

UII/FA/AP

Alla sig.ra prima Presidente della Corte di Cassazione

Al sig. Procuratore generale presso la Corte di Cassazione

Al sig. Presidente del Tribunale superiore delle acque pubbliche

Ai sigg. Presidenti delle Corti di Appello

Ai sigg. Procuratori generali presso le Corti di Appello

Ai sigg. Presidenti dei Tribunali

Ai sigg. Procuratori della Repubblica Presso i Tribunali

Ai sigg. Presidenti dei Tribunali per i minorenni

Ai sigg. Procuratori della Repubblica presso i Tribunali per i minorenni

Ai sigg. Presidenti coordinatori dei Giudici di Pace

Ai sigg. Commissari per la liquidazione degli usi civici

Ai sigg. Dirigenti delle cancellerie

Ai sigg. Referenti distrettuali per l'innovazione

Ai sigg. Magistrati di riferimento per l'informatica

e p.c.

Al sig. Capo Dipartimento per l'innovazione tecnologica della giustizia

OGGETTO: nota riassuntiva delle modifiche apportate ai sistemi informatici ai fini dell'implementazione dell'accettazione automatica prevista dalle specifiche tecniche adottate ai sensi dell'art. 34 d.m. 21 febbraio 2011, n. 44.

Facendo seguito alla nota del Capo Dipartimento DIT del 6 settembre 2024 (prot. DDSC 0006109.U), con la presente si forniscono opportuni chiarimenti sulle novità in tema di accettazione automatica degli atti processuali, prevista dall'art. 17 delle specifiche tecniche adottate dal Direttore generale DGSIA il 2 agosto 2024.

1. DEGLI ATTI SOGGETTI AD ACCETTAZIONE AUTOMATICA

Le patch che verranno rilasciate a fine settembre '24 implementeranno i flussi per l'accettazione automatica dei depositi di cancelleria nei sistemi dei Registri di Cancelleria SICID, SIECIC e SIGP., BEA, Consolle Magistrato, Consolle Udienza e Consolle PM., secondo quanto previsto nelle nuove specifiche tecniche del 2 agosto 2024.

In seguito a tale intervento, verrà creato un automatismo che permetterà l'accettazione di tali depositi senza alcun intervento da parte del cancelliere, esclusivamente per le seguenti tipologie di atti:

Rito ordinario di cognizione

1. *Memoria171ter1, associato all'evento M171- MEMORIA EX ART. 171-TER N.1*
2. *Replica171ter2, associato all'evento R171 - REPLICHE EX ART. 171-TER N.2*

3. Controrepliche171ter3, associato all'evento C171 - CONTROREPLICHE EX ART. 171-TER N.3

4. IstanzaAccoglimentoDomanda183ter, associato all'evento I183 - ISTANZA DI ACCOGLIMENTO DELLA DOMANDA (art. 183 ter cpc)

5. IstanzaRigettoDomanda183quater, associato all'evento J183 - ISTANZA DI RIGETTO DELLA DOMANDA (art. 183 quater cpc)

6. MemoriaIstruttoria183UC, associato all'evento DMIS- MEMORIA ISTRUTTORIA EX ART. 183, U.C., C.P.C.

7. MemoriaReplica183UC, associato all'evento DMRP - MEMORIA DI REPLICA EX ART. 183, U.C., C.P.C.

8. DepositoDocumentiAutorizzatiInUdienza, associato all'evento DDAU - DEPOSITO DOCUMENTI AUTORIZZATI ALL'UDIENZA

9. DepositoNoteScritteInSostituzioneUdienza, associato all'evento DNSU - DEPOSITO NOTE SCRITTE IN SOSTITUZIONE UDIENZA

10. NoteScrittePC, associato all'evento DNPC - NOTE SCRITTE PC

11. NoteConclusionali, associato all'evento NCON - NOTE CONCLUSIONALI

12. ComparsaConclusionale190, associato all'evento DQ - DEPOSITO COMPARSE CONCLUSIONALI

13. ComparsaConclusionaleReplica190, associato all'evento DD - DEPOSITO MEMORIE DI REPLICA

Rito semplificato

1. Memoria473Bis17c1, associato all'evento P473 - DEPOSITO MEMORIA ART. 473-bis.17, C.1, C.P.C.

2. Memoria473Bis17c2, associato all'evento S473 - DEPOSITO MEMORIA ART. 473-bis.17, C.2, C.P.C.

3. Memoria473Bis17c3, associato all'evento T473 - DEPOSITO MEMORIA ART. 473-bis.17, C.3, C.P.C.

Atti processuali davanti al giudice di pace

IstanzaGenerica, più specificatamente i dispositivi ivi previsti, quali:

- *istanzaExArt186Bis, associato all'evento X1 - DEPOSITO ISTANZA EX ART. 186 BIS CPC;*
- *istanzaExArt186Ter, associato all'evento X2 - DEPOSITO ISTANZA EX ART. 186 TER CPC;*
- *istanzaExArt186Quater, associato all'evento X3 - DEPOSITO ISTANZA EX ART. 186 QUATER CPC;*

- *istanzaFissazioneTermineNoteSostUdienza, associato all'evento DRTNS - RICHIESTA DI FISSAZIONE TERMINE PER NOTE IN SOST. UDIENZA*
- *opposizioneTermineNoteSostUdienza, associato all'evento ONSU - OPPOSIZIONE AL TERMINE PER NOTE IN SOSTITUZIONE UDIENZA*
- *depositoNoteSostitutiveUdienza, associato all'evento DNSU - DEPOSITO NOTE SCRITTE IN SOSTITUZIONE UDIENZA*
- *depositoMemorie, associato all'evento DN - DEPOSITO MEMORIE*

Atti del pm – sicid (cc e vg)

Alla lista di atti elencati nei paragrafi precedenti vanno aggiunti visti, pareri e memorie depositati dalla segreteria della procura presso il tribunale ordinario e dei minori.

Atti siecic - registro esecuzioni concorsuali

1) AttoGenericoCCIPU

Più specificatamente i dispositivi ivi previsti, quali:

- *DepositoMemorie => evento CMEMO - DEPOSITO MEMORIE*
- *RinunciaDebitore => evento CDES2 - DEPOSITO RINUNCIA DEL DEBITORE*
- *depositoRimessioneTermini => evento CIDRT -ISTANZA DI RIMESSIONE NEI TERMINI*
- *depositoNotaSpese => evento DEPNS – DEPOSITO NOTA SPESE*
- *depositoIstanzaLiquidazionePatrocinio => evento PSHP - P.S.S. (patrocinio a spese dello stato) -DEPOSITO ISTANZA DI LIQUIDAZIO NE*

2) IstanzaGenericaCCIPU. Più specificatamente i dispositivi ivi previsti, quali:

- *AmmAnticipataPSS => evento PSSIAA -P.S.S. - ISTANZA DI AMMISSIONE ANTICIPATA DA PARTE DEL COA*
- *AnticipazioneUdienza => evento IAU -ISTANZA DI ANTICIPAZIONE UDIENZA*
- *AutorizAttiStraordAmm => evento CASTR - ISTANZA DI AUTORIZZAZIONE A COMPIMENTO ATTI DI STRAORD. AMM.NE*
- *AutorizPagamCredPregressi => evento IAPCP - ISTANZA AUTORIZZAZIONE PAGAMENTO CREDITI PREGRESSI*
- *ConfermaMisureProtettive => evento ICMP -ISTANZA DI CONFERMA MISURE PROTETTIVE*

- *DifferimentoUdienza => evento IDU - ISTANZA DI DIFFERIMENTO UDIENZA*

- *RevocaMisureCautelari => evento IRMC - ISTANZA DI REVOCA DELLE MISURE CAUTELARI*

- *PartecProcAffidamentoContrPubb => evento IPPACP - ISTANZA DI PARTECIPAZIONE PROCEDURA AFFIDAMENTO CONTR. PUBBL.*

- *ProrogaMisureProtettive => evento IPMP -ISTANZA DI PROROGA MISURE PROTETTIVE*

- *RevocaMisureProtettive => evento IRMP - ISTANZA DI REVOCA DELLE MISURE PROTETTIVE*

- *SospensioneContrattoPendente => evento ISCP -ISTANZA SOSPENSIONE CONTRATTO PENDENTE*

- *TermineIntegDomComposizCrisi => evento ITIDCC - ISTANZA TERMINE INTEGRAZIONE DOMANDA COMPOSIZIONE CRISI*

Atti siecic - registro esecuzioni individuali

1) AttoGenerico

Più specificatamente i dispositivi ivi previsti, quali:

- *depositoIstanza41TUB => evento I8DI55 - DEPOSITO ISTANZA (EX. ART. 41 L.385/93)*

- *depositoRinunciaEsecuzione => evento IRIIN - RINUNCIA ALL'ESECUZIONE*

- *depositoRinunciaMandato => evento IRIMA DEPOSITO RINUNCIA AL MANDATO DELL'AVVOCATO*

- *depositoNotaSpese => evento DEPNS – DEPOSITO NOTA SPESE*

2. DEL FLUSSO DI ACCETTAZIONE AUTOMATICA

Dal 30 settembre 2024 l'accettazione automatica del deposito verrà implementata solo per quei depositi che non richiedano un intervento integrativo della cancelleria, elencati infra.

Nel caso sia attivo il flusso di accettazione automatica, al momento della ricezione di un deposito che rientra nelle casistiche adeguate, il sistema provvederà ad accettare automaticamente il deposito associandolo al fascicolo di pertinenza senza che sia necessaria alcuna operazione da parte della cancelleria, scaricando automaticamente l'evento relativo e ponendo il deposito in uno stato dedicato che evidenzi l'accettazione automatica.

Le pec che verranno inviate al mittente per comunicare lo stato del deposito e la sua accettazione saranno le medesime che riceve attualmente nel caso di accettazione manuale,

con specificazione della modalità di accettazione nella quarta pec. In particolare le pec ricevute saranno:

1) accettazione PEC, contenente la ricevuta di accettazione della PEC (RA);

2) consegna PEC, contenente la ricevuta di avvenuta consegna della PEC (RAC);

3) esito controlli deposito, contenente l'esito dei controlli automatici del deposito;

4) accettazione deposito, contenente l'esito di accettazione del deposito con la specifica della modalità di accettazione (manuale o automatica).

Nell'attuale maschera "Gestione depositi", presente nel menù "Pr. telematico", la cancelleria rinverrà i soli depositi che non sono stati accettati automaticamente e/o che dovranno essere lavorati manualmente come avviene attualmente. Pertanto, è di tutta evidenza che per questi ultimi permarrà, immutato, l'attuale menu di "intervento manuale" e tutte le funzionalità presenti in tale sezione. Permarranno altresì inalterati tutti i compiti ed i controlli che la cancelleria attualmente svolge.

Nella sezione "Gestione depositi" verranno visualizzati anche i depositi che sono in attesa di accettazione, sui quali non sarà possibile alcuna operazione perché sono in carico al sistema per verifiche ed eventuale accettazione automatica. Si precisa che questo è uno stato transitorio della busta, introdotto per avere evidenza dei depositi anche in caso di rallentamenti e/o grande carico nei sistemi. Verrà pertanto inserito un nuovo stato "In attesa di accettazione" il quale indica che il deposito è pervenuto nel sistema ed è in attesa di accettazione automatica, sul quale l'utente non potrà eseguire alcuna operazione. Successivamente, se l'accettazione automatica va a buon fine il deposito sarà visibile nella nuova sezione "Gestione depositi accettati automaticamente" passando nello stato "Accettato automaticamente" (come descritto successivamente), mentre se si verificheranno degli errori in fase di accettazione automatica il deposito permarrà in tale sezione "Gestione depositi" dove sarà possibile lavorarlo manualmente.

Come accennato sopra, nel caso in cui l'accettazione automatica vada in errore (ad esempio per un errore in fase di scarico dell'evento, ecc..), il sistema registrerà tale anomalia tra gli eventi busta e renderà disponibile il deposito in errore nella attuale maschera "Gestione depositi" per permetterne l'intervento manuale.

Per la gestione e la consultazione dei depositi accettati automaticamente verrà quindi implementata una nuova sezione, nel menù "Pr. telematico", denominata "Gestione depositi accettati automaticamente", all'interno della quale verranno convogliati tutti quei depositi che il sistema ha accettato automaticamente. In tale sezione sarà possibile per la cancelleria visionare i depositi ed effettuare tutte le operazioni presenti ad oggi nella sezione "Gestione depositi" ad eccezione dell'intervento manuale e del rifiuto. La cancelleria potrà quindi esaminare il deposito e segnalare al giudice assegnatario del processo la necessità di provvedere sull'istanza, ponendo "in visione" al magistrato il fascicolo. In tale caso il fascicolo, al termine dello scarico dei fascicoli nella consolle, comparirà anche nella cartella "atti ed istanze da esaminare".

I filtri di ricerca e la tabella dei risultati saranno i medesimi presenti in "gestione depositi" con la particolarità che nella tendina delle tipologie di deposito non sarà presente la voce "Errori fatali" e nella tendina degli stati sarà presente la voce "Accettato automaticamente" la quale indica che il deposito è stato correttamente accettato automaticamente dal sistema.

Concludendo, il flusso operativo di accettazione automatica può essere riassunto come segue:

*1- **Accettazione automatica del deposito**: in sede di accettazione automatica del deposito verrà registrato in automatico nello storico del fascicolo l'evento specifico cui è associato il deposito stesso (per dettagli sugli atti e gli eventi collegati si veda il capitolo 2.9.3 del documento di analisi).*

*2- Nella nuova sezione "**Gestione depositi accettati automaticamente**" la cancelleria potrà accedere alle funzionalità di consultazione dei depositi che il sistema ha accettato automaticamente e potrà verificarne la correttezza rispetto all'atto associato, essendo l'evento specifico già stato scaricato dal sistema, e quindi aggiungere ulteriori eventi e/o procedere direttamente allo svolgimento adempimenti successivi (invio notifiche, comunicazioni, pubblicazione, messa in visione al magistrato, ecc.).*

*3- Nel Cruscotto riassuntivo del Pr.Telematico presente nel SICID e nel SIGP verrà inserita una voce "**Depositi accettati automaticamente**" con il conteggio dei depositi che sono stati accettati automaticamente.*

3. DEGLI ATTI SOTTRATTI ALLA ACCETTAZIONE AUTOMATICA

A partire dal 30 settembre 2024 restano ancora esclusi dall'ambito del flusso di accettazione automatica, i depositi che versano nello stato ERROR o WARNING poiché si è reputato necessario effettuare un approfondimento di tali casistiche al fine di verificare le possibilità tecniche di automazione dell'accettazione.

Anche i depositi in stato FATAL non saranno oggetto di modifiche rispetto all'attuale gestione.

Restano esclusi dall'ambito del flusso di deposito automatico, altresì, le seguenti fattispecie di depositi che richiedono una puntuale valutazione da parte della cancelleria e/o uno specifico intervento in fase di accettazione:

1) gli atti che richiedono la preventiva individuazione del corretto evento da registrare a sistema poiché non legati ad uno specifico evento, ma associabili a più eventi presenti nella "stati-eventi". È pertanto necessario l'intervento manuale della cancelleria per associare l'evento specifico al corrispondente atto depositato telematicamente.

2) Gli atti che richiedono il completamento manuale dei dati e quindi l'attività (ad es. artt. 57 e 58 c.p.c.) di verifica della correttezza/completamento dei dati del provvedimento, proprio al fine di evitare interventi correttivi/integrativi manuali successivi (es. denominazioni,

codici fiscali delle parti ecc.), se non addirittura l'apertura di procedimenti di correzione errore materiale.

3) Le buste che hanno un deposito o una sequela di depositi complementari.

4) Gli atti che comportano transiti di stato tenuto conto della complessità che discende anche all'eventuale annullamento e ripristino dello stato precedente.

5) I seguenti depositi dei PM nei procedimenti civili/minorenni che per loro natura (vedi elenco infra) non sono passibili di accettazione manuale:

- *segnalazioni della Procura per i minorenni verso il Tribunale - la cancelleria in questo caso deve verificare preventivamente l'esistenza di segnalazioni su altro minore ecc;*
- *richiesta di visibilità della Procura verso fascicoli del Tribunale ordinario – il Tribunale effettua una valutazione prima dell'accettazione e conseguente apertura di visibilità;*
- *depositi da PM a propria segreteria – oltre alle considerazioni di cui sopra, in queste fattispecie la segreteria effettua un necessario lavoro di integrazione documentale contestualmente all'accettazione del deposito interno dell'atto, atto che diverrà poi introduttivo del giudizio presso il Tribunale.*

6) Gli atti che richiedono incombenti di cancelleria correlati all'accettazione: è necessario, infatti, che l'ufficio sia in grado di recuperare con assoluta precisione gli atti che prescrivono ineludibili adempimenti (di legge o su ordine del giudice) quali, a titolo esemplificativo, l'invio di comunicazioni/ notifiche/trasmissioni di cancelleria e l'invio al PM/PG.

Si invitano i signori dirigenti delle cancellerie a predisporre e diramare opportune istruzioni da destinare al personale di cancelleria.

Si prega di assicurare la massima diffusione alla presente nota.

Il Direttore Generale
Vincenzo De Lisi

Documento firmato digitalmente in epigrafe
ai sensi del D. Lgs. n. 82/2005

De Lisi
Vincenzo
MINISTERO
DELLA
GIUSTIZIA
18.09.2024
10:33:13
GMT+01:00

Ministero della Giustizia

Dipartimento per l'Innovazione Tecnologica della Giustizia

Direzione generale per i sistemi informativi automatizzati

AP/AR/mm-mp

Ai Sigg. Presidenti di Corte d'Appello

Ai Sigg. Procuratori Generali presso le Corti d'Appello

Agli Uffici Distrettuali per l'Innovazione presso le Corti di Appello

Ai Signori RID Requirenti e Giudicanti presso le Corti di Appello

Ai Sigg. Presidenti dei Tribunali

Ai Sigg. Procuratori della Repubblica

Al Signor Procuratore Europeo Delegato

Ai Sigg. Dirigenti Amministrativi di
Corti d'Appello
Procure Generali
Tribunali
Procure della Repubblica
Procura Europea Delegata

Alle Avvocature Distrettuali dello Stato
SEDI

Al Consiglio Nazionale Forense
SEDE

All'Unione delle Camere Penali
SEDE

e, per conoscenza,

Al Sig. Capo Dipartimento per gli Affari di Giustizia

Al Sig. Capo Dipartimento per l'Innovazione Tecnologica della Giustizia

Oggetto: Accettazione automatica degli atti. Chiarimenti. Atti esclusi dalla accettazione automatica.

Per agevolare gli Uffici Giudiziari nell'organizzazione e nella gestione delle attività di lavorazione dei depositi telematici operati dai difensori tramite il portale PdP, si forniscono i seguenti chiarimenti relativi alle tipologie di atti processuali esclusi dalla accettazione automatica e, rispetto ai quali, è ancora necessaria la verifica ed accettazione manuale da parte degli operatori addetti

Sono sempre escluse dall'accettazione automatica le seguenti tipologie di depositi:

- *Nomina difensiva nei casi in cui è necessario allegare un atto abilitante*
- *Richiesta di accesso agli atti*
- *Richiesta avocazione al Procuratore Generale*
- *Rescissione del giudicato*
- *Revisione*
- *Riparazione per ingiusta detenzione*
- *Denunce*
- *Querele*
- *Istanze procedimento*
- *Integrazioni di denuncia/querela/istanza procedimento*
- *Richieste di certificati 335*
- *Solleciti*
- *Tutti gli atti depositabili al Tribunale del Riesame*

Sono inoltre esclusi dall'accettazione automatica, per motivazioni relative alla tutela del segreto della fase delle indagini, tutti i depositi inviati al GIP relativi a fascicoli che si trovano in iter interlocutorio, con l'eccezione delle richieste di incidente probatorio, di convalida fermo o arresto, di proroga dei termini di indagine e di ammissione all'oblazione; sono inoltre esclusi i depositi indirizzati al GIP verso fascicoli oggetto di richiesta di emissione di decreto penale di condanna e di sentenza ex articolo 129 c.p.p.

Si evidenzia che, per gli stessi procedimenti qui richiamati, esclusi dall'operatività dell'accettazione automatica, non viene esposto al difensore sul PdP il numero di registro generale assunto presso l'ufficio GIP.

Nel ribadire l'assoluto spirito di collaborazione e confronto nell'avvio all'utilizzo dell'Applicativo per il Processo Penale, si coglie l'occasione per ricordare che al link https://helpdesk.giustizia.it è attivo il servizio di assistenza, deputato altresì a veicolare a questa Direzione ogni richiesta che possa contribuire al miglioramento dei sistemi.

Si ritiene opportuno indirizzare la presente nota di chiarimenti anche all'avvocatura tutta, al fine di rendere quanto più diffuse e consapevoli le modalità di utilizzo del Portale PdP e gli effetti del suo "colloquio" con gli applicativi degli Uffici Giudiziari.

In particolare, si coglie l'occasione per sensibilizzare gli utenti avvocati a verificare, nella fase preliminare all'invio del deposito sul PdP, l'esatta corrispondenza tra il contenuto dell'atto depositando e la selezione della relativa tipologia, così come la correttezza dei numeri di procedimento e dell'ufficio destinatario, prerequisiti per un corretto indirizzamento del deposito e una corretta alimentazione del fascicolo processuale digitale, nell'ottica della sua gestione interna e della successiva consultazione.

Il Direttore Generale reggente

Dott.ssa Gabriella De Stradis

Documento firmato digitalmente ai sensi del D.Lgs 82/2005

Prot. 5847/2024 del 13/11/2024

Da prot.tribunale.siracusa@giustiziacert.it

Oggetto **Accettazione automatica degli atti. Chiarimenti Atti esclusi dalla accettazione automatica** 12/11/2024 14:41:32

A ord.siracusa@cert.legalmail.it

---

2 allegati:

AccettazioneAutomatica_(atti_esIcusi)_(1)_signed.pdf (188.9 KB)

AccettazioneAutomatica_(atti_esIcusi)_(1)_signed_timbrato.pdf (158.6 KB)