PROVINCIA DI CUNEO

# MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE

## SOMMARIO


PARTE PRIMA – DISPOSIZIONI PRELIMINARI 5

1. Riferimenti normativi 5
2. Finalità, contenuti e metodologia del documento 6
3. Approvazione, aggiornamento e pubblicazione del Manuale 6

PARTE SECONDA – ORGANIZZAZIONE 7

4. Area organizzativa omogenea e Unità Organizzative 7
5. Responsabile della gestione documentale 7
6. Sistema informatico di gestione documentale dell'ente 8
7. Ufficio Protocollo e UUOO responsabili delle attività di protocollazione 8
8. Abilitazioni di accesso 9

PARTE TERZA – FORMAZIONE DEI DOCUMENTI 10

Sezione prima – Modalità di formazione 10

9. Modalità di formazione dei documenti informatici 10
10. Creazione e redazione tramite software di documenti informatici 10
11. Elementi essenziali del documento amministrativo informatico 11
12. Scelta del formato e modalità di sottoscrizione 11
13. Acquisizione di documenti informatici 12
14. Copie per immagine di documenti analogici 12
15. Duplicati, copie ed estratti informatici di documenti informatici 13
16. Conformità di copie ed estratti informatici di documenti informatici 14
17. Formazione di registri e repertori 14

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione 15

18. Dispositivi di firma elettronica 15
19. Scadenza dei certificati di firma 15

20. Identificazione univoca del documento informatico 15
21. Associazione degli allegati al documento principale 16
22. Accessibilità del documento informatico 16
23. Metadati del documento informatico 16
24. Immodificabilità e integrità del documento informatico 17
Sezione terza - Disposizioni sulla formazione di documenti analogici 17
25. Copie analogiche di documenti informatici 17
26. Casi in cui è ammessa la formazione o l'acquisizione di documenti originali analogici 18
PARTE QUARTA - GESTIONE DOCUMENTALE 19
Sezione prima - Flussi documentali esterni 19
27. Ricezione telematica di documenti informatici in entrata 19
28. Canali di ricezione 19
29. Formati accettati 20
30. Verifica sul formato dei documenti allegati 21
31. Controllo dei certificati di firma 21
32. Trasmissione telematica di documenti informatici in uscita 21
33. Individuazione del domicilio digitale presso cui effettuare la comunicazione 22
34. Modalità di consultazione ed estrazione dei domicili digitali contenuti negli elenchi pubblici 23
35. Disposizioni sui documenti analogici 23
Sezione seconda - Protocollo informatico 24
36. Sistema di protocollo informatico 24
37. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico 24
38. Registro generale di protocollo 24
39. Registro giornaliero di protocollo 25
40. Documenti soggetti a registrazione di protocollo e documenti esclusi 25
41. Protocollazione di documenti interni 26
42. Disposizioni per particolari tipologie di documenti 26
43. Registrazione di protocollo 26
44. Modalità di registrazione 27
45. Protocollazione delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione 28
46. Annullamento e modifiche della registrazione di protocollo 28
47. Gestione degli allegati 29
48. Informazioni agli utenti rese dal responsabile del procedimento 29

49. Tempi di registrazione e casi di differimento 30
50. Segnatura di protocollo 30
51. Protocollo riservato 31
52. Registro di emergenza 32
53. Documenti soggetti a registrazione particolare 33
Sezione terza - Disposizioni sulla protocollazione e gestione dei documenti analogici 34
54. Protocollazione dei documenti analogici 34
55. Registrazione, segnatura, annullamento 34
56. Rilascio della ricevuta di avvenuta protocollazione 34
57. Corrispondenza contenente dati sensibili 35
58. Corrispondenza personale o riservata 35
59. Corrispondenza cartacea non di competenza dell'Amministrazione 35
Sezione quarta – Classificazione e fascicolazione 36
60. Classificazione dei documenti 36
61. Fascicolazione informatica dei documenti 36
Sezione quinta – Flussi documentali interni 37
62. Assegnazione dei documenti in entrata agli uffici 37
63. Comunicazioni interne 38
64. Pubblicazioni nell'Albo pretorio e in Amministrazione Trasparente 38
PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI 39
65. Sistema di conservazione dei documenti informatici 39
66. Responsabile della conservazione 39
67. Oggetti della conservazione 40
68. Formati ammessi per la conservazione 41
69. Modalità e tempi di trasmissione dei pacchetti di versamento 41
70. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica (archivio corrente) 42
71. Accesso al Sistema di conservazione 42
72. Selezione e scarto dei documenti 42
73. Conservazione, selezione e scarto dei documenti analogici 42
74. Misure di sicurezza e monitoraggio del sistema di conservazione 43
PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI 43
75. Sicurezza dei sistemi informatici dell'ente 43
76. Amministratore di sistema 44
77. Uso del profilo utente per l'accesso ai sistemi informatici 44
78. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Ente 45

## ALLEGATI

| | |
|---|---|
| Allegato 1. | Organigramma con indicazione delle UUOO |
| Allegato 2. | Atto di nomina RGD e RC |
| Allegato 3. | Manuali operativi del software “Sistema di gestione documentale” e Allegato 3.1 |
| Allegato 4. | Sistema informatico di Gestione Documentale |
| Allegato 5. | Guida alla formazione del documento accessibile |
| Allegato 6. | Titolario di Classificazione |
| Allegato 7. | Piano di conservazione e scarto dell’archivio |
| Allegato 8. | Piano di Fascicolazione dell’Ente e Allegato 8.1 |
| Allegato 9. | Manuale di conservazione del Conservatore, Allegato 9.1 Manuale di Conservatore e 9.2 Note conservazione |
| Allegato 10. | Modello per registro di protocollo d’emergenza |

# PARTE PRIMA – DISPOSIZIONI PRELIMINARI

## 1. Riferimenti normativi

Il presente Manuale di gestione documentale (d'ora in avanti anche solo "Manuale") è adottato ai sensi delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (d'ora in avanti anche solo "Linee guida"), emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla determinazione del 17 maggio 2021 n. 371.

Gli allegati alle Linee guida sono parte integrante delle stesse e contengono disposizioni relative a:

1) Glossario dei termini e degli acronimi;
2) Formati di file e riversamento;
3) Certificazione di processo;
4) Standard e specifiche tecniche;
5) Metadati;
6) Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD")
- le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 *"Disposizioni legislative in materia di documentazione amministrativa"* (di seguito anche solo "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"*;
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento

(UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento “eIDAS”);

- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *“Regolamento generale sulla protezione dei dati”* (“GDPR”) e d.lgs. 30 giugno 2003 n. 196 “*Codice in materia di protezione dei dati personali*”.

## 2. Finalità, contenuti e metodologia del documento

Il presente Manuale, ai sensi del paragrafo 3.5. delle Linee guida, descrive il sistema di gestione informatica dei documenti della Provincia di Cuneo e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell’ente.

Il Manuale è reso noto anche esternamente all’ente. Il presente Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell’azione amministrativa.

## 3. Approvazione, aggiornamento e pubblicazione del Manuale

Il presente Manuale e i suoi allegati sono approvati con atto dell’organo della Provincia competente, su proposta del Responsabile della gestione documentale di cui al successivo par. 5.

I successivi aggiornamenti del Manuale devono essere altresì sottoposti all’approvazione dell’organo competente. L’aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale. Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Piano di classificazione (Titolario) e il Piano di conservazione dei documenti (Massimario di selezione e scarto).

Il Manuale e gli allegati sono pubblicati sul sito istituzionale dell’ente, nella sezione “Amministrazione Trasparente”, sottosezione “Atti generali”.

# PARTE SECONDA – ORGANIZZAZIONE

## 4. Area organizzativa omogenea e Unità Organizzative

La Provincia di Cuneo si configura come un'unica Area Organizzativa Omogenea ("AOO") identificata nell'Indice PA con il seguente codice univoco: AF56BEC.

L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

Le Unità Organizzative ("**UUOO**") che afferiscono alla AOO sono riportate nell'organigramma di cui all'**Allegato 1**, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa dell'ente. Le UUOO sono individuate in modo da rispecchiare l'organigramma dell'ente.

## 5. Responsabile della gestione documentale

L'ente, nell'ottica di gestire modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura direttiva, il "Responsabile della Gestione Documentale" (d'ora in avanti anche solo "**Responsabile**" o "**RGD**"), dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale di cui al par. 3.4 delle Linee guida.

Il RGD è stato individuato con il provvedimento di nomina di cui all'**Allegato 2** al presente Manuale.

Al RGD sono affidati i seguenti compiti:

a. è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica dell'ente;
b. provvede, d'intesa con il Responsabile della conservazione (di cui al **par. 69**) e il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
c. monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
d. assicura la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione
e. valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
f. vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo e produzione del registro giornaliero di protocollo;

g. assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati;
h. assicura, d'intesa con il Responsabile della Conservazione (di cui al **par. 69**), la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione (cfr. Parte quinta del presente Manuale);
i. effettua un periodico censimento degli strumenti software di gestione documentale in uso presso l'ente e, di concerto con il RTD, ne verifica la conformità alla normativa vigente

Ulteriori e specifici compiti del Responsabile sono indicati negli atti organizzativi che istituiscono il servizio per la tenuta del protocollo informatico, nel provvedimento di nomina e nelle sezioni pertinenti del presente Manuale.

Il RGD, ferma restando la propria responsabilità, può delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

## 6. Sistema informatico di gestione documentale dell'ente

L'ente, per la gestione documentale si avvale di un apposito sistema software gestionale (d'ora in avanti "**Sistema**"), che garantisce le seguenti funzionalità, tra loro integrate:

- protocollazione dei documenti e tenuta del protocollo informatico;
- acquisizione dei documenti informatici provenienti da caselle PEC e strumenti web di acquisizione delle istanze online;
- sistema di work flow per l'assegnazione, lo scambio e la lavorazione dei documenti da parte degli uffici;
- creazione e gestione dei fascicoli informatici;
- gestione dell'iter di approvazione degli atti amministrativi;
- pubblicazione degli atti in albo pretorio e nella sezione amministrazione trasparente del sito istituzionale dell'ente.

La puntuale descrizione delle componenti e delle funzionalità dei software di cui si compone il Sistema è rinvenibile nei relativi manuali operativi di cui all'**Allegato 3 e 3.1** al presente Manuale.

## 7. Ufficio Protocollo e UUOO responsabili delle attività di protocollazione

La protocollazione dei documenti informatici in entrata è centralizzata ed è curata dal personale dell'Ufficio responsabile della tenuta del Protocollo, che provvede all'organizzazione ed espletamento dei servizi di protocollo, di gestione dei flussi documentali e di conservazione e organizza e gestisce l'archivio cartaceo dell'Ente, anche ai fini del processo di digitalizzazione.

L'ufficio competente (di seguito per brevità anche solo "**Ufficio Protocollo**" o "**UP**"), inserito nell'Area Amministrativa, dunque, è individuato quale Unità Organizzativa ("**UO**") responsabile, in via generale, della protocollazione di tutti i documenti informatici acquisiti dall'Ente. L'UP provvede all'assegnazione dei protocolli alla Direzione o all'Ufficio competente.

Per quanto riguarda la protocollazione dei documenti informatici in uscita, tutti i dipendenti a cui è assegnata un'utenza per l'abilitazione d'accesso al Sistema informatico di gestione documentale dell'ente sono abilitati alla protocollazione, con esclusione degli utenti a cui sono attribuite funzioni di mera consultazione. La protocollazione in uscita, dunque, è decentrata presso ogni unità organizzativa dell'ente.

Il RGD, con proprio provvedimento, su indicazione dei Dirigenti e/o Responsabili di servizio, può individuare ulteriori unità organizzative responsabili per la protocollazione in entrata.

Ciascun Dirigente e/o Responsabile di servizio provvede a individuare, all'interno delle unità organizzative poste sotto la propria direzione, i delegati alle attività di protocollazione tra il personale in possesso di adeguate competenze in materia.

Sulle regole da seguire per la gestione dei flussi documentali, in ingresso e in uscita, e per la protocollazione o diversa modalità di registrazione dei documenti dell'ente, si rinvia alle indicazioni contenute nella Parte Quarta del presente Manuale.

## 8. Abilitazioni di accesso

Le abilitazioni di accesso degli utenti alle componenti del Sistema informatico di gestione documentale dell'ente sono assegnate personalmente a ciascun dipendente dall'Amministratore di Sistema, su indicazione di ciascun Dirigente e/o Responsabile di servizio entro cui è inquadrato il dipendente, nel rispetto dei criteri definiti dal RGD.

A ciascun utente del Sistema, pertanto, sono attribuite specifiche funzioni, diversificate in ragione dell'organigramma e, dunque, dell'appartenenza a una determinata area o servizio dell'organizzazione e dell'assunzione di specifici ruoli e compiti.

Le disposizioni riguardanti l'accesso al sistema informativo provinciale e all'acquisizione e messa a disposizione delle dotazioni informatiche di un nuovo utente del sistema informativo provinciale sono descritte nei paragrafi 6 e 7 del Regolamento del Sistema Informativo Provinciale, pubblicato sul portale intranet e internet della Provincia di Cuneo.

# PARTE TERZA – FORMAZIONE DEI DOCUMENTI

## *Sezione prima – Modalità di formazione*

### 9. Modalità di formazione dei documenti informatici

Tutti i documenti dell'ente sono formati in originale come documenti informatici, secondo le modalità individuate nella presente Parte del Manuale.

I documenti informatici degli uffici dell'Ente sono formati mediante una delle seguenti modalità:

a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati (ad esempio, mediante programmi di scrittura delle suite *Microsoft Office 365*, *Google Workspace* o *Libre Office*, o mediante l'utilizzo delle funzioni dei sistemi di gestione documentale);
b) acquisizione:
   - della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);
   - della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);
   - del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica oppure mediante l'utilizzo della funzione del sistema operativo "duplica");
c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari resi disponibili all'utente (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile online agli utenti);
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopra descritte.

### 10. Creazione e redazione tramite software di documenti informatici

Per la creazione dei documenti informatici mediante redazione, gli uffici dell'ente dispongono strumenti software con funzioni di text editing, integrati con gli applicativi gestionali per la formazione degli atti amministrativi.

Il testo del documento informatico creato dagli uffici dell'ente deve essere redatto utilizzando esclusivamente uno dei seguenti font: Arial, Helvetica, Trebuchet, Verdan

## 11. Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dall'ente deve recare i seguenti elementi:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. oggetto del documento;
4. riferimenti a procedimento o fascicolo;
5. sottoscrizione;
6. data e luogo;
7. numeri di pagina;
8. indicazione degli allegati (se presenti);
9. identificazione e dati dei destinatari (se si tratta di documento in uscita);
10. dati dell'Amministrazione (compresi codice fiscale, indirizzo e recapiti, se si tratta di documento in uscita);
11. mezzo di spedizione (se documento in uscita).

## 12. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dall'ente deve essere scelto tra i seguenti **formati standard**: **.pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods**. Inoltre:

- per le **immagini vettoriali** devono essere adottati i seguenti formati: **.dwg, .dwfx, .dwf, .svg, .svgz**;
- per le **immagini raster** devono essere adottati i seguenti formati: **.png .jpg, .jpeg, .tiff**;
- per i **dati strutturati** devono essere adottati i seguenti formati: **.sql, .csv, .accdb.**

Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico, in ogni caso, deve essere preferibilmente individuato tra i formati *standard* previsti nell'Allegato 2 alle Linee guida dell'AgID ed adottato osservando le raccomandazioni ivi contenute.

Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

I documenti che devono essere sottoscritti digitalmente, prima dell'apposizione della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). Anche al fine di facilitare la visualizzazione da parte degli utenti, i documenti in formato PDF e PDF/A sono sottoscritti preferibilmente con firma PADES, altrimenti CADES. Si precisa che, dal punto di vista giuridico, entrambe le tipologie di firma (PADES e CADES) sono idonee a garantire l'autenticità dei documenti informatici sottoscritti.

Nel caso il documento definitivo sia di un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (.p7m).

## 13. Acquisizione di documenti informatici

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

a) acquisizione di un duplicato informatico per via telematica o su supporto informatico (ciò avviene, ad esempio, quando si effettua il download di un documento dalla casella di posta elettronica, oppure, quando si duplica un file trasferendolo da un dispositivo di archiviazione esterno);
b) acquisizione della copia per immagine su supporto informatico di un documento analogico (ciò avviene, ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzando la copia in formato digitale);
c) acquisizione della copia informatica di un documento analogico (ciò avviene, ad esempio, quando un documento analogico di testo viene riversato in formato digitale tramite lettore OCR per il riconoscimento ottico dei caratteri).

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), può essere necessario assicurarne l'efficacia giuridico-probatoria, attraverso l'associazione o l'apposizione dell'attestazione di conformità della copia al documento originale. A tal fine, occorre seguire con le modalità indicate nei paragrafi successivi (cfr. par. 14 e 15).

In caso di acquisizione di un duplicato informatico (v. *supra*, lett. c), ai sensi dell'art. 23-*bis* del CAD, il documento acquisito ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto, non è mai richiesta l'attestazione di conformità.

## 14. Copie per immagine di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti. È questo il caso della scansione di documento cartaceo.

Di norma, i documenti cartacei trasmessi all'ente sono scansionati e acquisiti in copia digitale "semplice", per esigenze di uso lavoro e consultazione.

Tuttavia, nel caso in cui si debba garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il dirigente o il funzionario all'uopo delegato, che agisce in veste di pubblico ufficiale, archivia il documento analogico e appone sulla copia informatica, la propria firma digitale o altra tipologia di firma forte, previa iscrizione sul documento di dicitura del seguente tenore:

"*Io sottoscritto/a*, *ai sensi dell'art. 22, co. 2, d.lgs. n. 82/2005, attesto che la presente copia per immagine è conforme in ogni sua parte al documento originale analogico*

*dal quale è stata estratta.* [indicare: nome e cognome, nome ente e ufficio, data e luogo]."

Nel caso sia necessario attestare la conformità all'originale di più documenti, acquisiti per copia di immagine, ferma restando la necessità di effettuare il raffronto per ogni documento originale scansionato, è possibile effettuare un'unica attestazione di conformità, su foglio separato e collegato alle copie informatiche, da sottoscrivere digitalmente, contenente l'indicazione delle impronte hash associata a ciascuna copia informatica.

L'attestazione di conformità della copia per immagine al documento originale analogico è richiesta nei casi in cui è necessario o, comunque, vi sia l'esigenza di assicurare che la copia abbia la medesima efficacia giuridico probatoria del documento originale. Così deve avvenire, ad esempio:

a) quando si deve provvedere a **notificazione via PEC** di documento (o allegato a documento) sottoscritto in originale analogico (ad es., verbali di accertamento di sanzioni amministrative). In questi casi, come previsto dall'art. 6, comma 1-*quater* del CAD, la conformità della copia informatica all'originale analogico è attestata dal responsabile del procedimento;
b) quando si deve formare un contratto tra l'ente e un privato che sottoscrive con firma autografa (**formazione di contratti *ibridi***). In questi casi il pubblico ufficiale acquisisce la scansione del documento firmato in originale cartaceo dal privato e, previo raffronto, attesta la conformità della copia digitale (con le modalità sopra indicate). Infine, il soggetto competente alla stipula sottoscrive la copia con la propria firma digitale, così perfezionando il contratto. Quando pubblico ufficiale, che attesta la conformità della copia, e soggetto competente alla stipula coincidono, è sufficiente apporre un'unica firma digitale. Al fine di escludere il rischio di disconoscimento della firma, è preferibile che il pubblico ufficiale provveda contestualmente all'attestazione di conformità della copia digitale e all'autenticazione della sottoscrizione analogica ivi contenuta;
c) quando, ai fini della **conservazione digitale** dei documenti, si intende sostituire l'originale analogico con la copia informatica.

I documenti scansionati per mere esigenze di uso lavoro e consultazione non richiedono attestazione di conformità all'originale, ferma restando la necessità di conservare il documento originale analogico.

## 15. Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi (così avviene, ad esempio, quando si effettua un download, oppure, quando si duplica un documento nella memoria del proprio computer o verso dispositivo di archiviazione esterno). Tale modalità di formazione della copia del documento informatico non richiede alcuna

attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche.

L'identità tra due documenti informatici è rilevabile tramite il raffronto delle impronte *hash*. L'impronta *hash* di un documento informatico è una sequenza di lettere e cifre (lunga solitamente 64 caratteri), ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il *file* (per la verifica delle impronte *hash* è possibile utilizzare le funzioni del sistema di gestione documentale o appositi *software*).

La copia di un documento informatico, invece, è un documento il cui contenuto è il medesimo dell'originale, ma con una diversa evidenza informatica rispetto al documento da cui è tratto (ad esempio, quando si trasforma un .docx in .pdf, i due documenti avranno *hash* differenti. Lo stesso avviene se si estrae una parte di documento per formarne uno nuovo). Tale operazione è anche detta riversamento da un formato digitale verso un altro.

Se il documento originale è un documento firmato, affinché la copia abbia la medesima efficacia giuridico-probatoria, è necessario attestare la conformità della copia all'originale. Come per le copie per immagine, dunque, il dirigente o il funzionario delegato, che agisce in veste di pubblico ufficiale, dovrà apporre la propria firma digitale, previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

"*Io sottoscritto/a, ai sensi dell'art. 23-bis, comma 2, d.lgs. n. 82/2005, attesto che la presente copia informatica è conforme in ogni sua parte al documento originale informatico dal quale è stata estratta.* [indicare: nome e cognome, nome ente e ufficio, data e luogo]."

La necessità di apporre l'attestazione di conformità dipende dall'uso che viene fatto della copia, da valutare caso per caso, a seconda della rilevanza giuridica che si ritiene necessario conferire.

## 16. Conformità di copie ed estratti informatici di documenti informatici

Il personale con funzioni dirigenziali e gli ufficiali roganti hanno il potere di attestare la conformità delle copie di documenti originali formati o acquisiti dall'ente.

## 17. Formazione di registri e repertori

I registri e repertori tenuti dall'ente, ivi compreso il registro giornaliero di protocollo, sono formati mediante la generazione/raggruppamento in via automatica e memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale. Restano salve le speciali disposizioni che prescrivono la formazione di registri e repertori come documento originale analogico.

# *Sezione seconda – Disposizioni comuni a tutte le modalità di formazione*

## 18. Dispositivi di firma elettronica

L'ente garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma digitale o firma elettronica qualificata.

L'utilizzo da parte del personale dei dispositivi di firma e/o delle credenziali è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati o le credenziali di utilizzo.

## 19. Scadenza dei certificati di firma

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

## 20. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento del numero di protocollo o, per i documenti soggetti a registrazione particolare (cfr. **par. 55**), del numero del registro o repertorio sostituivo del protocollo.

Per i documenti informatici soggetti a registrazione di protocollo, inoltre, è prevista l'associazione dell'impronta *hash* del file, effettuata al momento della registrazione tramite le apposite funzioni del Sistema di protocollo informatico dell'ente. Il calcolo dell'impronta crittografica deve essere basato su una funzione di *hash* conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida (cfr. p. 2.2, tab. 1).

## 21. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte hash dei documenti allegati al documento principale.

Al documento principale, inoltre, devono essere associati i seguenti metadati:

- numero allegati;
- indice allegati;
- identificativo del documento allegato (IdDoc);
- titolo dell'allegato (Descrizione).

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc).

Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dal sistema di gestione documentale adoperato per la formazione del documento principale.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso (o, in alternativa, su foglio separato) l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta *hash*. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto immodificabile (ad esempio, dopo l'apposizione della firma digitale – cfr. **par. 25** del presente Manuale).

## 22. Accessibilità del documento informatico

Per garantire l'accessibilità dei documenti informatici ai soggetti portatori di disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nella "Guida pratica per la creazione di un documento accessibile" di cui all'**Allegato 5** al presente Manuale.

## 23. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi possono essere associati a particolari tipologie di documenti, secondo le indicazioni dei responsabili dei servizi e in conformità alle Linee guida.

L'associazione dei metadati al documento è effettuata tramite le apposite funzioni per la formazione degli atti del Sistema di gestione documentale. A tal fine, il Responsabile verifica la conformità degli strumenti software utilizzati e, eventualmente, richiede al fornitore i necessari interventi evolutivi.

I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione o del versamento in conservazione.

I criteri per valorizzare i metadati che prevedono un campo a testo libero sono definiti dal RDG e condivisi con tutto il personale addetto alla protocollazione.

### 24. Immodificabilità e integrità del documento informatico

Affinché sia garantito il valore giuridico-probatorio del documento informatico, ne deve essere assicurata l'immodificabilità e l'integrità.

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nelle fasi di accesso, gestione e conservazione.

L'immodificabilità e l'integrità dei documenti informatici dell'ente possono essere garantite:

- per i documenti di cui è richiesta la sottoscrizione, dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- per i documenti di cui non è richiesta la sottoscrizione, dalla memorizzazione nel sistema di gestione documentale, purché sia garantita la conformità agli standard indicati nelle Linee guida (cfr. allegato 4) e il rispetto delle misure di sicurezza;
- per tutte le tipologie documentali, dal versamento nel sistema di conservazione, conforme alle Linee guida e, in caso di esternalizzazione del servizio, alla determina AgID n. 455/2021, recante *Regolamento sui criteri per la fornitura di servizi di conservazione dei documenti informatici*.

Il versamento nel sistema di conservazione è il metodo che offre le maggiori garanzie di immodificabilità e integrità dei documenti informatici nel tempo. Pertanto, è essenziale che tutti i documenti siano versati in conservazione, secondo i tempi e le modalità descritte nella Parte Quinta del presente Manuale.

Il RGD assicura che i documenti informatici a cui è apposta una firma elettronica siano versati in conservazione prima che scada il certificato di firma.

## *Sezione terza - Disposizioni sulla formazione di documenti analogici*

### 25. Copie analogiche di documenti informatici

Fermo restando l'obbligo di formare i documenti originali informatici, in alcuni casi può essere necessario effettuare delle copie analogiche affinché siano spedite a mezzo

posta ai soggetti che non sono muniti di domicilio digitale e agli altri soggetti indicati all'art. 3-*bis*, comma 4-*bis*, CAD.

Quando è necessario che al destinatario giunga un documento avente la medesima efficacia giuridico probatoria del documento originale (ad esempio, quando bisogna assicurare l'efficacia legale della notificazione dell'avviso di accertamento relativo a tributi o a violazioni da cui discendono sanzioni amministrative), ai sensi dell'art. 3, d.lgs. n. 39/1993, la copia analogica dovrà essere accompagnata dall'indicazione della fonte del documento originale e del soggetto responsabile dell'immissione, riproduzione, trasmissione o emanazione del documento stesso. Quando il documento originale informatico è sottoscritto con firma digitale o altra firma elettronica qualificata, la firma è sostituita dalla firma a stampa accompagnata dall'indicazione del nominativo del soggetto sottoscrivente.

La copia analogica, inoltre, deve contenere apposita dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento nativo digitale ed è disponibile presso l'amministrazione (ad es.: "COPIA CARTCEA DI ORIGINALE DIGITALE. DETERMINAZIONE N. ..DEL …Documento firmato digitalmente da ….e stampato il giorno ……...Si attesta che la presente copia cartacea è conforme all'originale digitale ai sensi del D.Lgs.82/2005 e successive modificazioni. Provincia di Cuneo, …….. Firma").

## 26. Casi in cui è ammessa la formazione o l'acquisizione di documenti originali analogici

Fermo restando l'obbligo di produrre i propri documenti in originale informatico, è legittimo formare o acquisire documenti in originale analogico:

a) ai sensi dell'art. 2, comma 6, CAD, esclusivamente nell'ambito dell'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile;
b) quando si acquisisce un documento analogico, consegnato a sportello o a mezzo posta, e il richiedente è un soggetto privato che non agisce in qualità di professionista;
c) in tutti i casi in cui per legge o regolamento il documento deve essere formato e/o rilasciato in formato cartaceo.

La formazione di contratti e altre scritture private in originale analogico non è consentita. A tal fine, nel caso in cui la parte contraente non sia munita di strumenti di firma digitale o qualificata, si seguono le indicazioni riportate al par. 14, lett. b) del presente Manuale.

# PARTE QUARTA - GESTIONE DOCUMENTALE

## *Sezione prima - Flussi documentali esterni*

### 27. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella Sezione seconda della presente Parte del Manuale. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

Le istanze, le dichiarazioni e le comunicazioni trasmesse per via telematica, in ogni caso, devono ritenersi valide a tutti gli effetti di legge quando:

a) sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;
b) sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;
c) sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE o CNS;
d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma 4-quinquies del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domicilio digitale speciale per quel singolo procedimento o affare;
e) sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;
f) è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

È vietata l'acquisizione o la trasmissione di documenti soggetti a protocollazione, e relativi allegati, tramite canali diversi da quelli previsti dall'Ente (ad es. strumenti personali per il trasferimento dei file).

### 28. Canali di ricezione

La ricezione di comunicazioni e documenti informatici è assicurata tramite i seguenti canali:

- casella PEC dell'UP: protocollo@provincia.cuneo.legalmail.it . L'indirizzo di posta elettronica certificata è abilitato alla ricezione dei documenti provenienti da indirizzi di posta elettronica ordinaria;

- altri canali di trasmissione indicati per specifici procedimenti.
- Sportello telematico per le istanze relative ai Trasporti eccezionali integrato con il protocollo.

Gli indirizzi di posta elettronica certificata sono riportati nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti e cittadini, quando espressamente previsto dalla disciplina del procedimento; altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici dell'ente comunicazioni e documenti in modalità analogica, questi non saranno ritenuti correttamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell'UO assegnataria della comunicazione, o comunque il soggetto individuato quale responsabile del procedimento, ai sensi dell'art. 5, comma 3, l. n. 241/1990, provvede a comunicare al mittente le modalità di trasmissione corrette. La comunicazione, quando reperibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-*bis*, 6-*ter* o 6-*quater* del CAD (INI-PEC, IPA, INAD, v. sul punto **par. 35** sull'individuazione del domicilio digitale).

### 29. Formati accettati

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei seguenti **formati standard**: **.pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods, .eml.** Inoltre:

- per le **immagini vettoriali** devono essere preferibilmente accettati i seguenti formati: **.dwg, .dwfx, .dwf, .svg, .svgz**;
- per le **immagini raster** devono essere preferibilmente accettati i seguenti formati: **.png, .jpg, .jpeg, .tiff**;
- per i **dati strutturati** devono essere preferibilmente accettati i seguenti formati: **.sql, .csv, .accdb**.

Possono essere accettati, inoltre, i formati contemplati nell'Allegato 2 delle Linee guida dell'AgID e indicati come "standard".

Resta salva la possibilità, da parte del responsabile del procedimento, di prevedere espresse limitazioni in relazione allo specifico procedimento, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze.

È possibile protocollare un documento in qualunque formato, purché sia accompagnato da una copia informatica del documento in uno dei formati ammessi.

Qualora pervengano documenti in formati non conosciuti o non gestiti, la circostanza deve essere segnalata in nota alla registrazione. Le comunicazioni al mittente relative alla mancata accettazione del formato e all'indicazione dei formati accettati sono effettuate a cura del responsabile del procedimento.

L’accettazione di formati non previsti dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per obiettive esigenze rappresentate dal mittente, il documento non può essere riversato in altro formato tra quelli ammessi.

### 30. Verifica sul formato dei documenti allegati

L’eventuale presenza di allegati al documento principale in formati non ammessi deve essere verificata dal responsabile del procedimento, il quale provvede a comunicare al mittente la non conformità del documento e/o l’assenza dei requisiti previsti per l’utilizzo ai fini del procedimento amministrativo.

L’accettazione di formati non previsti dal presente Manuale, dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per obiettive e motivate esigenze rappresentate dal mittente, il documento non può essere riversato in altro formato tra quelli ammessi.

### 31. Controllo dei certificati di firma

Il responsabile del procedimento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, lo segnala al personale addetto alla protocollazione, affinché indichi la circostanza in nota alla registrazione di protocollo (v. procedura di modifica di cui al **par. 50** del presente Manuale). Il responsabile del procedimento, inoltre, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

### 32. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso di trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD. Eccezionalmente può avvenire invio di corrispondenza firmata olografa dal Presidente.

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati, fascicolati e protocollati secondo le disposizioni della presente Parte del Manuale.

Per la trasmissione di documenti tramite PEC, se il documento principale non ha un contenuto sufficientemente esplicativo (ad esempio, un provvedimento, un certificato, ecc.) deve essere predisposta una nota di accompagnamento alla trasmissione.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione o a registrazione particolare secondo le medesime regole per la registrazione di protocollo dei documenti.

## 33. Individuazione del domicilio digitale presso cui effettuare la comunicazione

La notificazione o comunicazione **a un soggetto privato** (cittadino o ente privato, ad es. associazione), che abbia ad oggetto un rapporto che si pone al di fuori dell'attività professionale, deve essere fatta:

I. se vi è stata elezione di domicilio digitale speciale per particolari atti, procedimenti o affari, all'indirizzo PEC espressamente dichiarato dal cittadino;
II. in assenza di elezione di domicilio digitale speciale, al domicilio digitale generale eletto nell'INAD (Indice Nazionale dei Domicili digitali), accessibile all'URL domiciliodigitale.gov.it. La consultazione e l'estrazione automatica dei domicili digitali deve essere effettuata con le modalità di cui al paragrafo successivo;
III. in assenza di alcun domicilio digitale eletto, al domicilio fisico, trasmettendo la copia cartacea del documento. Se si tratta di documento sottoscritto dall'Amministrazione, la copia analogica deve essere prodotta in conformità a quanto previsto al **par. 26** del presente Manuale.

Per la trasmissione telematica di documenti a **imprese e professionisti** tenuti obbligatoriamente all'iscrizione in albi o elenchi, quando non vi è stata elezione di domicilio digitale speciale, il domicilio è estratto dall'indice INI-PEC (www.inipec.gov.it). Le comunicazioni agli indirizzi estratti da INI-PEC devono essere fatte quando hanno a oggetto informazioni o documenti rilevanti nell'ambito di rapporti professionali intercorrenti tra l'Amministrazione e il destinatario.

Quando l'indirizzo PEC del soggetto destinatario (professionista o impresa) iscritto in INI-PEC non risulti attivo, si provvede alla notificazione al domicilio fisico. Inoltre, la circostanza deve essere segnalata alla Camera di Commercio competente per la registrazione nel registro delle imprese o al soggetto competente per la tenuta dell'albo o registro presso cui il professionista è iscritto.

La trasmissione di comunicazioni e documenti verso altre **pubbliche amministrazioni e gestori di pubblico servizio** avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. I domicili digitali sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-*ter* del CAD.

Nei casi in cui dalla comunicazione dipende il decorso, la sospensione o l'interruzione di termini di legge o, comunque, quando il suo contenuto impegni l'ente verso l'esterno, la trasmissione è sempre effettuata via PEC.

## 34. Modalità di consultazione ed estrazione dei domicili digitali contenuti negli elenchi pubblici

La consultazione degli elenchi pubblici INAD, INI-PEC e IPA è sempre garantita liberamente, senza necessità di autenticazione dell'utente.

In caso di notificazioni massive con estrazioni multiple, è opportuno ricorrere all'estrazione dei domicili digitali in modalità applicativa, cioè in interoperabilità tra elenco pubblico e Sistema di gestione documentale.

I domicili digitali devono essere acquisiti nel momento stesso in cui si intende utilizzarli, al fine di assicurare la qualità del dato, nonché di limitare il trattamento di dati personali. Pertanto, non devono essere archiviate estrazioni statiche dei domicili digitali presenti negli elenchi al fine di costituire una banca dati anagrafica del Sistema di gestione documentale dell'ente.

La prova circa l'effettiva esistenza di un dato domicilio digitale in un dato momento è conservata dal gestore dell'elenco pubblico.

## 35. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire all'ente attraverso:

- il servizio postale;
- la consegna diretta agli uffici agli addetti alle attività di sportello.

I documenti provenienti dal servizio postale tradizionale o da corrieri autorizzati sono consegnati all'Ufficio Protocollo, che provvede alla registrazione e al deposito dei documenti nell'apposito casellario chiuso o li rende disponibili al ritiro presso l'ufficio Protocollo a cura dei singoli uffici.

Qualora chi presenta il documento richieda anche l'apposizione della ricevuta prodotta dal sistema di protocollo informatico con gli estremi, l'addetto all'Ufficio Protocollo provvede al rilascio della stessa nei tempi permessi dalle esigenze dell'ufficio e dal numero di utenti presenti in quel momento.

Nel caso di presentazione che necessitino di protocollazione immediata, l'operatore dell'Ufficio Protocollo provvede alla protocollazione contestualmente alla presentazione della pratica. Nel caso di ricezione dei documenti informatici, l'informazione al mittente dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dall'Amministrazione.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

La ricezione di documenti a mezzo fax provenienti da altre pubbliche amministrazioni è esclusa (come previsto dall'art. 47, comma 2, lett. c del CAD). Pertanto, tali comunicazioni non devono essere ritenute valide. Fanno eccezione i soli casi di esclusione dell'applicazione della normativa del CAD previsti dall'art. 2, comma 6, D.lgs. n. 82/2005 (ad es., comunicazioni di protezione civile).

# *Sezione seconda - Protocollo informatico*

## 36. Sistema di protocollo informatico

L'ente, per la protocollazione dei documenti, utilizza un Sistema di protocollo informatico integrato con il Sistema di gestione documentale. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo di cui all'**Allegato 3 e 3.1**.

È vietata l'acquisizione o la trasmissione di documenti soggetti a protocollazione e relativi allegati tramite canali diversi da quelli messi a disposizione dall'ente (ad es. strumenti personali per il trasferimento dei file).

## 37. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, il Responsabile, nella veste di responsabile del protocollo informatico:

a. coordina la gestione del Sistema di protocollo informatico;
b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
c. esercita il controllo generale sui flussi documentali esterni e interni;
d. assicura la corretta esecuzione delle attività di protocollazione;
e. autorizza l'attivazione del protocollo di emergenza;
f. autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
g. vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti delegati dal Responsabile. La modalità di individuazione dei soggetti delegati alle attività di protocollazione è definita al **par. 8** del presente Manuale.

## 38. Registro generale di protocollo

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo è associato in modo univoco e immodificabile al documento, pertanto esso individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Non è consentita la protocollazione di un documento già protocollato.

## 39. Registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

## 40. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dell'ente, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo, ad eccezione di quelli indicati successivamente.

Ai sensi dell'articolo 53 del TUDA sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni: di norma sono documenti di lavoro di natura non ufficiale, interlocutoria o comunque non definitiva, a preminente carattere informativo od operativo, ad es. scambio di prime bozze di documenti, convocazioni e verbali di incontri interni ad una struttura o comunque non caratterizzati da particolare ufficialità, memorie informali, brevi appunti, indicazioni operative del Dirigente della struttura, ecc.);
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.

Non sono soggetti a protocollazione obbligatoria, inoltre, gli atti e i documenti registrati in repertori e registri differenti dal registro di protocollo ai sensi del **par. 39** del presente Manuale.

Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce.

## 41. Protocollazione di documenti interni

Fermo restando quanto precisato nel paragrafo precedente con riferimento agli atti preparatori interni, sono soggetti a protocollazione tutti i documenti interni aventi rilevanza giuridico-probatoria, redatti dal personale nell'esercizio delle proprie funzioni ed al fine di documentare fatti inerenti all'attività svolta ed alla regolarità dell'azione dell'Ente o qualsiasi altro documento dal quale possano nascere diritti, doveri, o legittime aspettative di terzi. Deve essere protocollata altresì la corrispondenza interna di carattere formale.

## 42. Disposizioni per particolari tipologie di documenti

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, della Regione o da altre piattaforme conformi alla normativa vigente, non è necessaria quando i gestori di tali sistemi assicurano la conservazione a tempo indeterminato della documentazione relativa alle singole gare. In tali casi si ritiene comunque opportuno, anche se non necessario, la protocollazione della richiesta d'offerta o dell'ordine diretto di acquisto e dell'offerta dell'impresa aggiudicataria acquisendo, per questa, tutti i documenti relativi e specificando, negli appositi campi, data e ora di arrivo.

La gestione dei documenti acquisiti dallo sportello telematico è assicurata dal servizio per cui l'ente ha aderito ad apposita convenzione. La scrivania telematica dello sportello consente all'ente aderente di effettuare tutte le operazioni relative alla gestione dei documenti e all'attribuzione del protocollo informatico. Tramite il sistema di registrazione del servizio sono associati ai documenti acquisiti le seguenti informazioni:

- codice identificativo univoco, automaticamente assegnato dal portale web;
- data e l'ora di ricezione;
- mittente;
- destinatario;
- oggetto.

Il protocollo attribuito automaticamente dal Portale all'atto di presentazione della pratica è sufficiente ai fini della protocollazione e non richiede l'attribuzione di un ulteriore numero di protocollo da parte dell'ente aderente.

## 43. Registrazione di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e

certa. Ai sensi dell'art. 53, comma 1, TUDA, metadati di registrazione di protocollo sono:

a) numero di protocollo del documento, generato automaticamente dal sistema;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema;
c) il mittente, per i documenti ricevuti, e il destinatario (o i destinatari), per i documenti spediti;
d) oggetto del documento
e) data e protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico.

A suddetti metadati registrati in forma non modificabile, inoltre, possono essere aggiunti (a seconda dei casi) i seguenti ulteriori metadati:

g) tipologia di documento;
h) classificazione (titolo e classe) sulla base del Titolario (v. **allegato 6**);
i) fascicolo di appartenenza;
j) assegnazione interna (per competenza o per conoscenza);
k) data e ora di arrivo;
l) allegati;
m) livello di riservatezza;
n) mezzo di ricezione o invio;
o) annotazioni;
p) (eventualmente) estremi del provvedimento di differimento della registrazione;
q) (se necessario) elementi identificativi del procedimento amministrativo.

## 44. Modalità di registrazione

La registrazione di protocollo di un documento è eseguita dopo averne verificato la provenienza e ogni ulteriore elemento essenziale al corretto inserimento dei metadati obbligatori di cui al precedente paragrafo, nonché a evitare doppie registrazioni.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal Sistema di protocollo informatico. Al documento indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo.

Il Sistema genera automaticamente il numero progressivo e la data di protocollazione associata. Alla registrazione di protocollo, inoltre, sono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi PEC in uscita, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione. L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo.

Come precisato e ribadito dall'AgID (cfr. il *Vademecum* pubblicato a ottobre 2022), al fine di garantire l'interoperabilità tra AOO, la produzione di un documento segue il seguente **processamento**:

I. Formazione del documento principale ed eventuali allegati (la formazione del documento principale e degli eventuali allegati si conclude con la firma elettronica degli stessi);
II. Calcolo dell'impronta (hash) del documento principale e degli eventuali allegati;
III. Generazione del numero di protocollo da assegnare al messaggio di protocollo;
IV. Formazione della segnatura di protocollo (che deve rispettare l'XML Schema indicato nelle LLGG utilizzando le impronte del documento principale e degli eventuali allegati);
V. Apposizione di un "sigillo elettronico qualificato" alla segnatura di protocollo per garantire l'integrità e autenticità.

## 45. Protocollazione delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione

Gli utenti non abilitati alla protocollazione in entrata, per la protocollazione della posta elettronica ordinaria, provvedono a scaricare il file .EML contenente il messaggio in entrata e a inoltrarlo in allegato all'indirizzo di posta ordinaria dell'Ufficio Protocollo, esplicitando nell'oggetto la richiesta di protocollare. In tali casi, dunque, l'operatore addetto al protocollo provvede alla protocollazione del messaggio inoltrato in allegato (e non del messaggio di inoltro), assicurandosi che siano registrati i relativi dati.

Al fine di evitare doppie registrazioni dello stesso documento, prima dell'inoltro per la registrazione l'operatore deve verificare se nella comunicazione è stato indicato anche il recapito PEC. In tali casi, infatti, non serve provvedere all'inoltro per la protocollazione.

## 46. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA.

Se le informazioni della registrazione di protocollo sono errate (anche in caso di mera svista), dunque, sarà necessario procedere alla richiesta di annullamento.

Come previsto dal par. 3.1.5 delle Linee guida AgID, le uniche informazioni che possono essere modificate – e che, dunque, non richiedono l'annullamento – sono quelle relative a:

- classificazione;
- assegnazione interna.

Pertanto, è opportuno che ogni operatore al momento della protocollazione presti la massima attenzione. Il registro di protocollo, infatti, è un atto pubblico a cui la legge riconosce un particolare valore giuridico-probatorio. Come per ogni atto pubblico, la formazione richiede solennità e, dunque, la massima accortezza e precisione.

Ogni annullamento della registrazione deve:

- essere autorizzato con provvedimento del Responsabile. Il provvedimento, dunque, deve risultare da comunicazione formale;
- comportare la memorizzazione di data, ora e estremi del provvedimento di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es., registrazione di informazioni errate, doppia registrazione, erronea registrazione di documenti non destinati all'Ente). Nell'inviare il documento già oggetto di precedente registrazione, poi annullata, nelle note di trasmissione si dovrà dichiarare che: "*Il presente documento sostituisce il documento prot. n.* […] *di data* […]".

L'annullamento e le modifiche avvengono secondo la procedura guidata dal Sistema, che consente di mantenere traccia di ogni operazione, così come richiesto alla normativa.

## 47. Gestione degli allegati

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Tutti gli allegati devono pervenire con il documento principale al fine di essere inseriti nel Sistema di protocollo informatico ed essere sottoposti a registrazione.

Gli allegati dei documenti ricevuti tramite il canale PEC sono gestiti in forma automatizzata dal sistema di protocollo informatico.

**Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo**. L'associazione di allegati successivamente alla registrazione non può essere effettuata, dunque in tali casi è necessario procedere ad annullamento ed a nuova registrazione, attraverso la procedura di cui al precedente paragrafo.

## 48. Informazioni agli utenti rese dal responsabile del procedimento

Ogni responsabile del procedimento deve curare la **corretta informazione degli utenti**, fornendo tutte le informazioni necessarie relative a:

- **dimensione massima** degli allegati;
- **formato** dei documenti informatici trasmessi in allegato;

- **modalità di trasmissione** ed i relativi canali predisposti per lo specifico procedimento.

Anche per gli allegati, così come per il documento principale soggetto a protocollazione, è vietata l'acquisizione o la trasmissione tramite strumenti personali per il trasferimento dei file diversi da quelli messi a disposizione dall'ente.

## 49. Tempi di registrazione e casi di differimento

La registrazione della documentazione in entrata deve avvenire in giornata o comunque non oltre il giorno lavorativo successivo a quello di arrivo. Ai fini della gestione del protocollo non sono in ogni caso considerati lavorativi il sabato e la domenica.

In casi eccezionali ed imprevisti che non permettono di evadere la corrispondenza ricevuta e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del Responsabile è autorizzato il differimento dei termini di registrazione (protocollo differito).

Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il Responsabile deve descrivere nel provvedimento. Il provvedimento individua i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento. In ogni caso, della ricezione del documento informatico da parte dell'ente, fa fede la ricevuta di consegna generata dal gestore della casella PEC.

Ai fini del computo di termini previsti dalla legge o da altri atti (es. bandi, contratti, ecc.), resta fermo quanto previsto dall'art. 45 del CAD, ai sensi del quale il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

## 50. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate nell'ambito delle fasi di processamento della registrazione di protocollo, come indicate al precedente par. 32.

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione della Amministrazione mittente;
b. codice identificativo dell'AOO mittente;
c. codice identificativo del registro;
d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Il file XML di segnatura viene sottoscritto con il sigillo elettronico qualificato dell'Ente, che garantisce integrità del file e alla certezza del mittente.

Per garantire l'interoperabilità dei documenti informatici trasmessi alle altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti in un file XML conforme alle indicazioni previste al p. 2 e ss. dell'Allegato 6 alle Linee guida dell'AgID e, in particolare, nel rispetto dello schema di cui all'Appendice A (v. p. 4.1. "Segnatura di protocollo XML Schema").

## 51. Protocollo riservato

La gestione del protocollo riservato può essere utilizzata per i documenti che richiedono una trattazione riservata in quanto dalla loro visibilità si ritiene possano derivare un pregiudizio a terzi o al buon andamento dell'attività amministrativa. Sono previste particolari forme di riservatezza e di accesso controllato al sistema di protocollo per:

- documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza (ad es. documenti provenienti dalla Prefettura);
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite all'art. 24 della legge n. 241/1990).
- segnalazioni indirizzate al RPCT (Responsabile della prevenzione della corruzione e della trasparenza) ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato dell'ente, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati. Le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del Sistema di protocollo informatico a cura del Responsabile, che ne definisce altresì le abilitazioni di accesso per la consultazione e la gestione (v. par. 7 del presente Manuale).

## 52. Registro di emergenza

L'utilizzo del registro di protocollo emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile, o in assenza dal suo Vicario, in situazioni nelle quali per cause tecniche non sia possibile utilizzare il registro generale di protocollo informatico e la sospensione del servizio si protragga per un tempo tale da poter pregiudicare la registrazione a protocollo in giornata. In tali casi, il Responsabile dà immediata comunicazione a tutti gli uffici della temporanea sospensione dell'utilizzo della procedura informatizzata ordinaria di protocollazione e della necessità, per la protocollazione sia in entrata che in uscita, di consegnare la documentazione all'Ufficio Protocollo.

Il registro di protocollo di emergenza ha una numerazione progressiva propria, perciò ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

- gli estremi del provvedimento di autorizzazione all'utilizzo del registro;
- la causa, la data e l'ora di inizio dell'interruzione;
- il numero totale di registrazioni effettuate nel corso di ogni giornata di utilizzo;
- la data e l'ora del ripristino della funzionalità del sistema
- ogni altra annotazione ritenuta rilevante.

Al ripristino della piena funzionalità del Sistema di protocollo informatico, il Responsabile provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate, la data e l'ora di chiusura, e dà disposizioni per il riversamento delle registrazioni sul registro di protocollo generale.

Per le ipotesi di sospensione del servizio dovute a guasti del Sistema di protocollo informatico, l'Ente utilizza la procedura dedicata riportata nell'Allegato di riferimento,

**allegato 10**

## 53. Documenti soggetti a registrazione particolare

La registrazione particolare dei documenti richiede lo svolgimento delle medesime operazioni di gestione documentale effettuate per la registrazione di protocollo, ivi incluse la classificazione e la fascicolazione.

Sono soggette a registrazione particolare nei repertori e registri all'uopo istituiti le tipologie di documenti di seguito riportate:

- Determinazioni dirigenziali
- Deliberazioni di Consiglio Provinciale
- Deliberazioni di Assemblea dei Sindaci
- Decreti Presidente della Provincia
- Decreti Alta Amministrazione
- Decreti Ufficio Espropri
- Decreti Dirigenziali
- Ordinanze/ingiuzioni
- Atti di liquidazione
- Autorizzazioni/Concessioni
- Registro albo pretorio
- Registro delle sanzioni per violazioni del codice della strada
- Registro delle sanzioni amministrative

I registri e repertori diversi dal protocollo contengono almeno le seguenti informazioni:

- tipologia del registro o repertorio;
- numero di registro o repertorio (cronologico e progressivo);
- data;
- elementi identificativi dell'atto (soggetto o soggetti; oggetto);
- dati di classificazione e di fascicolazione;
- annotazioni.

Al fine di garantire i medesimi effetti della registrazione di protocollo, i registri e repertori di cui al presente paragrafo sono conservati con modalità analoghe a quelle del registro giornaliero di protocollo informatico.

Il RGD, al fine di dare attuazione ai principi di unicità e onnicomprensività del registro di protocollo, valuta periodicamente l'opportunità di sopprimere le forme di registrazione particolare non necessarie per legge, prevedendo in sostituzione esclusivamente la registrazione di protocollo.

# *Sezione terza - Disposizioni sulla protocollazione e gestione dei documenti analogici*

## 54. Protocollazione dei documenti analogici

Il personale addetto a effettuare la registrazione di protocollo informatica in entrata è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale).

Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione.

La copia per immagine di documenti firmati, se sprovvista di attestazione di conformità, apposta ai sensi della normativa vigente (v. le procedure definite al **par. 14** del presente Manuale), può essere adoperata solo per uso lavoro.

## 55. Registrazione, segnatura, annullamento

Alla registrazione di protocollo dei documenti cartacei si applicano, in quanto compatibili, le medesime regole previste per la registrazione dei documenti informatici.

Le lettere anonime sono soggette a registrazione di protocollo, eventualmente riservato, indicando nel campo del mittente la dicitura “MITTENTE ANONIMO”.

I documenti in cui vi è l’indicazione del mittente, ma manca la sottoscrizione vengono protocollati e viene annotato nelle informazioni “DOCUMENTO NON SOTTOSCRITTO”.

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati al par. 36, lett. da a) a e).

Sul documento analogico soggetto ad annullamento della registrazione si deve riportare a margine il numero di protocollo e la data dell’autorizzazione di annullamento. La segnatura (timbro ed etichetta) deve essere barrata con la dicitura “*annullato*”.

## 56. Rilascio della ricevuta di avvenuta protocollazione

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l’avvenuta consegna del documento, è cura del personale dell’Ufficio Protocollo rilasciare la **ricevuta di avvenuta protocollazione** prodotta direttamente dal protocollo informatico.
La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta i seguenti dati:

- il numero e la data di protocollo;
- l’indicazione dell’AOO;

- il mittente;
- l'oggetto;
- numero e descrizione degli allegati se presenti;
- l'indicazione di Responsabilità: UO e Responsabile del Procedimento Amministrativo cui è assegnato il documento per competenza;
- l'operatore di protocollo che ha effettuato la registrazione.

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi – se richiesto – a far pervenire la ricevuta all'indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

### 57. Corrispondenza contenente dati sensibili

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati sensibili" e successivamente consegnati all'organo istituzionale interessato o al dirigente competente in base all'assegnazione.

### 58. Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, ad eccezione di quella diretta ai titolari di cariche istituzionali. Se la corrispondenza riveste carattere "riservato" o "personale", e ciò è desumibile prima dell'apertura della busta, questa viene inviata chiusa direttamente al destinatario priva di registrazione. Se il carattere "riservato" o "personale" della corrispondenza viene desunto dopo averne preso visione, il plico viene richiuso e inviato al destinatario privo di registrazione. L'eventuale registrazione di protocollo potrà essere effettuata in un momento successivo.

### 59. Corrispondenza cartacea non di competenza dell'Amministrazione

Qualora pervenga, tramite posta tradizionale, un documento cartaceo che non è evidentemente indirizzato all'ente (es. altro destinatario), lo stesso è trasmesso a chi di competenza, se individuabile, altrimenti è restituito al mittente.

Nel caso in cui un documento della fattispecie sia erroneamente registrato al protocollo, questi è spedito a chi di competenza, oppure restituito al mittente, con una lettera di trasmissione protocollata.

# *Sezione quarta – Classificazione e fascicolazione*

## 60. Classificazione dei documenti

I documenti formati e acquisiti dall'ente sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Piano di classificazione (Titolario) di cui all'**Allegato 6**.

I documenti devono essere classificati prima della registrazione di protocollo. Non è ammessa la registrazione di protocollo di documenti non classificati.

La classificazione dei documenti in entrata è effettuata dal personale addetto alla protocollazione, mentre la classificazione dei documenti prodotti dall'Ente è effettuata dal Responsabile dell'UO o dal personale da questo delegato.

## 61. Fascicolazione informatica dei documenti

Al fine di garantire la consultazione dei documenti informatici, da parte sia di altre amministrazioni che degli utenti, questi sono raccolti in fascicoli informatici secondo le indicazioni fornite nel piano di fascicolazione dell'ente di cui all'**allegato 8**.

I documenti soggetti a protocollazione sono inseriti nel pertinente fascicolo tramite le apposite funzioni del Sistema di gestione documentale. Quando è necessario aprire un nuovo fascicolo informatico, l'utente abilitato alla creazione dei fascicoli della UO che ha prodotto il documento provvede all'apertura del fascicolo in cui inserire il documento.

Per i documenti in entrata, quando occorre provvedere all'apertura di un nuovo fascicolo informatico e vi sia incertezza sul criterio di fascicolazione da adottare, il personale addetto alla protocollazione provvede di concerto con il Responsabile della UO a cui è assegnato il documento.

I fascicoli informatici possono essere organizzati:

a. **per affare**, quando i documenti raccolti nel fascicolo, accomunati secondo un criterio di classificazione basato sulla competenza amministrativa, non sono tutti riferibili a un singolo procedimento amministrativo. Il fascicolo per affare deve avere una data di apertura e una durata circoscritta;
b. **per attività**, quando i documenti raccolti nel fascicolo attengono allo svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;
c. **per persona** (fisica o giuridica), quando i documenti raccolti nel fascicolo, anche con classificazioni diverse, sono riferibili a un medesimo soggetto. Sono fascicoli di tipo "aperto", con durata pluriennale e indeterminata;

d. **per procedimento amministrativo**, quando i documenti raccolti nel fascicolo rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

I fascicoli informatici devono recare i **metadati obbligatori delle aggregazioni documentali** previsti nell'allegato 5 alle Linee guida AgID. A tal fine, il RGD verifica che il software del sistema di gestione documentale che consente la creazione dei fascicoli informatici sia adeguato alla normativa tecnica vigente e, all'occorrenza, ne richiede l'adeguamento. Si ricorda che, a prescindere dalla tipologia, il fascicolo in ogni caso deve recare almeno i seguenti metadati:

- metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
- tipologia di fascicolo (ad es. procedimento amministrativo, affare, persona fisica, ecc.);
- codice IPA Amministrazione titolare (campo "Ruolo");
- codice IPA Amministrazioni partecipanti (campo "Ruolo");
- dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

## *Sezione quinta – Flussi documentali interni*

### 62. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate.

Ulteriori criteri di assegnazione automatica sono definiti dal RGD, sentite le UUOO interessate.

I documenti non assegnati automaticamente sono assegnati dal personale addetto alla protocollazione, in base all'oggetto del documento e alla classificazione, alle UO responsabili "per competenza".

Quando un documento è di interesse anche per più UUOO, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

Per i documenti analogici di interesse per più uffici, l'ufficio Protocollo provvede alla scannerizzazione documentale.

I documenti interni devono essere assegnati e consultati attraverso il Sistema di gestione documentale e la componente Sistema di protocollo informatico.

## 63. Comunicazioni interne

Tutte le comunicazioni interne sono effettuate esclusivamente in modalità telematiche, ivi compresa la pubblicazione di avvisi e comunicazioni a carattere informativo.

Lo scambio di documenti tra le diverse UUOO dell'ente è effettuato principalmente per mezzo di posta elettronica ordinaria, posta elettronica certificata o del sistema di *work flow* del Sistema di gestione documentale.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando una comunicazione è indirizzata a più destinatari e, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn).

In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dell'ente. Non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, Telegram, ecc.) per lo scambio di documenti nell'ambito dell'attività lavorativa.

## 64. Pubblicazioni nell'Albo pretorio e in Amministrazione Trasparente

Tutti gli atti prodotti dall'Ente che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto immodificabile (cfr. par. 15 del presente Manuale). Gli atti oggetto di notificazione tramite pubblicazione ai sensi del codice di procedura civile, una volta ricevuti e scansionati, sono inseriti manualmente dal personale abilitato.

Tutti gli atti prodotti dall'ente che, ai sensi della normativa vigente, sono soggetti a pubblicazione nella sezione Amministrazione Trasparente del sito istituzionale, sono trasmessi per la pubblicazione dagli utenti abilitati solo dopo che il documento sia divenuto immodificabile.

# PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

## 65. Sistema di conservazione dei documenti informatici

L'ente, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato a un conservatore accreditato dall'AgID (d'ora in avanti anche solo "Conservatore").

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al manuale di conservazione del Conservatore di cui all'**Allegato 9** al presente Manuale, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione.

Per quanto riguarda i documenti antecedenti il 2022, l'Ente utilizza un Conservatore diverso da quelli indicati negli allegati sopra descritti. Queste specifiche si trovano nell'**Allegato 9.2**

## 66. Responsabile della conservazione

Come precisato al par. 5 del presente Manuale, l'ente ha individuato un'unica figura Responsabile della gestione e della conservazione dei documenti informatici. Nella presente parte del Manuale sono indicati funzioni e compiti del Responsabile nella veste di Responsabile della Conservazione.

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD (DPO) dell'Ente. In particolare, il Responsabile:

a) esegue il monitoraggio in merito al corretto funzionamento del sistema di conservazione dei documenti informatici, provvedendo altresì a segnalare tempestivamente al conservatore gli eventuali guasti e le proposte di miglioramento del sistema medesimo;

b) provvede, sotto il profilo organizzativo e gestionale, ad assicurare l'interfacciamento e il collegamento con il sistema di conservazione digitale dei documenti informatici.

c) cura il rapporto con il Conservatore individuato, verificando, anche per mezzo di personale espressamente delegato, il corretto svolgimento dell'attività di conservazione.

Il Responsabile, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

### 67. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati e acquisiti dall'Ente e i rispettivi metadati, conformi all'allegato 5 alle Linee guida dell'AgID;
- i fascicoli informatici dell'Ente e rispettivi metadati, conformi all'allegato 5 alle Linee guida dell'AgID;
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dall'Ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie di documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel manuale utente del Sistema di gestione documentale e nel Manuale del Conservatore.

## 68. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'**allegato 2 alle Linee guida dell'AgID**. Prima di individuare un formato tra quelli versati in conservazione occorre dunque verificare che sia tra quelli ivi menzionati e che non vi siano raccomandazioni contrarie all'utilizzo per la conservazione.

Il Responsabile della conservazione, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal Responsabile attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Seconda del presente Manuale.

## 69. Modalità e tempi di trasmissione dei pacchetti di versamento

All'inizio di ogni anno ciascuna UO individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al Responsabile della conservazione, che provvede alla formazione e alla trasmissione dei pacchetti di versamento, secondo le modalità operative definite nel manuale del Conservatore e nei documenti tecnici sull'affidamento del servizio.

Il Responsabile della conservazione genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il Responsabile della conservazione verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, richiede al produttore dell'oggetto di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento annuale, per cui ogni anno entro il mese di febbraio sono versati in conservazione tutti i documenti informatici dell'Ente, anche a fascicolo aperto;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti;
- versamento anticipato, nelle particolari ipotesi che richiedono un versamento in conservazione prima del versamento a cadenza annuale (ad esempio, documenti con certificato di firma in scadenza).

## 70. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica (archivio corrente)

La memorizzazione dei documenti correnti è effettuata in *cloud*, nel repository del Sistema di gestione documentale, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore o della selezione per lo scarto.

## 71. Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati dal RC possono accedere al Sistema tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati e le configurazioni specifiche adottate.

## 72. Selezione e scarto dei documenti

Periodicamente, secondo quanto previsto nel piano di conservazione dell'archivio (v. **Allegato 7**), viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale.

In particolare, l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione del Conservatore e trasmesso al RC dell'ente, il quale verifica il rispetto dei termini temporali stabiliti dal Piano di conservazione.

Gli archivi dell'ente sono archivi pubblici, pertanto, ai sensi della normativa vigente in materia di beni culturali, per procedere allo scarto deve essere richiesta autorizzazione alla competente Soprintendenza. Le proposte di scarto di pacchetti di archiviazione contenenti documenti e/o dati sottratti alla libera consultabilità devono essere altresì autorizzate dal Ministero dell'interno.

Il RC, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

Le modalità operative per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Manuale del Conservatore (v. **Allegato 9**). L'operazione di scarto viene tracciata sul sistema mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

## 73. Conservazione, selezione e scarto dei documenti analogici

La documentazione analogica corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

I documenti analogici dell'Amministrazione sono conservati nei locali dell'Amministrazione: depositi di archivio corrente presso i rispettivi uffici, archivio di deposito presso l'archivio al 2° piano e nei locali nel seminterrato.

Il Responsabile della gestione documentale cura il versamento nell'archivio di deposito delle unità archivistiche non più utili per la trattazione degli affari in corso, individuate dagli uffici produttori. I fascicoli non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge, per poi essere trasferiti nell'archivio storico per la conservazione permanente. Delle operazioni di trasferimento deve essere lasciata traccia documentale.

Periodicamente il Responsabile Gestionale in collaborazione con il Responsabile archivistico valuta l'opportunità, anche sotto il profilo economico, di provvedere al riversamento in formato digitale di tutti o parte dei documenti analogici presenti negli archivi.

### 74. Misure di sicurezza e monitoraggio del sistema di conservazione

Il Manuale di conservazione e il piano della sicurezza del Conservatore descrivono le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti previsti nell'atto di affidamento del servizio.

# PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

### 75. Sicurezza dei sistemi informatici dell'ente

Gli strumenti software del Sistema informatico di gestione documentale, utilizzati per la formazione e gestione dei documenti informatici, sono resi accessibili al personale dell'Ente tramite servizi cloud (SaaS) qualificati dall'Agenzia per l'Italia Digitale.

Ciascun servizio consente altresì l'archiviazione dei documenti, prodotti mediante l'utilizzo dell'applicativo, nel rispetto degli standard di sicurezza previsti dalla normativa, garantendone così l'integrità e l'immodificabilità ai sensi delle Linee guida (cfr. par. 2.1.1. e 3.9).

La memorizzazione dei documenti correnti, diversi da quelli formati con l'ausilio dei suddetti strumenti software, è effettuata sui server dell'ente, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore, o della selezione per lo scarto.

## 76. Amministratore di sistema

Il ruolo di Amministratore del Sistema di gestione documentale è svolto dal RGD. Il personale delegato svolge i compiti operativi relativi alla gestione delle abilitazioni di accesso di cui al **par. 7** (quali il rilascio, la revoca, l'attribuzione di particolari privilegi, ecc.), previa autorizzazione del RGD, in base alle richieste dei responsabili di servizio.

## 77. Uso del profilo utente per l'accesso ai sistemi informatici

La gestione degli utenti abilitati ad accedere al protocollo informatico, in base alla pianta organica dell'ente e sulla base delle indicazioni dei responsabili competenti**,** è affidata all'Ufficio Protocollo.

In particolare, per l'accesso ai sistemi informatici dell'Ente è necessaria l'assegnazione di un profilo utente formalmente autorizzata dal Responsabile.

Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password temporanea. Al primo accesso dell'utente, viene richiesto l'inserimento di una nuova password, mentre lo username resta invariato. Le richieste concernenti il recupero delle credenziali devono essere effettuate per iscritto al RGD, che le accetta con formale comunicazione.

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali. Ciascun dipendente deve associare al proprio profilo una password di almeno otto cifre, che preveda almeno una lettera maiuscola, una lettera minuscola, un numero e un segno (ad esempio: #, !, ?, -, &, ecc.). La password non deve mai coincidere con altre password associate ad altri profili o utenze (ad esempio, non si deve usare la stessa password del proprio account email personale).

Il Sistema è configurato in modo che a cadenza periodica per ogni profilo utente sia richiesto il rinnovo della password.

## 78. Accesso alle postazioni di lavoro, ai locali e agli archivi dell’Ente

L’accesso alle postazioni di lavoro è consentito esclusivamente al personale degli uffici ed ai soggetti terzi regolarmente autorizzati (ad es., per necessità connesse a esigenze di manutenzione, interventi tecnici, consegne di forniture, ecc.).
L'archivio storico dell’Ente è collocato nella sede provinciale, in locali opportunamente chiusi al pubblico, le cui chiavi di accesso sono custodite dall'archivista (in via esclusiva). L'accesso al medesimo è consentito, previo appuntamento, per finalità di lettura, studio e ricerca. La consultazione avviene esclusivamente in presenza dell'archivista.