



Comune di  
**San Miniato**

COMUNE DI SAN MINIATO  
MANUALE DI GESTIONE, FORMAZIONE E  
PROTOCOLLAZIONE DEI DOCUMENTI

# INDICE

## PARTE PRIMA

### PRINCIPI GENERALI E DISPOSIZIONI PRELIMINARI

Art. 1 – Riferimenti normativi

Art. 2 – Ambito di applicazione

## PARTE SECONDA

### ORGANIZZAZIONE

Art. 3 - Area Organizzativa Omogenea (AOO), Unità Organizzativa Responsabile (UOR)

Art. 4 - Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

Art. 5 – Sistema di protocollo informatico

Art. 6 - Unicità del protocollo informatico

Art. 7 Abilitazioni di accesso

Art. 8 – Soggetti delegati alle attività di protocollazione

Art.9 – Rilascio di abilitazioni di accesso

Art. 10 – Abilitazioni interne ad accedere al protocollo

Art. 11 – Ripristino delle credenziali private d'accesso

Art. 12 – Abilitazione alle registrazioni di protocollo riservato

## PARTE TERZA

### FORMAZIONE DEI DOCUMENTI

Art. 13 – Modalità di formazione dei documenti informatici

Art. 14 – Elementi essenziali del documento amministrativo informatico

Art. 15 – Tipologie di formato del documento informatico

Art. 16 – Copie per immagine di documenti analogici

Art. 17 – Duplicati, copie ed estratti informatici di documenti informatici

- Art. 18 – Dispositivi di firma elettronica
- Art. 19 – Scadenza dei certificati di firma
- Art. 20 – Identificazione univoca del documento informatico
- Art. 21 – Associazione degli allegati del documento principale
- Art. 22 – Accessibilità del documento informatico
- Art. 23 – Metadati del documento informatico
- Art. 24 – Immodificabilità e integrità del documento informatico
- Art. 25 – Copie analogiche di documenti informatici
- Art. 26 – Casi in cui è ammessa la formazione di documenti originali analogici

#### PARTE QUARTA

##### GESTIONE DOCUMENTALE

- Art. 27 – Ricezione telematica di documenti informatici in entrata
- Art. 28 – Canali di ricezione
- Art. 29 – Formati accettati
- Art. 30 – Verifica sul formato dei documenti allegati
- Art. 31 – Controllo dei certificati di firma
- Art. 32 – Trasmissione telematica di documenti informatici in uscita
- Art. 33 – Individuazione del domicilio digitale presso cui effettuare la comunicazione
- Art. 34 – Disposizioni sui documenti analogici
- Art. 35 – Documenti interni
- Art. 36 – Sistema di protocollo informatico
- Art. 37 – Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico
- Art. 38 – registro generale di protocollo
- Art. 39 – Registro giornaliero di protocollo

- Art. 40 – Documenti soggetti a registrazione di protocollo e documenti esclusi
- Art. 41 – Disposizioni per particolari tipologie di documenti
- Art. 42 – Registrazione di protocollo
- Art. 43 – Modalità di registrazione
- Art. 44 – Protocollazione delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione
- Art. 45 – Annullamento e modifiche della registrazione di protocollo
- Art. 46 – Gestione degli allegati
- Art. 47 – Tempi di registrazione e casi di differimento
- Art. 48 – Segnatura di protocollo
- Art. 49 – Protocollo riservato
- Art. 50 – Registro di emergenza
- Art. 51 – Documenti soggetti a registrazione particolare
- Art. 52 – Disposizioni sulla protocollazione e gestione dei documenti analogici
- Art. 53 – Registrazione, segnatura, annullamento
- Art. 54 – Corrispondenza personale o riservata
- Art. 55 – Corrispondenza cartacea non di competenza dell'Amministrazione
- Art. 56 Integrazioni documentarie
- Art. 57 – Regole di smistamento e di assegnazione
- Art. 58 – Classificazione dei documenti
- Art. 59 – Fascicolazione informatica dei documenti
- Art. 60 – Processo di assegnazione dei fascicoli

## PARTE QUINTA

### FLUSSI DOCUMENTALI INTERNI

- Art. 61 – Assegnazione dei documenti in entrata agli uffici

Art. 62 – Comunicazioni interne

Art. 63 – Pubblicazioni all’Albo Pretorio

## PARTE SESTA

### SICUREZZA E PROTEZIONE DEI DATI PERSONALI

Art. 64 – Sicurezza dei sistemi informatici del Comune

Art. 65 – Amministratore di sistema

Art. 66 – Uso del profilo utente per l’accesso ai sistemi informatici

Art. 67 – Gestione dei dati personali negli atti amministrativi e nei protocolli

## **PARTE PRIMA**

### **PRINCIPI GENERALI E DISPOSIZIONI PRELIMINARI**

#### **Art. 1. Riferimenti normativi**

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

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

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

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" (di seguito anche solo "CAD");
- le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 "Disposizioni legislative in materia di documentazione amministrativa" (di seguito anche solo "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".

#### **Art. 2 - Ambito di applicazione**

Il presente manuale descrive le regole per la gestione delle attività di formazione, registrazione, classificazione, fascicolazione dei documenti, oltre la gestione dei flussi documentali relativi ai procedimenti amministrativi del Comune di San Miniato.

Il presente Manuale di gestione sostituisce il Manuale di gestione del protocollo e dei flussi documentali adottato con Delibera della Giunta Comunale n. 163 del 30/12/2003.

Descrive altresì le attività di registrazione dei documenti pervenuti al Comune di San Miniato.

Il presente Manuale, i suoi allegati e i successivi aggiornamenti sono approvati con delibera di Giunta comunale, su proposta del Responsabile della gestione documentale dell'ente.

I successivi aggiornamenti del Manuale devono essere sottoposti all'approvazione della Giunta Comunale. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale. Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Piano di classificazione (Titolario).

Il Manuale e gli allegati sono pubblicati sul sito istituzionale del Comune, nella sezione "Amministrazione Trasparente", sottosezione "Atti generali".

## **PARTE SECONDA**

### **ORGANIZZAZIONE**

#### **Art. 3 - Area Organizzativa Omogenea (AOO), Unità Organizzativa Responsabile (UOR)**

Ai fini della gestione dei documenti con deliberazione di Giunta Comunale n. 41 dell'11/04/2025 è costituita una sola Area Organizzativa Omogenea (AOO) denominata Comune di San Miniato composta dall'insieme di tutte le Unità Organizzative (UO), come da allegato 1) Organigramma dell'Ente.

Nell'ambito dell'AOO viene utilizzato un unico sistema di protocollazione, che consente l'autonomia di ogni UOR (unità organizzativa responsabile) per la registrazione della corrispondenza in uscita ed interna.

Una UOR è un sottoinsieme di una AOO, cioè un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali i dipendenti assumono la responsabilità nella trattazione di affari o procedimenti amministrativi.

Alle UOR competono le operazioni in capo alle stesse affidate, riguardanti la gestione del flusso documentale, dei procedimenti nonché della fascicolazione, come meglio descritto nei successivi articoli.

#### **Art. 4 - Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi**

A norma dell'art. 61 del D.P.R. 445/2000, la Giunta Comunale, in ultimo con delibera n. 41 dell'11/04/2025, ha istituito, all'interno del servizio "Segreteria generale, Contratti e supporto giuridico amministrativo l'Ufficio protocollo al quale è assegnata la seguente casella di posta elettronica: protocollo@comune.san-miniato.pi.it.

Con decreto sindacale n. 15 del 22/05/2025 è stato nominato quale Responsabile della gestione documentale il Segretario Generale, a cui, sono ricondotti i compiti ai sensi dell'art. 61 del Testo Unico sulla documentazione amministrativa (TUDA), DPR 445/2000:

I compiti del Responsabile della gestione documentale (d'ora in avanti anche solo "Responsabile") sono definiti nell'atto di nomina. In particolare, il Responsabile:

- a) è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica del Comune;
- b) provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
- c) monitora i processi e le attività che governano le fasi di formazione e gestione dei documenti informatici;
- d) valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
- e) vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo, di produzione e conservazione del registro giornaliero di protocollo;
- f) assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso e, d'intesa con l'Ufficio Sistemi Informativi, vigila sul rispetto delle misure di sicurezza e di protezione dei dati;
- g) partecipa al periodico censimento degli strumenti software di gestione documentale in uso presso il Comune e, d'intesa con il RTD e l'Ufficio Sistemi Informativi, ne verifica la conformità alla normativa vigente.

Ulteriori e specifici compiti del Responsabile sono indicati nelle sezioni pertinenti del presente Manuale.

Il Responsabile può delegare in tutto o in parte i propri compiti al personale comunale.

#### **Art. 5 - Sistema di protocollo informatico**

Il Comune di San Miniato, avendo individuato un'unica AOO, si serve di un unico sistema di protocollo informatico denominato Sicr@Web, utilizzato da tutte le UOR dell'Ente.

Il protocollo unico è lo strumento attraverso il quale l'Amministrazione garantisce l'effettiva ricezione e trasmissione dei documenti.

#### **Art. 6 - Unicità del protocollo informatico**

Nell'ambito dell'area organizzativa omogenea la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva. Essa si chiude al 31 dicembre e ricomincia da 1 all'inizio di ogni anno. Il numero di protocollo è costituito da almeno sette cifre numeriche, ai sensi dell'art. 57 del Testo Unico sulla Documentazione Amministrativa (TUDA – D.P.R. 445/2000). Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

#### **Art. 7. Abilitazioni di accesso**

Le abilitazioni di accesso degli utenti alle componenti del Sistema informatico di gestione documentale del Comune sono assegnate personalmente a ciascun dipendente dal Responsabile della Gestione documentale su richiesta di ciascun Responsabile di servizio, Dirigente o Elevata Qualificazione, entro

cui è inquadrato il dipendente, nel rispetto dei criteri definiti dal Responsabile per la gestione documentale. A ciascun utente del Sistema, pertanto, sono attribuite specifiche funzioni, diversificate in ragione dell'appartenenza a un determinato settore dell'organizzazione o dell'assunzione di specifici ruoli e compiti, che ne abilitano la ricerca e l'accesso ai relativi documenti (visualizzazione e modifica).

#### **Art. 8. Soggetti delegati alle attività di protocollazione**

Tutti i dipendenti a cui è assegnata un'utenza per l'abilitazione d'accesso al Sistema informatico 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, di norma, centralizzata ed è curata dal personale, individuato dal Responsabile, addetto all'ufficio Protocollo, che provvede alla protocollazione di tutti i documenti informatici acquisiti dal Comune. La corrispondenza in arrivo per via postale viene di norma acquisita dal Servizio Segreteria Generale, che provvede all'apertura, alla protocollazione e allo smistamento della stessa. Spetta invece alle singole UOR abilitate a protocollare i documenti in arrivo che affluiscono direttamente agli uffici stessi a mano, per e-mail, ecc.

Le 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.

Gli operatori di protocollo, in base al loro livello di abilitazione, sono profilati come:

- a. supervisore del protocollo
- b. operatori Protocollo Generale
- c. operatori uffici decentrati.

#### Supervisore del protocollo

Il responsabile della gestione documentale, in quanto supervisore del protocollo, ha tutte le abilitazioni consentite dal programma di gestione del protocollo:

- Immissione protocollo in entrata, in uscita e posta interna;
- Annullamento di protocolli già inseriti;
- Ricerca dati;
- Visione di tutti i documenti archiviati;
- Gestione delle tabelle degli operatori e della relativa definizione delle abilitazioni;
- Creazione e tenuta delle credenziali di tutti gli operatori.
- Gestione e tenuta della tabella degli indirizzi e-mail per l'inoltro della corrispondenza.

#### Operatori Protocollo Generale

Sono il Responsabile della U.O. Protocollo e tutti gli addetti al protocollo dell'U.O. Protocollo.

Le abilitazioni concesse sono:

- Immissione protocollo in entrata, uscita e posta interna;
- Modifica dei protocolli già inseriti su autorizzazione del supervisore;
- Ricerca dati;
- Visione dei documenti archiviati.
- Smistamento successivo alle altre strutture per competenza

#### Operatori degli uffici decentrati

Sono i dipendenti appartenenti agli uffici che effettuano la protocollazione in sede decentrata rispetto all'U.O. Protocollo. Le abilitazioni concesse sono:

- Immissione protocollo in entrata per documenti inerenti le attività di competenza dell'ufficio;
- Immissione protocollo in uscita e per posta interna;
- Ricerca dati;
- Visione dei documenti di competenza dell'ufficio.
- Eventuale smistamento successivo ad altre strutture per competenza

#### **Art. 9. - Rilascio di abilitazioni di accesso**

Ad ogni utente è assegnata una credenziale di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

#### **Art. 10. Abilitazioni interne ad accedere ai servizi protocollo**

Il rilascio delle credenziali per l'autenticazione è effettuato dall'Ufficio CED su autorizzazione del responsabile del Settore richiedente tranne nei casi di richieste di credenziali di livello superiore a visualizzazione e protocollo in partenza che dovranno essere autorizzate dal responsabile della gestione documentale. Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato, la cui password non è accessibile.

Le sessioni multiple con la stessa *user* ID sono proibite e impedito.

#### **Art. 11. Ripristino delle credenziali private d'accesso**

In caso di smarrimento della password l'utente contatta l'amministratore del sistema e fa richiesta di una nuova password per accedere al sistema di Protocollo.

#### **Art. 12. Abilitazione alle registrazioni di protocollo riservato**

Attraverso il sistema di protocollo viene applicata la riservatezza ai documenti oggetto di protocollo. Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale. In modo analogo il responsabile del procedimento che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza. Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono.

## PARTE TERZA

### FORMAZIONE DEI DOCUMENTI

#### **Art. 13. Modalità di formazione dei documenti informatici**

Tutti i documenti del Comune di San Miniato sono formati in originale come documenti informatici, secondo le modalità individuate nel presente Manuale.

I documenti informatici del Comune di San Miniato sono formati mediante una delle seguenti modalità:

a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi *cloud* qualificati (ad esempio, mediante programmi di scrittura delle suite Microsoft Office o Libre Office, o mediante l'utilizzo delle funzioni dei sistemi di gestione documentale);

b) acquisizione:

- della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);

- della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);

- del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica o da chiave usb);

c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari resi disponibili all'utente (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile *online* agli utenti);

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

Le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
- memorizzazione su sistemi di protocollo e gestione documentale che adottino idonee politiche di sicurezza;
- versamento ad un sistema di conservazione.

Al documento informatico immodificabile, identificato in modo univoco e persistente attraverso la segnatura di protocollo, e ai documenti soggetti a registrazione particolare vengono associati i metadati che sono stati generati durante la sua formazione.

L'insieme minimo dei metadati è costituito da:

- Identificativo unico e persistente;
- Riferimento temporale;
- Oggetto;
- Soggetto che ha formato il documento;
- Destinatario;
- Impronta del documento informatico;
- Metadati aggiuntivi stabiliti dal Comune di San Miniato a fini gestionali e conservativi.

Nel caso specifico del documento amministrativo informatico l'insieme dei metadati minimi è costituito da:

- Numero protocollo;
- Data di protocollo;
- Mittente-destinatario;
- Oggetto;
- Data e protocollo del documento ricevuto, se disponibili;
- Impronta del documento informatico;
- Metadati aggiuntivi stabiliti dal Comune di San Miniato a fini gestionali e conservativi.

#### **Art. 14. Elementi essenziali del documento amministrativo informatico**

I documenti in uscita devono riportare le seguenti informazioni, organizzate per blocchi logici:

##### 1. Individuazione dell'autore del documento:

- Stemma del Comune e dicitura "Comune di San Miniato" nelle forme stabilite dall'Amministrazione;
- Unità Organizzativa Responsabile con eventuale indicazione del servizio e dell'ufficio;
- Indirizzo completo: via /piazza, numero civico, cap, città;
- Codice fiscale e partita IVA;
- Numero di telefono;
- Indirizzo istituzionale di posta elettronica;
- Indirizzo di posta elettronica certificata;
- Orario di apertura al pubblico.

##### 2. Individuazione e descrizione del documento

- Numero di protocollo;
- Data di protocollo (giorno/mese/anno);
- Eventuale numero di repertorio;

- riferimento a procedimento o fascicolo;
- Numero degli allegati, se presenti;
- Numero e data del documento cui si risponde;
- Oggetto del documento.
- Individuazione del destinatario del documento (se è un documento in uscita)
- Cognome e nome (per le persone)/Denominazione (per gli enti e le imprese)/UOR (per i documenti interni);
- A seconda dei casi:
  - Indirizzo completo: via/piazza, numero civico, cap. città;
  - Indirizzo informatico (PEC ...).

### 3. Individuazione del Responsabile del Procedimento:

- Cognome, nome e qualifica del Responsabile del Procedimento Amministrativo;
- Sottoscrizione (firma autografa o digitale).

### **Art. 15. Tipologie di formato del documento informatico**

Il Comune di San Miniato, in considerazione di quanto previsto dall'allegato 2 alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici in materia di conservazione, al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, interoperabilità, supporto allo sviluppo e diffusione adotta i seguenti formati:

FORMATO	ESTENSIONE
PDF-PDF/A	.pdf
TIFF	.tiff
JPG	.jpeg, .jpg
Office Open XML (OOXML)	.odt, .ods, .odp, .odg, .odb
XML	.xml Derivati da XML: .svg
TXT	.txt, .csv
Formati messaggi di posta elettronica	.eml
AUtoCAD DXF	.dxf
M4a	.m4a, .m4b, .mp4
MP3	.mp3
WAV	.wav

Eventuali integrazioni al presente elenco vengono definite in considerazione di specifiche previsioni normative o tecniche. In caso di utilizzo di formati diversi da quelli elencati nell'Allegato 2 alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici dovrà essere effettuata annualmente una valutazione di interoperabilità. A seguito della valutazione di interoperabilità potrà essere valutata l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato ad un altro, sempre tenendo in considerazione quanto previsto nell'Allegato 2.

I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Sindaco e degli organi collegiali, i contratti, le determine a contenuto provvedimentoale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma CADES o PADES in quanto, dal punto di vista giuridico, entrambe le tipologie di firma sono idonee a garantire l'autenticità dei documenti informatici sottoscritti.

#### **Art. 16. Copie per immagine di documenti analogici**

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

Nel caso in cui si debba garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il Responsabile di Servizio o il dipendente 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, è possibile effettuare un'unica attestazione di conformità, su foglio separato e collegato alle copie, da sottoscrivere digitalmente, contenente l'indicazione delle impronte *hash* associate a ciascun documento scansionato.

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

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

La verifica della conformità del documento è a carico dell'ufficio destinatario interno.

#### **Art. 17. 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 trasferendolo dall'*hard disk* del proprio computer a un dispositivo di archiviazione esterno quale una chiave usb). 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. Tale identità è rilevabile tramite raffronto delle impronte *hash*.

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 conservi la medesima efficacia giuridico-probatoria, è necessario attestarne la conformità della copia all'originale. Come per le copie per immagine, dunque, il Responsabile di Servizio o il dipendente all'uopo 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.

La verifica della conformità del documento è a carico dell'ufficio destinatario interno.

#### **Art. 18. Dispositivi di firma elettronica**

Il Comune di San Miniato garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica. A tal fine, il Comune è dotato di sistema di gestione documentale che consente ai dipendenti in possesso di profilo utente l'apposizione della firma digitale.

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.

#### **Art. 19. Scadenza dei certificati di firma**

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo. Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

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

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

#### **Art. 20. Identificazione univoca del documento informatico**

Ogni documento informatico deve essere identificato in modo univoco e persistente. L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica *hash*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata 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 AgID sulla formazione, gestione e conservazione dei documenti informatici (cfr. p. 2.2, tab. 1).

#### **Art. 21. Associazione degli allegati al documento principale**

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

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

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

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

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

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso 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 (ad esempio, dopo l'apposizione della firma digitale).

#### **Art. 22. Accessibilità del documento informatico**

Per garantire l'accessibilità dei documenti informatici ai soggetti portatori di disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nelle Linee Guida AgID sull'accessibilità degli strumenti informatici

#### **Art. 23. Metadati del documento informatico**

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID sulla formazione, gestione e conservazione dei documenti informatici.

Ulteriori metadati facoltativi sono associati a particolari tipologie di documenti, secondo le indicazioni riportate nell'allegato 2 al presente Manuale.

L'associazione dei metadati al documento è effettuata tramite le apposite funzioni dei *software* di gestione documentale utilizzati per la formazione degli atti. 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.

#### **Art. 24. Immodificabilità e integrità del documento informatico**

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

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

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

- per i documenti di cui è richiesta la sottoscrizione, dall'apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- per i documenti di cui non è richiesta la sottoscrizione, dalla memorizzazione nel sistema di gestione documentale, purché sia garantito il rispetto delle misure di sicurezza previste;
- per tutte le tipologie documentali, dal versamento nel sistema di conservazione.

In ogni caso, il versamento nel sistema di conservazione è il metodo che offre le maggiori garanzie di immodificabilità e integrità dei documenti informatici nel tempo. Pertanto, è essenziale che tutti i documenti siano versati in conservazione, secondo i tempi e le modalità descritte nel manuale di conservazione documentale.

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

#### **Art. 25. Copie analogiche di documenti informatici**

Fermo restando l'obbligo di formare i documenti originali informatici, in alcuni casi può essere necessario effettuare delle copie analogiche affinché siano spedite a mezzo posta ai soggetti che non sono muniti di domicilio digitale e agli altri soggetti indicati all'art. 3-bis, comma 4-bis, CAD.

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

La copia analogica inviata al cittadino, 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 dell'Ufficio

[indicazione UO]. Il documento originale informatico è archiviato nel sistema informatico del Comune di San Miniato, presso cui è disponibile per l'accesso").

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

#### **Art. 26. Casi in cui è ammessa la formazione di documenti originali analogici**

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

- ai sensi dell'art. 2, comma 6, CAD, esclusivamente nell'ambito dell'esercizio di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile;
- in tutti i casi in cui il documento è consegnato a sportello e il richiedente è un soggetto privato che non agisce in qualità di professionista (ad esempio, la tessera elettorale, la carta d'identità, ecc.).

La formazione di contratti e altre scritture private in originale analogico non è consentita. A tal fine, nel caso in cui la parte contraente non sia munita di strumenti di firma digitale o qualificata, si seguono le indicazioni riportate all'art. 16 comma 5, lett. b) del presente Manuale.

### **PARTE QUARTA**

#### **GESTIONE DOCUMENTALE**

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

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

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

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

#### **Art. 28. Canali di ricezione**

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

- casella PEC: [comune.sanminiato.pi@postacert.toscana.it](mailto:comune.sanminiato.pi@postacert.toscana.it), presidiata dall'ufficio Protocollo -
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti.

La posta elettronica ordinaria può essere trasmessa all'indirizzo [protocollo@comune.san-miniato.pi.it](mailto:protocollo@comune.san-miniato.pi.it)

L'indirizzo di posta elettronica certificata è riportato nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale.

L'indirizzo di posta elettronica certificata non è abilitato alla ricezione dei documenti provenienti da indirizzi di posta elettronica ordinaria.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, 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 validamente trasmessi.

Non è in nessun caso ammessa la ricezione di documenti e/o allegati tramite l'indicazione di *link* esterni.

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 il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-bis e 6-ter del CAD.

#### **Art. 29. Formati accettati**

Sono accettati documenti informatici esclusivamente nei seguenti formati standard: .pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods, .eml.

Inoltre:

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

Sono accettati, altresì, gli ulteriori formati eventualmente previsti nell'allegato 2, al presente manuale. Possono essere accettati, inoltre, i formati contemplati nell'Allegato 2 delle Linee guida dell'AgID sulla formazione, gestione e conservazione dei documenti informatici.

Resta salva la possibilità, da parte del Responsabile del procedimento, di prevedere esposte 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.

Il controllo sulla conformità del formato dei documenti in entrata è effettuato dal personale dell'ufficio assegnatario. 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 della UO assegnataria.

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.

### **Art. 30. Verifica sul formato dei documenti allegati**

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

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

### **Art. 31. Controllo dei certificati di firma**

Il personale abilitato alla protocollazione effettua una prima verifica sui certificati di firma contestualmente alla registrazione di protocollo del documento in entrata. In caso di certificati scaduti, revocati o sospesi, procede alla registrazione, segnalando in nota il risultato della verifica di firma.

Il Responsabile del procedimento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

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

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso 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 o posta elettronica ordinaria, se il documento principale non ha un contenuto sufficientemente esplicativo (ad esempio, un provvedimento, un certificato, ecc.) deve essere predisposta una nota di accompagnamento debitamente sottoscritta.

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

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

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

Per la trasmissione telematica di documenti a imprese e professionisti tenuti obbligatoriamente all'iscrizione in albi o elenchi, il domicilio digitale è estratto dall'indice INI-PEC ([www.inippec.gov.it](http://www.inippec.gov.it)).

Quando l'indirizzo PEC del soggetto destinatario (professionista o impresa) 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 tenuto all'iscrizione.

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.

Quindi, la comunicazione a un soggetto privato che abbia ad oggetto un rapporto che si pone al di fuori dell'attività professionale, deve essere fatta:

- I. se vi è stata elezione di domicilio digitale, all'indirizzo PEC espressamente dichiarato dal cittadino;
- II. se non vi è stata elezione di domicilio digitale, all'indirizzo PEC risultante dall'INAD (Indice Nazionale dei Domicili digitali);
- III. In caso di assenza di indirizzo PEC dall'INAD, deve essere trasmessa al domicilio fisico la copia cartacea del documento. Se si tratta di documento sottoscritto dall'Amministrazione, la copia deve essere prodotta in conformità a quanto previsto all'art. 20 del presente Manuale.

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione 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.

#### **Art. 34. Disposizioni sui documenti analogici**

I documenti su supporto analogico possono pervenire al Comune attraverso:

- il servizio postale;
- la consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata agli uffici agli addetti alle attività di sportello durante l'orario di apertura;
- consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata allo sportello del Protocollo generle aperto al pubblico durante l'orario di apertura.

I documenti provenienti dal servizio postale tradizionale o da corrieri autorizzati sono consegnati all'Ufficio Segreteria Generale, che provvede alla registrazione e al deposito dei documenti nell'apposito casellario in cui vengono ritirati a cura dei singoli uffici. Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti, e successivamente aperti per gli ulteriori controlli preliminari alla registrazione; la busta o contenitore si allega al documento per la parte relativa ai timbri postali

Qualora un documento sia consegnato personalmente dal mittente o da altra persona incaricata, l'Ufficio Protocollo o altro Ufficio che svolge attività di sportello/ricevimento al pubblico provvede alla protocollazione contestualmente alla presentazione della pratica.

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta almeno i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO;
- il mittente;
- l'oggetto;

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

Nel caso di ricezione dei documenti informatici, l'informazione al mittente dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dall'Amministrazione.

Nei casi consegna diretta da parte dell'interessato o da un delegato all'Ufficio Protocollo o al personale addetto agli uffici durante l'orario di sportello/ricevimento al pubblico, qualora i tempi permessi dalle esigenze dell'ufficio e dal numero di utenti presenti in quel momento non consentano la protocollazione immediata il dipendente è autorizzato a fotoreprodurre gratuitamente il documento da protocollare ed apporre il solo timbro ricezione presso l'Ente, comprensivo di data e di firma autografa. Qualora il documento sia composto di più pagine, è sufficiente la fotoreproduzione della prima pagina, mentre eventuali ulteriori costi di riproduzione sono a carico di chi presenta il documento da protocollare.

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

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

- La corrispondenza cartacea riportante l'indicazione "offerta", "gara d'appalto", "preventivo" o simili, o dal cui involucro sia possibile evincere che si riferisca alla partecipazione ad una gara, non deve essere aperta, ma protocollata in base agli elementi rilevabili dal plico o dal bando dell'Amministrazione, apponendo numero di protocollo e data di registrazione direttamente sulla busta. Il responsabile del procedimento amministrativo relativo ad una gara, ne invia il bando all'U.O. Protocollo il bando, comunicando, altresì, la data e l'ora di scadenza della presentazione delle offerte, avendo cura di far corrispondere quest'ultima con l'ora di chiusura dell'ufficio di front-office del Protocollo. Sull'esterno della busta, accanto alla segnatura di protocollo, viene annotato l'orario di arrivo unicamente nei casi in cui il documento venga consegnato *brevi manu* oltre il limite orario stabilito nel bando o nell'avviso pubblico: la specifica oraria viene pertanto a contrassegnare soltanto le offerte pervenute oltre la prevista scadenza. L'ufficio competente allo svolgimento della procedura di gara provvede alla custodia della busta o dei contenitori così protocollati, sino all'espletamento della gara; lo stesso ufficio, successivamente alla fase di apertura delle buste, riporterà gli estremi di protocollo presenti sulle buste su ogni documento che le stesse contengano

- La corrispondenza recante la dicitura "RISERVATA", "SPM" o "PERSONALE" viene trattata con le modalità stabilite al successivo articolo 54.

### **Art. 35. Documenti 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.

I documenti interni, cioè i documenti prodotti e destinati all'interno dell'AOO del Comune, si distinguono in formali e informali. I documenti interni sono formati prevalentemente con tecnologie informatiche.

La trasmissione tra UOR di documenti informatici formali avviene per mezzo del sistema di gestione documentale Sicr@web. Il documento interno è registrato nel sistema di gestione documentale come protocollo interno e viene trasmesso alla UOR destinataria tramite la funzione di assegnazione, non deve pertanto essere registrato dalla UOR destinataria.

La trasmissione tra UOR di documenti informatici informali, che non devono essere registrati a protocollo, avviene per mezzo di posta elettronica o di sistemi informatici interni.

### **Art. 36. Sistema di protocollo informatico**

Il Comune, per la protocollazione dei documenti, utilizza un Sistema di protocollo informatico integrato con il Sistema di gestione documentale. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo presente nella sezione .

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

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

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

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

### **Art. 38. Registro generale di protocollo**

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche. La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo (vedi art. 6 del presente Manuale).

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

### **Art. 39. Registro giornaliero di protocollo**

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

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

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

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

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

Non sono soggetti a protocollazione, inoltre, gli atti e i documenti registrati in repertori e registri differenti dal registro di protocollo ai sensi dell'art. 51 del presente Manuale.

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

### **Art. 41. 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.

### **Art. 42. Registrazione di protocollo**

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell'art. 53, comma 1, TUDA, metadati di registrazione di protocollo sono:

- a) numero di protocollo del documento, generato automaticamente dal sistema;

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

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

- g) tipologia di documento;
- h) classificazione (titolo e classe) sulla base del Titolario (vedi allegato 3);
- i) fascicolo di appartenenza;
- j) assegnazione interna (per competenza o per conoscenza);
- k) data e ora di arrivo;
- l) allegati;
- m) livello di riservatezza;
- n) mezzo di ricezione o invio;
- o) annotazioni;
- p) (eventualmente) estremi del provvedimento di differimento della registrazione;
- q) (se necessario) elementi identificativi del procedimento amministrativo.

#### **Art. 43. 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.

Il responsabile di ciascuna UOR prende atto tramite il sistema informatico che gli sono stati smistati dei documenti, provvede sotto la propria responsabilità e con cadenza quotidiana a prendere in carico il documento dalla scrivania virtuale.

#### **Art. 44. Protocollo delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione**

Per la protocollazione della posta elettronica ordinaria gli utenti abilitati alla protocollazione in entrata provvedono a scaricare il file .EML contenente messaggio in entrata e a protocollare il messaggio, 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.

#### **Art. 45. 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 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).

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

#### **Art. 46. 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. Negli altri casi, l'associazione degli allegati al documento principale avviene con le modalità indicate all'art. 16 del presente Manuale.

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.

Per la trasmissione di allegati di dimensioni superiori a 60 MB, sono previsti appositi canali di trasmissione diversi dalla PEC. Pertanto, la trasmissione e successiva registrazione delle comunicazioni dovrà avvenire tramite tali canali. A tal fine, 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.

Non è in nessun caso ammessa la ricezione di documenti e/o allegati tramite l'indicazione di *link* esterni.

#### **Art. 47. 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.

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.

#### **Art. 48. Segnatura di protocollo**

La segnatura di protocollo è l'apposizione o associazione al documento originale, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso, per consentire l'individuazione

di ciascun documento in modo inequivocabile. L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

Le informazioni minime apposte o associate al documento mediante l'operazione di segnatura, sono quelle previste dall'art. 55 del TUDA e precisamente:

- identificativo dell'Amministrazione;
- progressivo di protocollo;
- data di registrazione.

Ulteriori informazioni previste sono:

- indicazione della UOR del Comune di Montespertoli responsabile del documento prodotto;
- identificazione degli allegati;
- anno;
- titolo;
- classe.

I dati relativi alla segnatura di protocollo di un documento trasmesso da una AOO sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale.

All'interno del file XML devono essere contenute anche le seguenti informazioni minime:

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

La segnatura di protocollo permette di realizzare l'interoperabilità tra i sistemi di gestione informatica dei documenti di amministrazioni diverse, automatizzando, fino al massimo livello possibile, la registrazione di protocollo di documenti informatici provenienti da altri sistemi interoperabili.

Qualora il documento venga prodotto su formato analogico al termine della registrazione la segnatura viene apposta tramite timbro o etichetta (le cui informazioni sono il risultato dell'estrazione delle informazioni minime contenute nella segnatura informatica). Questa riporterà il numero e la data di protocollo, la classificazione, il numero di fascicolo, la UOR

#### **Art. 49. Protocollo riservato**

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 da Case di Reclusione);

- 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.

- altri documenti considerati riservati a discrezione dell'ufficio competente 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.

### **Art. 50. Registro di emergenza**

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le sei ore o che sia comunque tale da pregiudicare la registrazione a protocollo in giornata, nel caso in cui vi siano scadenze inderogabili e prescrittive (es. bandi, concorsi etc.).

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico ogni evento deve essere registrato su un supporto alternativo, denominato Registro di emergenza autorizzato per scritto dal Responsabile della gestione documentale.

Il Registro di emergenza è unico ed è tenuto presso l'Ufficio Protocollo.

Le informazioni da inserire nel registro di emergenza, ovvero i campi obbligatori da compilare, sono gli stessi previsti dal protocollo generale.

Per la registrazione di emergenza si utilizza:

- nel caso di disponibilità dei PC un modulo redatto su un foglio di calcolo elettronico, che potrà essere compilato mediante l'immissione dei dati direttamente sulla tabella e dovrà essere successivamente salvato;
- nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modello di registro di emergenza (Allegato 6) che verrà compilato manualmente.

La numerazione adottata sarà una numerazione di emergenza (che si azzera ogni anno e che è contraddistinta dalla lettera E).

Le modalità di registrazione e di recupero sono le seguenti:

- devono essere riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- la sequenza numerica utilizzata sul Registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO (Comune);
- una volta ripristinata la piena funzionalità del sistema, il Responsabile della gestione documentaria, provvede alla chiusura del Registro di emergenza, annotando il numero di registrazioni effettuato e la

data e ora di chiusura. I dati delle registrazioni di emergenza dovranno essere inseriti nel sistema informatico di protocollo e si configurano come un repertorio dello stesso;

- le informazioni relative ai documenti protocollati in emergenza sono inserite nel protocollo informatico al ripristino delle funzionalità dello stesso. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, avendo cura di mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

Quindi i documenti annotati nel Registro di emergenza e trasferiti nel protocollo informatico unico recheranno, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero attribuito dal Registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

Scheda di apertura /chiusura del registro di emergenza:

### **Servizio di protocollo**

*Scheda di apertura/chiusura del registro di emergenza*

*Area Organizzativa Omogenea Comune di San Miniato*

*Unità Organizzativa di registrazione di Protocollo*

Causa dell'interruzione:

Data: gg/mm/aa di inizio/fine interruzione

Ora dell'evento hh/mm Annotazioni:

Numero protocollo XXXXXXXXX iniziale/finale

Pagina n. \_\_\_\_\_

Firma del responsabile del servizio di protocollo \_\_\_\_\_

### **Art. 51. Documenti soggetti a registrazione particolare**

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

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

- Verbali delle sedute del Consiglio comunale;
- Verbali delle sedute della Giunta comunale;
- Verbali delle sedute delle Commissioni Consiliari permanenti e speciali;
- Verbali delle Commissioni istituite per legge;
- Atti di stato civile;
- Carte d'identità;

- Certificati anagrafici;
- Tessere elettorali;
- Atti di liquidazione;
- Mandati di pagamento;
- Reversali d'incasso;
- Verbali di violazioni al Codice della Strada emessi dall'Ente
- Verbali di violazioni amministrative emessi dall'Ente;
- Delibere del Consiglio comunale,
- Delibere della Giunta Municipale;
- Determinazioni dirigenziali;
- Ordinanze
- Contratti pubblici;
- Scritture private;

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

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

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

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

#### **Art. 52. Disposizioni sulla protocollazione e gestione dei documenti analogici.**

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

Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione. La copia per immagine di documenti firmati, se sprovvista di attestazione di conformità, apposta ai sensi della normativa vigente, può essere adoperata solo per uso lavoro.

#### **Art. 53. 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 anonimi il cui contenuto sia giuridicamente irrilevante o inequivocabilmente da ricondurre a scherzi o situazioni similari, vengono distrutti; se, invece, si ritiene che contengano dati o informazioni rilevanti, dopo la registrazione di protocollo, si provvede ad inviarli agli uffici competenti per ulteriori eventuali determinazioni.

I documenti sottoscritti, di cui non sia identificabile l'autore, vengono protocollati indicando nel campo mittente la dicitura “mittente non identificabile” e sono inoltrati al responsabile competente; quest'ultimo, ricevuto il documento, valuterà la possibilità nonché la necessità di acquisire gli elementi mancanti per perfezionare l'atto, provvedendo affinché venga integrata la registrazione di protocollo.

I documenti ricevuti privi di firma, ma il cui mittente sia comunque identificabile, vengono protocollati e inoltrati al responsabile del procedimento, che valuterà la necessità di acquisire la dovuta sottoscrizione per il perfezionamento degli atti.

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati all'art. 48.

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”.

#### **Art. 54. 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, previa firma di ricevuta di cui al precedente articolo 46. Il destinatario, se reputa che i documenti ricevuti debbano comunque essere protocollati, provvede a effettuare registrazione e segnatura di protocollo.

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.

#### **Art. 55. 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), non viene protocollato e viene restituito al mittente.

Nel caso in cui un documento della fattispecie sia erroneamente registrato al protocollo, viene restituito al mittente, con una lettera di trasmissione protocollata.

#### **Art. 56. Integrazioni documentarie**

L'addetto al Protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati.

Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente

indicando con precisione l'indirizzo al quale inviarli e specificando che la mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento. I documenti pervenuti ad integrazione di quelli già disponibili sono protocollati dalla UOR competente sul protocollo generale e, a cura del RPA, sono inseriti nel fascicolo relativo.

#### **Art. 57. Regole di smistamento e di assegnazione**

L'operazione di smistamento consiste nell'assegnazione di un documento registrato alla UOR competente e al conseguente conferimento di responsabilità del relativo procedimento amministrativo.

Si adottano le modalità operative seguenti:

- nel caso di documento analogico, l'originale sarà conservato dal Settore assegnatario;
- nel caso di documenti informatici, l'originale sarà acquisito direttamente nel sistema di protocollo attraverso i canali previsti;
- è prevista una forma di assegnazione per conoscenza per i soli documenti a carattere conoscitivo privi di adempimenti per le UOR (come circolari di contenuto informativo);
- quotidianamente gli operatori e/o i responsabili aprono la scrivania di lavoro, attraverso la quale possono verificare i documenti pervenuti e monitorare i movimenti, precedenti o successivi degli stessi.

Il responsabile dell'UOR visualizza i documenti, attraverso l'utilizzo della scrivania digitale e in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente sulla materia oggetto del documento;

Il RPA provvede alla visione e alla gestione del documento assegnato e mediante una delle seguenti azioni:

- smistamento: ad utenti del proprio ufficio;
- rifiuto: restituzione del documento all'ufficio mittente in caso di errata assegnazione;
- fascicolazione: inserimento nel fascicolo procedimentale.

Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

La traccia risultante definisce ai fini normativi e regolamentari i tempi e le modalità di gestione del flusso documentale ed i conseguenti riflessi sotto il profilo della responsabilità.

La presa in carico dei documenti viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOR di competenza coincide con la data di assegnazione degli stessi.

#### **Art. 58. 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 3.

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

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

#### **Art. 59. 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. I fascicoli eventualmente possono essere organizzati in sotto-fascicoli.

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

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

I fascicoli informatici possono essere organizzati:

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

I fascicoli informatici devono recare i metadati obbligatori delle aggregazioni documentali previsti nell'allegato 5 alle Linee guida AgID.

Nelle more dell'implementazione di modalità automatizzate creazione e gestione dei fascicoli, organizzate secondo il piano di fascicolazione del Comune, gli utenti tenuti alla formazione dei fascicoli informatici assicurano che siano associati almeno i seguenti metadati, distinti per tipologia di fascicolo.

Il fascicolo informatico organizzato per procedimento amministrativo deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (procedimento amministrativo);

3. codice IPA Amministrazione titolare (campo “Ruolo”);
4. codice IPA Amministrazioni partecipanti (campo “Ruolo”);
5. dati identificativi del RUP (nome, cognome, codice IPA dell’Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per affare deve recare:

1. metadati identificativi del tipo di aggregazione (campo “TipoAggregazione” = Fascicolo; campo “IdAggregazione” = codice identificativo);
2. tipologia di fascicolo (affare);
3. codice IPA Amministrazione titolare (campo “Ruolo”);
4. codice IPA Amministrazioni partecipanti (campo “Ruolo”)
5. dati identificativi del RUP (nome, cognome, codice IPA dell’Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per persona deve recare:

1. metadati identificativi del tipo di aggregazione (campo “TipoAggregazione” = Fascicolo; campo “IdAggregazione” = codice identificativo);
2. tipologia di fascicolo (“persona fisica” o “persona giuridica”);
3. dati anagrafici della persona a cui fa riferimento il fascicolo (almeno nome e cognome per le persone fisiche, denominazione per le persone giuridiche, denominazione e codice IPA per le PA);
4. dati identificativi del RUP (nome, cognome, codice IPA dell’Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato per attività deve recare:

1. metadati identificativi del tipo di aggregazione (campo “TipoAggregazione” = Fascicolo; campo “IdAggregazione” = codice identificativo);
2. tipologia di fascicolo (attività);
3. dati identificativi del RUP o dell’assegnatario dell’attività (nome, cognome, codice IPA dell’Amministrazione di appartenenza, domicilio digitale).

#### **Art. 60. Processo di assegnazione dei fascicoli**

Quando un nuovo documento viene recapitato all’amministrazione, l’UOR abilitato all’operazione di fascicolazione stabilisce, con l’ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso debba essere ricollegato ad un fascicolo già esistente, oppure sia necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

Se il documento si ricollega ad un fascicolo aperto, l’addetto:

- seleziona il relativo fascicolo;

- collega la registrazione di protocollo del documento al fascicolo selezionato
- (se si tratta di un documento cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).

Se il documento non è collegabile ad alcun fascicolo aperto, il soggetto preposto:

- esegue l'operazione di apertura del fascicolo
- collega la registrazione di protocollo del documento al nuovo fascicolo aperto

## **PARTE QUINTA**

### **FLUSSI DOCUMENTALI INTERNI**

#### **Art. 61. Assegnazione dei documenti in entrata agli uffici**

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnati alle UO Responsabili preventivamente individuate le fatture provenienti dal Sistema Di Interscambio (SDI). Ulteriori criteri di assegnazione automatica sono definiti dal Responsabile, sentite le UUOO interessate.

I documenti non assegnati automaticamente sono assegnati agli Unità Organizzative Responsabili in base all'oggetto del documento e alla classificazione.

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

Su espressa richiesta dei Responsabili delle Unità Organizzative e per esigenze particolari può essere previsto che l'assegnazione avvenga per Ufficio/U.O. di livello immediatamente successivo a quello della U.O.R., ma solo quando l'oggetto della comunicazione sia facilmente riferibile al singolo Ufficio/U.O.

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

Nel caso di assegnazione errata, la U.O.R. che riceve il documento, lo restituisce all'Ufficio Protocollo per consentire di procedere ad una nuova assegnazione. Se la U.O.R. destinataria individua la competenza può procedere autonomamente all'assegnazione corretta.

I termini per la definizione del procedimento amministrativo che, eventualmente, prende avvio dal documento, decorrono, comunque, dalla data di protocollazione.

Il sistema di gestione informatica dei documenti memorizza tutti i singoli passaggi conservandone, per ciascuno di essi, l'identificativo dell'operatore, la data e l'ora di esecuzione.

La traccia risultante dalle operazioni di cui al comma precedente definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

#### **Art. 62. 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 mediante l'utilizzo del sistema di workflow di cui è dotato il Sistema di gestione documentale. In alternativa, gli

scambi di documenti tra gli uffici sono effettuati per mezzo di posta elettronica ordinaria, attraverso rete intranet o mediante cartelle condivise.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria.

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

Le comunicazioni di interesse generale sono trasmesse tramite apposite liste di distribuzione.

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.

### **Art. 63. Pubblicazioni nell'Albo pretorio**

Tutti gli atti prodotti dal Comune che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto imm modificabile (cfr. art. 24 del presente Manuale). Gli atti oggetto di notificazione tramite pubblicazione ai sensi del codice di procedura civile, una volta ricevuti e scansionati, sono inseriti manualmente dal personale abilitato.

Ciascuna direzione è responsabile dei dati pubblicati all'Albo Pretorio, relativamente agli atti di propria competenza, in particolare per quanto riguarda la protezione dei dati.

## **PARTE SESTA**

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

#### **Art. 64. Sicurezza dei sistemi informatici del Comune**

La memorizzazione dei documenti correnti è effettuata sui server del Comune, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore o della selezione per lo scarto.

#### **Art. 65. Amministratore di sistema**

Il Responsabile dei servizi informatici, nel rispetto dei criteri definiti da Responsabile e delle indicazioni provenienti dai responsabili di servizio, gestisce le abilitazioni di accesso al sistema.

#### **Art. 66. Uso del profilo utente per l'accesso ai sistemi informatici**

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

Per l'accesso ai sistemi informatici del Comune è necessaria l'assegnazione di un profilo utente da parte del Responsabile.

Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password che coincidono con le credenziali di accesso al dominio dell'Ente.

Le richieste concernenti il recupero delle credenziali devono essere effettuate per iscritto al Responsabile, che le accetta con formale comunicazione.

L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali.

I criteri di sicurezza applicati alla complessità delle password e le politiche di scadenza sono quelli del dominio Windows.

#### **Art. 67. Gestione dei dati personali negli atti amministrativi e nei protocolli**

I dati personali eventualmente presenti negli atti amministrativi (determinazioni, delibere, ordinanza) devono essere protetti, a cura del Dirigente designato al loro trattamento, nel rispetto dei principi previsti dal Regolamento generale per la protezione dei dati personali (GDPR) ed in particolare del principio di minimizzazione.

A tale fine:

##### 1. Oggetto

L'oggetto dell'atto, sempre visibile all'albo pretorio, non può essere mai oscurato perciò dovrà essere redatto senza contenere dati personali, salvo i casi in cui la pubblicazione dei dati personali sia prevista obbligatoriamente per legge.

##### 2. Testo dell'atto

I dati personali contenuti nel testo riferiti all'interno dell'atto possono essere oscurati usando la funzionalità del software di gestione documentale; il documento verrà pubblicato all'albo pretorio con la dicitura "omissis" in corrispondenza dei dati personali oscurati.

All'interno dell'Ente i dati personali contenuti negli atti amministrativi risulteranno comunque visibili in chiaro (non oscurati).

Il Dirigente, Designato al trattamento dati, può tuttavia disporre motivatamente particolari misure ritenute necessarie per tutelare la riservatezza degli interessati utilizzando la funzionalità del software di gestione che consente di limitare la visibilità dei documenti.

##### 3. Allegati

Eventuali allegati, contenenti dati personali la cui pubblicazione non sia obbligatoria per legge, dovranno essere depurati dei dati personali non ostensibili o, laddove ciò non sia possibile o troppo gravoso, dovranno essere marcati in modo da non essere pubblicati all'albo pretorio.

##### 4. Protocolli

Per quanto riguarda i protocolli può essere utilizzata la funzione protocollo riservato descritta all'art. 54. Protocollo riservato del presente manuale.

#### **ALLEGATI:**

- 1) Organigramma
- 2) Formati dei documenti
- 3) Titolario

4) Modello di registro di protocollo di emergenza