



**MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE  
DEL COMUNE DI ALBUGNANO**

*Approvato con Delibera Giunta Comunale n. 34 del 30/06/2025*

## INFORMAZIONI GENERALI

Titolo	Manuale di gestione e conservazione documentale del Comune di Albugnano
Versione	“Manuale di gestione e conservazione documentale” (Deliberazione della Giunta Comunale n. 134 del 26 giugno 2025)
Aggiornamenti al Manuale	I successivi aggiornamenti del Manuale devono essere sottoposti all’approvazione della Giunta Comunale.
Distribuzione	All’interno dell’Amministrazione nel sito web del Comune nella sezione “Amministrazione Trasparente”

## **SOMMARIO**

### **PARTE PRIMA - DISPOSIZIONI GENERALI, ORGANIZZAZIONE E RESPONSABILITÀ**

1. Riferimenti normativi e definizioni
2. Ambito di applicazione
3. Servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali
4. Area organizzativa omogenea e unità organizzative
5. Responsabile della gestione documentale

### **PARTE SECONDA - SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI**

6. Sistema informatico di gestione documentale del Comune
7. Requisiti tecnologici e funzionali
8. Ufficio protocollo e UUOO responsabili delle attività di protocollazione
9. Gestione degli accessi

### **PARTE TERZA - FORMAZIONE DEI DOCUMENTI**

#### *SEZIONE PRIMA - MODALITÀ DI FORMAZIONE*

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

#### *SEZIONE SECONDA - DISPOSIZIONI COMUNI A TUTTE LE MODALITÀ DI FORMAZIONE*

19. Dispositivi di firma elettronica
20. Scadenza dei certificati di firma
21. Identificazione univoca del documento informatico
22. Associazione degli allegati al documento principale
23. Accessibilità del documento informatico
24. Metadati del documento informatico
25. Immodificabilità e integrità del documento informatico

*SEZIONE TERZA - DISPOSIZIONI SULLA FORMAZIONE DI DOCUMENTI ANALOGICI*

- 26. Copie analogiche di documenti informatici
- 27. Casi in cui è ammessa la formazione o l'acquisizione di documenti originali analogici

**PARTE QUARTA - GESTIONE DOCUMENTALE**

*SEZIONE PRIMA - FLUSSI DOCUMENTALI ESTERNI*

- 28. Ricezione telematica di documenti informatici in entrata
- 29. Canali di ricezione
- 30. Formati accettati
- 31. Verifica sul formato dei documenti allegati
- 32. Controllo dei certificati di firma
- 33. Trasmissione telematica di documenti informatici in uscita
- 34. Individuazione del domicilio digitale presso cui effettuare la comunicazione
- 35. Modalità di consultazione ed estrazione dei domicili digitali presso cui effettuare la comunicazione
- 36. Disposizioni sulla formazione di documenti analogici

*SEZIONE SECONDA - FLUSSI DOCUMENTALI INTERNI*

- 37. Assegnazione dei documenti in entrata agli uffici
- 38. Comunicazioni interne
- 39. Pubblicazioni nell'Albo Pretorio e in Amministrazione Trasparente

*SEZIONE TERZA - PROTOCOLLO INFORMATICO*

- 40. Sistema di protocollo informatico
- 41. Funzioni del responsabile della gestione documentale in materia di protocollo informatico
- 42. Registro generale di protocollo
- 43. Registro giornaliero di protocollo
- 44. Documenti soggetti a registrazione di protocollo e documenti esclusi
- 45. Protocollo di documenti interni
- 46. Disposizioni per particolari tipologie di documenti
- 47. Registrazione di protocollo
- 48. Modalità di registrazione
- 49. Protocollo delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione
- 50. Annullamento e modifiche della registrazione di protocollo
- 51. Gestione degli allegati
- 52. Informazioni agli utenti rese dal responsabile del procedimento
- 53. Tempi di registrazione e casi di differimento
- 54. Segnatura di protocollo
- 55. Protocollo riservato
- 56. Registro di emergenza

57. Documenti soggetti a registrazione particolare

*SEZIONE QUARTA - DISPOSIZIONI SULLA PROTOCOLLAZIONE E GESTIONE  
DEI DOCUMENTI ANALOGICI*

58. Protocollazione dei documenti analogici

59. Registrazione, segnatatura, annullamento

60. Corrispondenza contenente dati sensibili

61. Corrispondenza personale o riservata

62. Corrispondenza cartacea non di competenza dell'Amministrazione

*SEZIONE QUINTA - CLASSIFICAZIONE E FASCICOLAZIONE*

63. Classificazione dei documenti

64. Fascicolazione informatica dei documenti

**PARTE QUINTA - TENUTA E CONSERVAZIONE DEI DOCUMENTI**

65. Sistema di conservazione dei documenti informatici

66. Responsabile della conservazione

67. Oggetti della conservazione

68. Formati ammessi per la conservazione

69. Modalità e tempo di trasmissione dei pacchetti di versamento

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

71. Accesso al Sistema di conservazione

72. Selezione e scarto dei documenti

73. Conservazione, selezione e scarto dei documenti analogici

74. Misure di sicurezza e monitoraggio del sistema di conservazione

**PARTE SESTA - SICUREZZA E PROTEZIONE DEI DATI PERSONALI**

75. Sicurezza dei sistemi informatici del Comune

76. Amministratore di sistema

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

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

## ELENCO DEGLI ALLEGATI

<b>NUMERO ALLEGATO</b>	<b>DENOMINAZIONE DELL'ALLEGATO</b>
Allegato 1	Allegato 1 - Definizioni
Allegato 2	Allegato 2 - Organigramma con indicazione delle UUOO
Allegato 3	Allegato 3 - Atto di nomina del Responsabile per la gestione e la conservazione documentale con Vicario
Allegato 4	Allegato 4 - Manuale Operativo del Software
Allegato 5	Allegato 5 - Guida pratica creazione documento accessibile
Allegato 6	Allegato 6 - Piano di classificazione Titolario
Allegato 7	Allegato 7 - Linee guida alla fascicolazione
Allegato 8	Allegato 8 - Piano di conservazione
Allegato 9	Allegato 9 - Manuale di conservazione del Conservatore
Allegato 10	Allegato 10 - Modello registro d'emergenza
Allegato 11	Allegato 11 - Sistema informatico di gestione
Allegato 12	Allegato 12 - Formati dei documenti
Allegato 13	Allegato 13 - Le raccomandazioni Alba

# **PARTE PRIMA**

## **DISPOSIZIONI GENERALI, ORGANIZZAZIONE E RESPONSABILITÀ**

### **1. Riferimenti normativi e definizioni**

Il presente Manuale di gestione documentale (da ora in poi solo “Manuale”) è stato adottato in conformità con le Linee guida sulla formazione, gestione e conservazione dei documenti informatici (da ora in poi solo “Linee guida”), emanate dall’Agenzia per l’Italia Digitale con la determinazione del Direttore generale n. 407 del 9 settembre 2020 e pubblicate il 10 settembre 2020, successivamente modificate con la determinazione n. 371 del 17 maggio 2021.

Parte integrante delle Linee Guida sono i sei allegati che includono disposizioni riguardanti:

1. Glossario dei termini e degli acronimi: Fornisce una definizione chiara e precisa dei termini tecnici utilizzati nel contesto della gestione documentale, facilitando la comprensione e l’applicazione delle Linee guida;
2. Formati di file e riversamento: Specifica i formati di file accettabili per la conservazione a lungo termine dei documenti digitali e le procedure per il riversamento dei dati, garantendo l’integrità e l’accessibilità nel tempo;
3. Certificazione di processo: Descrive i requisiti per la certificazione dei processi di gestione documentale, assicurando che le procedure adottate siano conformi agli standard di qualità e sicurezza;
4. Standard e specifiche tecniche: Elenca gli standard tecnici e le specifiche che devono essere seguiti per garantire l’interoperabilità e la compatibilità dei sistemi di gestione documentale;
5. Metadati: Definisce i metadati necessari per la catalogazione e la ricerca dei documenti, migliorando l’efficienza nella gestione e nel recupero delle informazioni;
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati: Sostituisce la circolare 60 dell’AgID e stabilisce le modalità di comunicazione tra le Aree Organizzative Omogenee (AOO) per la gestione dei documenti amministrativi protocollati.

Come indicato nell’elenco il glossario si trova all’interno dell’Allegato 1 delle Linee Guida, ma in allegato (Allegato 1) al presente manuale si trova solo l’elenco

specifico delle definizioni effettivamente utilizzate nella redazione di questo documento al fine di agevolare la consultazione.

Altre norme rilevanti per la gestione documentale sono:

- Codice dell'Amministrazione Digitale (CAD): Le disposizioni sulla formazione dei documenti informatici, anche amministrativi, e sulla digitalizzazione dell'attività amministrativa, come previsto dal d.lgs. 7 marzo 2005, n. 82. Il CAD rappresenta il quadro normativo di riferimento per la digitalizzazione della Pubblica Amministrazione in Italia;
- Testo Unico sulla Documentazione Amministrativa (TUDA): Le disposizioni sulla documentazione amministrativa, come stabilito dal D.P.R. 28 dicembre 2000, n. 445. Il TUDA regola la formazione, gestione e conservazione dei documenti amministrativi;
- Norme sul procedimento amministrativo: Le norme sul procedimento amministrativo, come definite dalla l. 7 agosto 1990, n. 241, che disciplinano il processo decisionale delle amministrazioni pubbliche e il diritto di accesso ai documenti amministrativi;
- Disposizioni sulla trasparenza: Le disposizioni sulla trasparenza, come indicate nel d.lgs. 14 marzo 2013, n. 33, che promuovono la pubblicità, la trasparenza e la diffusione delle informazioni da parte delle pubbliche amministrazioni;
- Regolamento eIDAS: Le disposizioni sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno, come stabilito dal Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014;
- Regolamento generale sulla protezione dei dati (GDPR): Le disposizioni sulla protezione dei dati personali, come previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, e dal d.lgs. 30 giugno 2003 n. 196. Il GDPR stabilisce le norme per la tutela della privacy e la protezione dei dati personali nell'Unione Europea.

## **2. Ambito di applicazione**

Il presente Manuale, ai sensi del paragrafo 3.5 delle Linee Guida, descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici. Fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Nello specifico il manuale riporta le fasi di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti informatici inviati, ricevuti e ad uso interno. Descrive



inoltre le modalità di produzione e di accesso ai documenti informatici con riferimento alla sicurezza e alla protezione dei dati personali.

L'adozione del Manuale risponde ad esigenze pratico-operative e deve essere sottoposto ad aggiornamenti, in un contesto in continua evoluzione tecnologica.

Il manuale è un documento interno a disposizione di tutto il personale dell'Amministrazione, deve essere adottato con un provvedimento formale e deve essere pubblicato sul sito istituzionale, in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art.9 del D. Lgs 33/2013.

Le indicazioni riportate all'interno del Manuale si applicano per la gestione dei documenti del Comune e quindi dell'Area organizzativa omogenea.

### **3. Servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali**

Il servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi è fondamentale per la gestione efficiente dei documenti. Questo servizio è regolato dall'art. 61 del DPR 445/2000 e prevede l'istituzione di un'area organizzativa omogenea (da ora in avanti "AOO") per garantire la corretta gestione dei documenti, sia cartacei che digitali. Il Responsabile della gestione documentale (da ora in avanti "Responsabile" o "RGD") ha il compito di supervisionare tutte le fasi del ciclo di vita dei documenti, dall'acquisizione alla conservazione, assicurando che siano rispettate le normative vigenti.

### **4. Area organizzativa omogenea e unità organizzative**

Il Comune di Albugnano si configura come unica Area Organizzativa Omogenea (da ora in poi anche solo "AOO"), con il codice IPA c\_c704, denominazione "Amministrazione Comune di Albugnano" (codice univoco AOO AA5CC1E).

L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice IPA. Le Unità Organizzative (da ora in poi solo UUOO) che afferiscono alla AOO sono riportate nell'organigramma di cui all'Allegato 2, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa del Comune.

### **5. Responsabile della gestione documentale**

Il Comune di Albugnano, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato il "Responsabile della gestione documentale" ai sensi del par. 3.4 delle Linee Guida AgID in materia di formazione,

gestione e conservazione dei documenti informatici. Figura dotata di competenze giuridiche, informatiche e archivistiche a cui affidare le funzioni e i compiti previsti dalla normativa vigente. Il Responsabile della gestione documentale del Comune di Albugnano è stato individuato con decreto del Sindaco. In caso di vacanza o assenza, è stato altresì nominato il vicario del Responsabile (Allegato 3).

Al RGD sono affidati i seguenti compiti:

- 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 del Comune;
- provvede, d'intesa con il Responsabile della conservazione 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;
- monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
- assicura, d'intesa con il Responsabile della Conservazione, la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione;
- valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
- vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo;
- assicura la corretta produzione e conservazione del registro giornaliero di protocollo, autorizzando le operazioni di annullamento delle registrazioni in caso di errori;
- assicura l'elaborazione e l'aggiornamento del Piano di classificazione dei documenti, del Piano di conservazione e del Piano di organizzazione delle aggregazioni documentali (il Piano di fascicolazione);
- 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. Assicura quindi la predisposizione di un piano per la sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio e accesso ai documenti informatici;
- effettua un periodico censimento degli strumenti software di gestione documentale in uso presso il Comune 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, fermo restando la propria responsabilità, può delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

## **PARTE SECONDA**

### **SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI**

#### **6. Sistema informatico di gestione documentale del Comune**

Il Comune, per la gestione documentale si avvale di un apposito sistema software gestionale (da adesso in poi “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, strumenti web di acquisizione delle istanze online, scansioni nei casi di consegna allo sportello;
- sistema di workflow per l’assegnazione, lo scambio e la lavorazione dei documenti da parte degli uffici;
- creazione e gestione dei fascicoli informatici;
- pubblicazione degli atti in albo pretorio e nella sezione amministrazione trasparente del sito istituzionale dell’Ente (sezione all’interno di amministrazione trasparente “Bandi di gara e contratti”).

#### **7. Requisiti tecnologici e funzionali**

La descrizione dettagliata delle componenti e delle funzionalità dei software di cui si compone il Sistema è disponibile nel Manuale Operativo di cui all’Allegato 4 al presente Manuale.

#### **8. Ufficio protocollo e UUOO responsabili delle attività di protocollazione**

##### **I protocolлисти dei vari**

Tutti i dipendenti a cui è assegnata un’utenza per l’abilitazione di accesso al Sistema di gestione documentale del Comune sono abilitati alla protocollazione informatica dei documenti in uscita (con esclusione degli utenti a cui sono attribuite funzioni di mera consultazione).

La protocollazione dei documenti informatici in entrata è, invece, curata innanzitutto dal personale dell’Ufficio Anagrafe.

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 del Comune si rinvia alle indicazioni contenute nella Parte Quarta del presente Manuale.

## **9. Gestione degli accessi**

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.

Il sistema registra e storicizza ogni operazione effettuata sul sistema stesso, con l'indicazione dell'autore per permettere di verificare e di risalire a tutte le operazioni eseguite.

# **PARTE TERZA FORMAZIONE DEI DOCUMENTI**

## ***SEZIONE PRIMA - MODALITÀ DI FORMAZIONE***

### **10. Modalità di formazione dei documenti informatici**

I documenti informatici del Comune sono formati in originale come documenti informatici. I documenti informatici degli uffici dell'Ente sono formati mediante una delle seguenti modalità:

- creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati (cioè, mediante il ricorso a programmi di scrittura, quali, a mero titolo esemplificativo, quelli inclusi nelle suite Office o simili e mediante l'utilizzo delle funzioni dei sistemi di gestione documentale.
- acquisizione:
  - della copia per immagine di un documento analogico su supporto informatico (per esempio mediante scansione di un documento cartaceo);
  - della copia informatica di un documento analogico (per esempio con l'acquisizione del documento tramite lettore OCR);
  - del duplicato di un documento informatico per via telematica o da supporto informatico (per esempio mediante download da posta elettronica oppure mediante l'utilizzo della funzione del sistema operativo "duplica");

- 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 (per esempio la memorizzazione dei dati immessi in un form reso disponibile online agli utenti;
- generazione o raggruppamento anche in via automatica di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (per esempio la generazione del registro di protocollo giornaliero).

Di seguito sono fornite le indicazioni specifiche per ciascuna delle modalità indicate.

## **11. Creazione e redazione tramite software di documenti informatici**

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

Ad esempio: suite Microsoft Office.

Il testo del documento informatico creato dagli uffici del Comune deve essere redatto utilizzando uno dei font:

Arial, Helvetica, Trebuchet, Verdana, Times new Roman e Calibri.

## **12. Elementi essenziali del documento amministrativo informatico**

Ogni documento amministrativo informatico creato e redatto dal Comune deve recare i seguenti elementi:

- denominazione dell'Amministrazione;
- Autore e ufficio responsabile;
- Oggetto del documento;
- Riferimento al procedimento o al fascicolo;
- Sottoscrizione;
- Data e luogo;
- Numero di pagina;
- Indicazione degli allegati (se presenti);
- Identificazione e dati dei destinatari (se si tratta di documenti in uscita);
- Dati dell'Amministrazione (compresi codice fiscale, indirizzo e recapiti, se si tratta di documenti in uscita);
- Mezzo di spedizione (se si tratta di documenti in uscita).

(Allegato 14 al presente manuale - Carta intestata).

### **13. Scelta del formato e modalità di sottoscrizione**

Il formato del documento informatico creato dal Comune deve essere scelto tra i seguenti formati standard: .pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods.

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 con firma PADES altrimenti CADES. Si precisa che, dal punto di vista giuridico, entrambe le tipologie di firma (CADES e PADES) sono idonee a garantire l'autenticità dei documenti informatici sottoscritti.

Il tipo di firma PADES è integrato direttamente nel documento PDF, invece il tipo di firma CADES (.p7m) è utilizzato quando è necessario firmare i documenti in formati diversi dal PDF.

### **14. 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 assicurare 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. parr. 15 e 16).

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.

## **15. Copie per immagine di documenti analogici**

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia (Art. 22 del CAD).

Di norma, i documenti cartacei trasmessi al Comune 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 digitale, 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:

- 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;

- 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;
- 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.

## **16. 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.

## **17. Acquisizione di istanze tramite moduli online**

Le istanze provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e form messi a disposizione dal Comune attraverso gli sportelli telematici, resi accessibili previa identificazione dell’utente con gli strumenti di identificazione SPID, CIE o CNS.

I dati immessi dall’istante sono memorizzati su supporto informatico. Le istanze e le dichiarazioni così formate costituiscono a tutti gli effetti documenti amministrativi informatici, acquisiti in interoperabilità dal Sistema di protocollo informatico e trattati come documenti in entrata soggetti a registrazione di protocollo (protocollazione automatica), secondo le modalità definite nella Parte Quarta del presente Manuale.

## **18. Formazione di registri e repertori**

I registri e i repertori tenuti dal Comune, 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 di repertori come documento originale analogico.

# ***SEZIONE SECONDA - DISPOSIZIONI COMUNI A TUTTE LE MODALITA' DI FORMAZIONE***

## **19. Dispositivi di firma elettronica**

Il Comune stabilisce che per le posizioni organizzative, ai dirigenti ed ai delegati con potere di firma 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.

## **20. 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.

## **21. 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. L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.

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 del Comune. 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).

## **22. 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 devono essere associati i seguenti metadati: il numero degli allegati;

- l'indice degli allegati;
- l'identificativo del documento allegato (IdDoc);
- il titolo dell'allegato (la sua descrizione).

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

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 imm modificabile (per esempio dopo l'apposizione della firma digitale).

## **23. 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.

## **24. 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.

## **25. Immodificabilità e integrità del documento informatico**

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

il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

L’immodificabilità e l’integrità dei documenti informatici sono garantite con differenti operazioni in base alla modalità di formazione dei documenti stessi:

1. Per i documenti informatici formati con l'utilizzo di strumenti software o servizi cloud qualificati:

mediante l'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al paragrafo 3.9 delle Linee Guida "Misure di sicurezza"; il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale; attraverso il versamento ad un sistema di conservazione.

2. Per i documenti informatici formati mediante acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico:

apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo

elettronico qualificato o firma elettronica avanzata; memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al paragrafo 3.9 delle Linee Guida "Misure di sicurezza"; versamento ad un sistema di conservazione.

3. Per i documenti informatici formati mediante memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente o mediante generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica:

apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema; produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Vediamo che il versamento nel sistema di conservazione è la modalità con la quale si possono avere più garanzie di immodificabilità e di 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.

Tra i compiti del responsabile della gestione documentale rientra quello di assicurare che i documenti informatici a cui è apposta una firma elettronica siano versati nel sistema di conservazione prima della scadenza del certificato di firma.

## ***SEZIONE TERZA - DISPOSIZIONI SULLA FORMAZIONE DI DOCUMENTI ANALOGICI***

### **26. Copie analogiche di documenti informatici**

Fermo restando l'obbligo di formare i documenti originali informatici, ai sensi dell'art. 3 - bis, comma 4- bis del CAD, in alcuni casi può essere necessario effettuare delle copie analogiche affinché siano spedite per posta ordinaria o raccomandata con avviso di ricevimento ai soggetti che non hanno un domicilio digitale, o se il domicilio digitale non è funzionante o non raggiungibile.

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 sottoscrittore.

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.: "La presente copia è tratta da documento informatico, predisposto come documento nativo digitale da [nome responsabile], Responsabile del procedimento [in alternativa, indicare Dirigente o Responsabile Ufficio]. Il documento originale informatico è archiviato nel sistema informatico del Comune, presso cui è disponibile per l'accesso").

Quando possibile, la dicitura deve essere integrata con indicazioni sulle modalità per effettuare l'accesso online al documento informatico.

## **27. 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:

- ai sensi dell'art.2 comma 6 del 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;
- 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;
- in tutti i casi in cui per legge o regolamento il documento deve essere formato e/o rilasciato in formato cartaceo.

## **PARTE QUARTA - GESTIONE DOCUMENTALE**

### **SEZIONE PRIMA - FLUSSI DOCUMENTALI ESTERNI**

## **28. 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 validi a tutti gli effetti di legge quando:

- sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;
- sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domiciliazione digitali previsti dalla normativa vigente;
- sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con sistemi SPID, CIE o CNS;

- 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;
- sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento di identità dell'autore;
- 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 (per esempio gli strumenti personali per il trasferimento dei file).

## **29. Canali di ricezione**

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

- [albugnano@cert.ruparpiemonte.it](mailto:albugnano@cert.ruparpiemonte.it)
- acquisizione di istanze, formate e trasmesse tramite gli sportelli telematici dei servizi online;
- altri canali di trasmissione indicati per specifici procedimenti.

Gli indirizzi di posta elettronica sono riportati nell'Indice delle Pubbliche Amministrazioni e pubblicizzati 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 del Comune 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. 34 sull'individuazione del domicilio digitale).

## **30. Formati accettati**

Sono accettati 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 espressa 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.

### **31. 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.

### **32. Controllo dei certificati di firma**

La Segreteria alla notifica della scadenza informa i Sistemi Informativi per poter procedere al rinnovo degli stessi.

### **33. 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.

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 trasmessi a mezzo PEC.

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

### **34. 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:

- se vi è stata elezione di domicilio digitale speciale per particolari atti, procedimenti o affari, all'indirizzo PEC espressamente dichiarato dal cittadino;
- 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](http://domiciliodigitale.gov.it). La consultazione e l'estrazione automatica dei domicili digitali deve essere effettuata con le modalità di cui al paragrafo successivo;
- 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 all'interno 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](http://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](http://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 dei termini di legge o, comunque, quando il suo contenuto impegni il Comune verso l'esterno, la trasmissione è sempre effettuata via PEC.

### **35. Modalità di consultazione ed estrazione dei domicili digitali presso cui effettuare la comunicazione**

Gli elenchi pubblici INAD, INI-PEC e IPA sono liberamente consultabili e non è richiesta l'autenticazione da parte dell'utente.

### **36. Disposizioni dei documenti analogici**

I documenti su supporto analogico possono pervenire al Comune attraverso:

- il servizio postale;
- la consegna diretta all'Ufficio Protocollo

L'Ufficio Protocollo, a sua volta, effettua lo smistamento ai vari uffici. Se necessario avviene la protocollazione e successivamente il documento originale con l'etichetta



del protocollo viene inserito nella cassettona dell'ufficio di competenza.

## **SEZIONE SECONDA - FLUSSI DOCUMENTALI INTERNI**

### **37. Assegnazione dei documenti in entrata agli uffici**

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

In particolare, sono assegnati in modo automatico alle UO competenti i documenti acquisiti tramite lo sportello telematico.

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" e "per conoscenza".

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

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

### **38. 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 del Comune è effettuato principalmente per mezzo di posta elettronica ordinaria, mediante protocollo interno.

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

### **39. 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 solo dopo che il documento sia divenuto immodificabile (cfr. par. 26 del presente Manuale).

Tutti gli atti prodotti dal Comune 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.

## **SEZIONE TERZA - PROTOCOLLO INFORMATICO**

### **40. Sistema di protocollo informatico**

I Comune, per la protocollazione dei documenti, utilizza un Sistema di protocollo informatico integrato con il Sistema di gestione documentale.

È vietata l'acquisizione o la trasmissione di documenti soggetti a protocollazione e relativi allegati tramite canali diversi da quelli messi a disposizione dal Comune.

#### **41. 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, come Responsabile del protocollo informatico:

- coordina la gestione del Sistema di protocollo informatico;
- assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
- esercita il controllo generale sui flussi documentali esterni e interni;
- assicura la corretta esecuzione delle attività di protocollazione; garantisce lo svolgimento delle operazioni di registrazione e segnatura di protocollo nel rispetto della normativa vigente;
- garantisce la corretta produzione e conservazione del registro giornaliero di protocollo;
- autorizza l'attivazione del protocollo di emergenza;
- autorizza con comunicazione formale le operazioni di annullamento o di differimento delle registrazioni di protocollo;
- 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.

#### **42. Registro generale di protocollo**

Il registro di protocollo si qualifica come atto pubblico di fede privilegiata e come strumento di organizzazione oltre che archivistico.

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

La numerazione si chiude il 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo è costituito da almeno sette cifre numeriche, un codice numerico generato automaticamente dal sistema e associato in modo univoco e imm modificabile al documento.

Non è consentita la protocollazione di un documento già protocollato.

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.

Il registro è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendo quindi l'immodificabilità del contenuto.

Nella fase di versamento nel sistema di conservazione, l'immodificabilità del contenuto del registro è garantita attraverso la sottoscrizione con la firma digitale del

Responsabile della gestione documentale, oppure con le soluzioni tecnologiche riportate all'interno del manuale di conservazione e nel contratto stipulato dall'ente con il conservatore.

#### **43. Documenti soggetti a registrazione di protocollo e documenti esclusi**

Tutti i documenti prodotti e ricevuti dal Comune, indipendentemente dal supporto sui quali sono formati, sono registrati al protocollo.

Eccezione sono i documenti che ai sensi dell'articolo 53 DPR 445/2000 non sono soggetti a registrazione di protocollo:

- le Gazzette Ufficiali, i Bollettini Ufficiali e i notiziari della Pubblica Amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli 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.);
- i giornali, le riviste, i materiali pubblicitari, stampe varie, plichi di libri;
- i biglietti augurali, gli inviti a manifestazioni e tutti quei documenti d'occasione vari che non attivino procedimenti amministrativi;
- le bolle accompagnatorie;
- richiesta/invio di comunicazioni informali.

Inoltre, non sono soggetti a protocollazione obbligatoria, gli atti e i documenti già soggetti a registrazione particolare dell'Amministrazione e quindi 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.

#### **44. Protocollo 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.

è consentito lo scambio di documenti interni sottoscritti con firma autografa ciò qualora necessario per impossibilità di trasporre in forma digitale i documenti stessi. In questa ipotesi il documento interno formale può essere di tipo analogico e lo scambio deve aver luogo con apposite funzioni del sistema di protocollo informatico e gli eventuali allegati cartacei possono essere consegnati con mezzi tradizionali all'interno dell'Amministrazione.

Per i documenti interni informali, la cui conservazione è facoltativa, vale quanto specificato ad eccezione dell'obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

#### **45. 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 direttamente all'interno del portale, che consente di effettuare tutte le operazioni relative alla gestione dei documenti e all'attribuzione del protocollo informatico con modalità automatizzate.

#### **46. 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, DPR 445/2000, i metadati della 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 o, in alternativa, il destinatario o i destinatari per i documenti spediti;
- d. oggetto del documento. Tale metadato deve essere valorizzato in conformità alla normativa;
- e. data e protocollo del documento ricevuto, se disponibili;
- f. l'impronta del documento informatico, se trasmesso per via telematica. L'impronta è costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto.

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

- tipologia di documento;
- classificazione (titolo e classe) sulla base del Titolario (v. allegato 6);
- fascicolo di appartenenza;
- assegnazione interna (per competenza o per conoscenza);
- data e ora di arrivo;
- allegati (se presenti). Tale metadato deve essere valorizzato in conformità alla normativa;
- livello di riservatezza;
- mezzo di ricezione o invio;
- annotazioni;
- (eventualmente) estremi del provvedimento di differimento della registrazione;
- (se necessario) elementi identificativi del procedimento amministrativo.

#### **47. 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.

#### **48. Protocollo 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 messaggio in entrata e a inoltrarlo in allegato all'indirizzo di posta ordinaria del SP, 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 che nella comunicazione è stato indicato anche il recapito PEC. In tali casi, infatti, non serve provvedere all'inoltro per la protocollazione.

#### **49. 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 dalla normativa.

## **50. 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.

## **51. 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 dal Comune.

## **52. 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 del Comune, 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.

### **53. Segnatura di protocollo**

La segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

Le operazioni di segnatura sono effettuate nell'ambito delle fasi di processamento della registrazione di protocollo, come indicare al precedente par. 47.

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 loro identificazione univoca e certa, come indicato all'art. 53, comma 1, TUDA.

I requisiti necessari di ciascuna segnatura di protocollo sono:

- indicazione della Amministrazione mittente;
- codice identificativo dell'AOO mittente;
- codice identificativo del registro;
- numero progressivo di protocollo;
- data di registrazione;
- oggetto del messaggio di protocollo;
- classificazione del messaggio di protocollo;
- indicazione del fascicolo in cui è inserito il messaggio di protocollo.



L'acquisizione dei documenti cartacei in formato immagine è effettuata solo dopo che l'operazione di segnatura di protocollo è stata eseguita in modo da acquisire con l'operazione di scansione, come immagine, anche il segno sul documento; in tali casi il segno deve essere apposto sulla prima pagina dell'originale.

Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, il file di segnatura può includere tutte le informazioni di registrazione del documento:

- l'oggetto;
- il mittente;
- il destinatario o i destinatari.

Per i documenti informatici trasmessi ad 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").

#### **54. 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 ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato del Comune, 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.

## **55. 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. Il Responsabile del servizio per la tenuta del protocollo informatico autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza. 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 al SP.

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.

Il Responsabile provvede alla formazione del registro di emergenza su supporto analogico, redatto secondo lo schema di cui all'Allegato 10 al presente Manuale.

## **56. Documenti soggetti a registrazione particolare**

Il Comune ha provveduto all'unificazione dei repertori e registri di settore, prevedendo il ricorso al registro di protocollo informatico per tutti i documenti dell'ente.

Ferma restando la registrazione al protocollo informatico, si provvede altresì alla registrazione particolare in appositi repertori dei seguenti atti adottati dagli organi politico amministrativi dell'ente:

- degli atti soggetti a vidimazione

## **SEZIONE QUARTA**

### **DISPOSIZIONI SULLA PROTOCOLLAZIONE E GESTIONE DEI DOCUMENTI ANALOGICI**

#### **57. Protocollo dei documenti analogici**

Il personale addetto ad effettuare la registrazione di protocollo informatico in entrata è competente anche per la protocollazione dei documenti analogici in entrata.

#### **58. 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". Si rinvia al settore di competenza la specifica relativa alla regolarizzazione della richiesta o della comunicazione.

Per i documenti analogici la segnatura è apposta con timbro ed etichetta.

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".

#### **59. Corrispondenza contenente dati sensibili**

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansati 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.

#### **60. 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.

#### **61. Corrispondenza cartacea non di competenza dell’Amministrazione**

Qualora pervenga, tramite posta tradizionale, un documento cartaceo che non è evidentemente indirizzato al Comune (es. altro destinatario), lo stesso 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 QUINTA CLASSIFICAZIONE E FASCICOLAZIONE**

#### **62. Classificazione dei documenti**

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

#### **63. 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 i criteri previsti dalle Linee Guida alla fascicolazione di cui all’allegato 7.

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:

- 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;
- 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;
- 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;
- 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.

## **PARTE QUINTA**

### **TENUTA E CONSERVAZIONE DEI DOCUMENTI**

#### **64. Sistema di conservazione dei documenti informatici**

Il Comune, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, 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 qualificato 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, si rinvia al Manuale del Conservatore e agli ulteriori documenti tecnici.

Il sistema di conservazione viene erogato in modalità SaaS.

#### **65. Responsabile della conservazione**

Come precisato al par. 5 del presente Manuale, verifica come nel paragrafo del RGD 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:

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

## **66. 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:

- pacchetti di versamento;
- pacchetti di archiviazione;
- pacchetti di distribuzione.

Il pacchetto di versamento viene inviato dal Soggetto produttore al sistema di conservazione e presenta due elementi: file indice xml e oggetto - dati. Le modalità del versamento sono mediante interfaccia REST: previa autenticazione ed autorizzazione.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel Disciplinare tecnico e nel Manuale del Conservatore.

Nello specifico, le tipologie di documenti in conservazione sono:

Protocollo Informatico: registro di protocollo, email protocollo, documento protocollato;

- Atti amministrativi: delibera, determina, ordinanza;
- Contabilità finanziaria: fattura attiva, fattura passiva;
- Contratti;
- SUAP Documento.

La frequenza del trasferimento in conservazione è giornaliera, tranne per la tipologia "fattura

attiva e fattura passiva". In quest'ultimo caso la frequenza di trasferimento al sistema di conservazione è mensile.

#### **67. 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.

#### **68. Modalità e tempi di trasmissione dei pacchetti di versamento**

Il versamento dei documenti avviene secondo le seguenti tempistiche

- 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.

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

La memorizzazione dei documenti correnti viene effettuata su Cloud in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore o della selezione per lo scarto.

#### **70. Accesso al Sistema di conservazione**

Gli utenti espressamente autorizzati dal Responsabile 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. L'accesso al sistema avviene tramite la piattaforma Cohesion e richiede un processo di autenticazione forte. L'utente dovrà disporre di uno dei seguenti strumenti: PIN Cohesion, SPID, Carta Raffaello, TS- CNS abilitata, CNS, CIE.

#### **71. Selezione e scarto dei documenti**

Il sistema di conservazione permette di effettuare la procedura di selezione e scarto della documentazione.

Le modalità operative per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Manuale del Conservatore. 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.

## **72. 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. Il Responsabile 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 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, nel rispetto della normativa vigente.

## **73. 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.

# **PARTE SESTA**

## **SICUREZZA E PROTEZIONE DEI DATI PERSONALI**

## **74. Sicurezza dei sistemi informatici del Comune**

All'interno del Comune è presente un regolamento relativo ai sistemi informativi, l'utilizzo degli strumenti informatici e ICT, di internet e della posta elettronica.

## **75. Amministratore di sistema**

È compito dei responsabili di settore comunicare tempestivamente al Settore ICT eventuali



cambi di mansione dei dipendenti assegnati che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche o in generale ai sistemi ICT.

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

Ad ogni account è associato sempre un profilo che identifica le operazioni che è possibile eseguire all'interno dello specifico contesto operativo. Per la corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole: Le password sono personali e segrete e devono rispettare i criteri minimi previsti dai sistemi (es. lunghezza minima, presenza di caratteri speciali, ecc.), devono essere modificate periodicamente e possibilmente devono essere costituite da almeno un carattere numerico, almeno un carattere non alfabetico (caratteri speciali es. \$, \* , % ecc.), con lunghezza pari ad almeno dieci caratteri e non devono contenere riferimenti agevolmente riconducibili all'utente. Le password hanno, di norma, una durata massima configurabile da sistema. L'utente, dopo il primo accesso ai sistemi, provvederà a modificare la password che quindi non potrà essere nota a nessun altro e dovrà aver cura che nessuno possa anche accidentalmente venirne a conoscenza. L'utente è responsabile di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali.

Nel caso in cui si sospetti che una password abbia perso la sua riservatezza, l'utente provvederà ove possibile a modificarla personalmente, altrimenti provvederà a modificarla con il supporto dell'Amministratore di Sistema. È esplicitamente vietato, anche su richiesta o indicazione del titolare, utilizzare l'account e in generale le credenziali di accesso e quindi il profilo personale di altri soggetti per utilizzare qualunque sistema informativo, informatico o in ambito ICT. Nel caso l'utente venisse a conoscenza delle credenziali di accesso (account e password o altro sistema adottato) di un altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema competente.

#### **77. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Ente**

Le postazioni di lavoro sono accessibili mediante l'utilizzo di credenziali di identificazione informatica e sono protette, in caso di assenza anche temporanea, tramite la sospensione o il blocco della sessione di lavoro.

L'archivio corrente è collocato presso gli uffici. L'archivio di deposito e l'archivio storico sono collocati nelle strutture in gestione o di proprietà dell'ente.