

# Manuale di gestione dei documenti e dei flussi documentali del Comune di Padova

Versione 3.0 del 30/11/2018



## INFORMAZIONI SUL DOCUMENTO

<b>Titolo</b>	Manuale di gestione dei documenti e dei flussi documentali del Comune di Padova – v. 3.0	
<b>Versione</b>	3.0	
<b>Nome file</b>	Manuale_di_gestione_Comune_di_Padova_V.3.0.pdf	
<b>Redazione</b>	Gruppo di lavoro Padova PA digitale	data: 30/11/2018
<b>Verifica</b>	Segretario/Direttore Generale dott. Giovanni Zampieri	data: 24/01/2019
<b>Approvazione</b>	Deliberazione della Giunta Comunale n. 2019/0040	data: 29/01/2019
<b>Distribuzione</b>	Comitato di Direzione	data: 04/02/2019
	Rete Intranet del Comune di Padova e sito <a href="http://www.padovanet.it">www.padovanet.it</a>	data: 18/02/2019

## STORIA DELLE MODIFICHE APPORTATE AL DOCUMENTO

Versione	Variazioni	Data approvazione
1.0	Prima emissione	19 maggio 2003
2.0	Adeguamento al Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - <i>Regole tecniche per il protocollo informatico</i>	6 ottobre 2015
3.0	Adeguamento al Decreto Legislativo n. 82 del 7 marzo 2005 – <i>Codice dell'amministrazione digitale, e al Regolamento Europeo n. 679 del 27 aprile 2016 - Regolamento generale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati - General Data Protection Regulation (GDPR)</i>	29 gennaio 2019

## NOTE DI REDAZIONE

Per la stesura del capitolo 5 si ringrazia il personale dell'ufficio protocollo (Tullio Baveo, Emanuela Cecchinato, Mirca Faggin, Paola Galiazzo, Mariaelena Ghilotti, Martina Mazzucato, Mariagrazia Testa).

Per la stesura del capitolo 9 si ringrazia Giorgio Zanaga dell'Archivio Generale.

Gruppo di lavoro PA digitale: Valeria Pavone, Alessandro Businaro, Nicola Carraro, Bruna Ferro, Valentina Meggiato, Daniele Tarcisio Rampin.

## Indice generale

1. PRINCIPI GENERALI.....	6
1.1 Premessa.....	6
1.2 Ambito di applicazione del Manuale.....	6
1.3 Norme di riferimento e definizioni.....	7
1.4 Struttura organizzativa (Area Organizzativa Omogenea e Unità Organizzative Responsabili). .	7
1.5 Ruoli e responsabilità.....	8
1.5.1 Responsabile del servizio archivistico comunale per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi.....	8
1.5.2 Responsabile della conservazione.....	9
1.5.3 Responsabile della transizione al digitale.....	10
1.5.4 Responsabile della protezione dei dati.....	11
1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento.....	12
1.7 Politiche di gestione e conservazione documentale.....	12
2. PROTEZIONE DEI DATI PERSONALI E PIANO DI SICUREZZA.....	14
2.1 Contesto.....	14
2.2 Il principio di <i>accountability</i> ed il registro delle attività di trattamento.....	14
2.3 Il piano di sicurezza.....	15
2.3.1 Formazione dei documenti - Aspetti di sicurezza.....	17
2.3.2 Gestione dei documenti informatici - Aspetti di sicurezza.....	17
2.3.2.1 Componente organizzativa della sicurezza.....	17
2.3.2.2 Componente fisica e infrastrutturale della sicurezza.....	18
2.3.2.3 Componente logica della sicurezza.....	19
2.3.3 Gestione delle registrazioni di protocollo e di sicurezza.....	20
2.3.4 Criteri di utilizzo degli strumenti tecnologici.....	21
2.4 Trasmissione e interscambio dei documenti informatici - Aspetti di sicurezza.....	22
2.5 Accesso ai documenti informatici – Aspetti di sicurezza.....	23
2.6 Conservazione dei documenti informatici – aspetti di sicurezza.....	23
2.7 Politiche di sicurezza adottate dall’Ente.....	23
2.8 Verifica della conformità, miglioramento della sicurezza dei dati e responsabile della protezione dei dati.....	24
3. FORMAZIONE DEI DOCUMENTI.....	25
3.1 I documenti del Comune di Padova.....	25
3.2 Formazione dei documenti - Elementi informativi essenziali.....	25
3.3 Formazione dei documenti - aspetti operativi generali.....	26
3.4 Formazione del documento informatico e del documento amministrativo informatico.....	26
3.4.1 Metadati.....	27
3.4.2 Sottoscrizione dei documenti.....	28
3.4.3 Riferimento temporale.....	28
3.4.4 Tipologie di formato del documento informatico.....	29
4. SCAMBIO DEI DOCUMENTI.....	31

4.1 Documenti in entrata.....	31
4.2 Documenti in uscita.....	32
4.3 Documenti interni.....	32
4.3.1 Documenti interni formali.....	33
4.3.2 Documenti interni informali.....	33
4.4 Descrizione del flusso di lavorazione dei documenti.....	33
4.4.1 Flusso in entrata.....	34
4.4.2 Flusso in uscita.....	35
5. PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO.....	36
5.1 Registrazione dei documenti.....	36
5.2 Registro di protocollo.....	36
5.3 Elementi della registrazione di protocollo.....	37
5.4 Modalità di registrazione di protocollo e di assegnazione.....	38
5.5 La segnatura di protocollo.....	38
5.6 Documenti soggetti a registrazione particolare (Repertoriazione).....	39
5.7 Procedure specifiche nella registrazione di protocollo.....	40
5.7.1 Protocolli riservati.....	40
5.7.2 Documenti esclusi dalla registrazione di protocollo.....	41
5.7.3 Protocollo differito.....	41
5.7.4 Correzioni ortografiche e informazioni aggiunte alle registrazioni.....	41
5.7.5 Annullamento delle registrazioni di protocollo.....	42
5.8 Casi particolari di registrazioni di protocollo.....	43
5.8.1 Lettere anonime.....	43
5.8.2 Segnalazioni anonime.....	43
5.8.3 Lettere prive di firma.....	43
5.8.4 Corrispondenza da non aprire.....	43
5.8.5 Domicili eletti.....	44
5.8.6 Documenti inviati o presentati allo sportello che non siano afferenti ad alcun procedimento dell'Ente.....	44
5.8.7 Integrazioni documentarie.....	44
5.8.8 Documenti pervenuti per errore al Comune di Padova.....	45
5.8.9 Trattamento dello stesso documento inviato o consegnato a diverse UOR dell'Ente o pervenuto attraverso canali diversi.....	45
5.8.10 Documenti con pluralità di oggetti.....	45
5.8.11 Documenti in partenza con più destinatari.....	46
5.9 Modalità operative per la gestione dei documenti e dei relativi allegati.....	46
5.10 Modalità operative per lo smistamento.....	47
6. IL REGISTRO DI EMERGENZA.....	48
6.1. Situazioni che prevedono l'utilizzo del Registro di emergenza.....	48
6.2. Modalità di utilizzo del Registro di emergenza.....	48
7. DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO.....	50
7.1 Descrizione funzionale ed operativa.....	50
7.1.1. Il sistema di protocollo generale all'interno del piano di formazione dell'Ente.....	50

7.2 Rilascio delle abilitazioni di accesso.....	51
7.2.1 Abilitazioni interne ad accedere al sistema.....	52
7.2.2 Modalità di creazione e gestione delle utenze e dei relativi profili d'accesso.....	52
7.2.3 Abilitazione alle registrazioni di protocollo riservato.....	54
8. GESTIONE E CONSERVAZIONE DEI DOCUMENTI.....	55
8.1 Sistema di classificazione.....	55
8.2 Attività di fascicolazione.....	55
8.2.1 Processo di assegnazione dei fascicoli.....	56
8.2.2 Repertorio dei fascicoli.....	56
8.3 Documenti repertoriati.....	57
8.4 Gestione documenti cartacei degli archivi di deposito.....	57
8.4.1 Gli archivi di deposito delle Unità organizzative.....	57
8.4.2 Il versamento dei fascicoli.....	57
8.4.3 La movimentazione dei fascicoli.....	58
8.5 Conservazione dei documenti.....	58
8.6 Gestione dell'archivio storico.....	58
9. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA...	60
9.1 Regolamenti.....	60
9.2 Amministrazione trasparente.....	60
9.3 Procedure di accesso ai documenti e di tutela della riservatezza.....	61
9.3.1 Accesso dei documenti per fini amministrativi.....	61
9.3.2 Accesso dei documenti per fini di ricerca storico-scientifica.....	61
10. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI.....	62
10.1 Modalità di approvazione e aggiornamento del Manuale.....	62
10.2 Pubblicità del presente Manuale.....	62
ELENCO DEGLI ALLEGATI.....	63

# 1. PRINCIPI GENERALI

## 1.1 Premessa

Il Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - *Regole tecniche per il protocollo informatico* (d'ora in avanti citato come *Regole tecniche per il protocollo informatico*) prevede per tutte le pubbliche amministrazioni l'adozione del Manuale di gestione che, ai sensi dell'art. 5, comma 1 "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile della gestione documentale, così come già previsto dall'art. 50, comma 4 del Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000 (d'ora in avanti citato come DPR 445/2000) - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* .

Obiettivo del Manuale di gestione è descrivere il sistema e le componenti della gestione documentale e di elencare le ulteriori funzionalità disponibili.

Il protocollo informatico e il sistema di gestione documentale costituiscono il fulcro della struttura tecnologica ed organizzativa dell'Ente con riferimento alla gestione dei documenti, dei flussi documentali, dei processi e dei procedimenti amministrativi, nel rispetto della normativa vigente.

## 1.2 Ambito di applicazione del Manuale

Il Manuale è destinato alla più ampia diffusione interna, in quanto fornisce le istruzioni complete per la corretta gestione dei documenti da parte dei responsabili e degli addetti alle attività di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti nel Comune di Padova.

L'adozione del Manuale di gestione dei documenti e dei flussi documentali del Comune di Padova (d'ora in avanti citato come Manuale di gestione) si pone l'obiettivo di raggiungere, attraverso i sistemi che l'Ente ha a disposizione per la gestione documentale, una corretta ed uniforme metodologia per:

- il trattamento dei documenti sia analogici che digitali;
- le procedure condivise per la gestione dei procedimenti amministrativi;
- l'accesso agli atti ed alle informazioni;
- l'archiviazione e la conservazione dei documenti.

Il Manuale inoltre, come prescritto dall'art. 5, comma 3 delle *Regole tecniche per il protocollo informatico*, è pubblicato sul sito istituzionale del Comune di Padova al fine di garantire la diffusione anche esterna all'Ente.

Nel Manuale di gestione sono riportati:

- le politiche di protezione dei dati e il piano di sicurezza;
- le modalità di formazione e scambio dei documenti;
- l'utilizzo del sistema di protocollo informatico e gestione documentale;
- la gestione dei flussi documentali;
- l'uso del titolario di classificazione e le aggregazioni documentali (fascicoli);
- la gestione e la conservazione dei documenti;
- le modalità di accesso ai documenti e alle informazioni e le relative responsabilità;
- la gestione dei procedimenti amministrativi.

### **1.3 Norme di riferimento e definizioni**

Il Manuale di gestione si basa sui principi definiti dalle norme e dagli standard nazionali ed internazionali in materia di amministrazione digitale e gestione documentale, procedimenti e documenti amministrativi, tutela e conservazione degli archivi, protezione dei dati personali.

Le definizioni di riferimento del presente Manuale sono riportate nell'*Allegato 1 - Definizioni*.

### **1.4 Struttura organizzativa (Area Organizzativa Omogenea e Unità Organizzative Responsabili)**

Ai fini della gestione unica e coordinata dei documenti il Comune di Padova è costituito da un'unica Area organizzativa omogenea (AOO unica), formalmente definita con Deliberazione di Giunta comunale n. 933 del 14 novembre 2002.

All'interno della AOO viene utilizzato un unico sistema che consente l'autonomia di ogni UOR nella gestione documentale.

Le Unità organizzative responsabili (UOR) sono individuate dall'Organigramma del Comune di Padova come stabilito nella Deliberazione di Giunta comunale che definisce la struttura organizzativa dell'Ente (*Allegato 2 - Organigramma del Comune di Padova*).

La presa in carico dei documenti e l'assegnazione dell'istruttoria e degli adempimenti collegati a ciascun procedimento nel sistema di protocollo informatico costituisce responsabilità del dirigente di ciascuna UOR, come previsto dall'art. 5 comma 1 della Legge 7 agosto 1990, n. 241 - *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi 241/1990 e s.m.i.* (d'ora in avanti citata come L. 241/1990).

## 1.5 Ruoli e responsabilità

Nel sistema di gestione documentale si individuano i seguenti ruoli principali:

Ruoli	Norma di riferimento
Responsabile del servizio archivistico comunale per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi	Art. 61 del Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000 - <i>Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa</i>
Responsabile della conservazione	Art. 7 del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 – <i>Regole tecniche in materia di sistema di conservazione</i>
Responsabile della transizione digitale	Art. 17 del Decreto Legislativo n. 82 del 7 marzo 2005 – <i>Codice dell'amministrazione digitale</i>
Responsabile della protezione dei dati	Art. 37 del Regolamento Europeo n. 679 del 27 aprile 2016 - <i>Regolamento generale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati - General Data Protection Regulation (GDPR)</i>

### 1.5.1 Responsabile del servizio archivistico comunale per la gestione informatica del protocollo informatico, dei flussi documentali e degli archivi

A norma dell'art. 61 del DPR 445/2000, la Giunta comunale ha istituito, con Deliberazione n. 274 del 6 maggio 2003, nell'ambito del Settore Organi Istituzionali e Affari generali, l'ufficio denominato Servizio archivistico comunale, con il compito di gestire il protocollo informatico, i flussi documentali e gli archivi. Con la medesima Deliberazione è stato individuato il Responsabile del Servizio.

Al Servizio archivistico è demandata la gestione dell'archivio e nello specifico il governo del sistema di protocollo informatico e di gestione documentale, il coordinamento degli archivi di deposito dei Settori e la gestione dell'Archivio storico.

Ai sensi dell'art. 5, comma 3 delle *Regole tecniche per il protocollo informatico* sono compiti del Responsabile del Servizio:

- a) predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;



- b) proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici.

Sono inoltre compiti del Servizio:

- d) abilitare gli addetti dell'amministrazione all'utilizzo del sistema di protocollo informatico e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.);
- e) garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- f) garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
- g) curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- h) conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- i) garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
- j) autorizzare le operazioni di annullamento delle registrazioni di protocollo;
- k) aprire e chiudere il registro di emergenza.

### **1.5.2 Responsabile della conservazione**

Si identifica come la persona fisica formalmente incaricata dal Comune di Padova quale responsabile dell'insieme delle attività finalizzate alla conservazione dei documenti.

Il Comune di Padova affida il ruolo di Responsabile della Conservazione al Capo Settore Servizi Informatici e Telematici, ed affida il ruolo di Responsabile della funzione archivistica di conservazione e di vicario del Responsabile della conservazione al Responsabile del Servizio Archivistico comunale.

A norma dell'art. 44 del Decreto Legislativo 7 marzo 2005, n. 82 – *Codice dell'amministrazione digitale* (d'ora in avanti citato come CAD) e dell'art. 7 del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - *Regole tecniche in materia di sistema di conservazione* (d'ora in avanti citato come *Regole tecniche in materia di sistema di conservazione*), il commissario straordinario nella competenza della Giunta comunale ha nominato con Deliberazione n. 172 del 18 maggio 2017 il Responsabile della conservazione ed il Responsabile della funzione archivistica della conservazione.

I compiti del Responsabile della conservazione sono:

- a) definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- b) gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
- c) generare il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
- j) assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) predisporre il manuale di conservazione di cui all'art. 8 e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Ai sensi dell'art. 6, comma 6, il Responsabile della conservazione può delegare, con atto formale, lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate.

### **1.5.3 Responsabile della transizione al digitale**

A norma dell'art. 17 del CAD, la Giunta comunale nomina con propria Deliberazione il Responsabile della transizione al digitale quale responsabile dell'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Regole tecniche di cui all'articolo 71 del CAD.

Al Responsabile della transizione al digitale sono affidati i seguenti compiti:

- a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
- e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
- g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.
- j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

#### **1.5.4 Responsabile della protezione dei dati**

A norma dell'art. 37 del Regolamento Europeo n. 679 del 27 aprile 2016 - *Regolamento generale relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (d'ora in avanti citato come Regolamento EU 2016/679 - *GDPR*), il

Capo settore Risorse umane con Determinazione n. 101 del 21 maggio 2018 ha affidato l'incarico di Responsabile della protezione dei dati personali per lo svolgimento dei seguenti compiti:

- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d) cooperare con l'autorità di controllo;
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

## **1.6 Sistema di protocollo informatico unico e strumenti per il suo funzionamento**

Il Comune di Padova, avendo individuato un'unica AOO, si serve di un unico sistema di protocollo informatico denominato p@doc, utilizzato da tutte le UOR dell'Ente.

Il protocollo informatico unico è lo strumento attraverso il quale l'Ente garantisce l'effettiva ricezione e trasmissione dei documenti. Con la messa a regime di tale sistema è cessata di fatto la necessità di mantenere tutti i cosiddetti protocolli interni (protocolli di settore, servizio, ufficio, etc., protocolli multipli, protocolli del telefax, etc.) di cui è vietato l'utilizzo.

Il protocollo informatico unico si serve degli strumenti di gestione quali il titolare di classificazione, l'oggettario, l'organigramma, il repertorio dei fascicoli, il piano di fascicolazione e il piano di conservazione, descritti nei successivi capitoli.

## **1.7 Politiche di gestione e conservazione documentale**

Le politiche di gestione e conservazione del Comune di Padova sono definite in base alla vigente normativa, con particolare riferimento al Decreto Legislativo 22 gennaio 2004, n.42 - *Codice dei Beni culturali e del Paesaggio* (d'ora in avanti citato come *Codice dei beni culturali e del paesaggio*) e al CAD, e tengono conto dell'evoluzione tecnologica e dell'organizzazione interna dell'Ente al fine

di programmare adeguatamente e di progettare l'implementazione dei sistemi di gestione documentale.

La gestione e la conservazione hanno come obiettivo la tutela dei documenti nel loro valore giuridico-probatorio mantenendone l'integrità e affidabilità, e la valorizzazione finalizzata alla fruibilità a scopi storici delle informazioni e dei dati contenuti nei documenti.

## 2. PROTEZIONE DEI DATI PERSONALI E PIANO DI SICUREZZA

Il presente capitolo, ai sensi dell'art. 4, comma c), e dell'art. 7 delle *Regole tecniche per il protocollo informatico*, riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

### 2.1 Contesto

Il contesto normativo ha subito un'importante trasformazione dovuta dall'entrata in vigore del Regolamento EU 2016/679 - *GDPR*. Attraverso il D.Lgs 101/2018 il legislatore italiano ha armonizzato il Decreto legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali* alla norma europea, determinando un nuovo approccio alla sicurezza e alla privacy attraverso il concetto di *accountability*, intesa come responsabilizzazione e possibilità di dimostrare che il titolare del trattamento abbia messo in atto misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento EU 2016/679 - *GDPR*). In questo contesto il Comune di Padova ha avviato un percorso volto all'implementazione di un sistema per la corretta gestione della componente di sicurezza e di protezione del dato, partendo dalle regole e dalle politiche di sicurezza già condivise quali:

- il *Regolamento per l'utilizzo degli strumenti informatici e telematici del Comune di Padova* approvato con Deliberazione di Giunta Comunale n. 324 del 29/06/2010;
- il *Documento programmatico per la sicurezza – DPS*, redatto e approvato dal Comune di Padova con Deliberazione della Giunta Comunale n. 175 del 17 aprile 2012.

All'interno del piano di sicurezza verranno illustrate le soluzioni organizzative implementate volte a garantire la disponibilità, la riservatezza e l'integrità dei documenti e a dimostrare la conformità al principio di *accountability*.

### 2.2 Il principio di *accountability* ed il registro delle attività di trattamento

Il principio di *accountability* non fa riferimento solamente al rispetto delle regole dettate dal Regolamento EU 2016/679 - *GDPR*, ma anche alla capacità di comprovare e dimostrare che il trattamento avvenga secondo i principi del Regolamento, ossia che i dati siano:

- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati rispetto alle finalità (minimizzazione dei dati);
- esatti e, se necessario, aggiornati (esattezza);

- limitati nella conservazione;
- trattati garantendo integrità e riservatezza.

Nel processo di trasformazione digitale previsto dal CAD, il Comune di Padova ha costituito una base informativa dei procedimenti esistenti all'interno dell'Ente attraverso la realizzazione del censimento delle istanze e dei documenti. Il censimento si configura come uno strumento di rilevazione della produzione documentale dal punto di vista quantitativo e qualitativo (conformità alle regole tecniche e agli standard), che permette la definizione degli attori coinvolti nei processi, le responsabilità e gli strumenti di produzione utilizzati.

In adempimento all'art. 30 del Regolamento EU 2016/679 - *GDPR*, questa base informativa è stata successivamente implementata con i dati inerenti al registro delle attività di trattamento e nello specifico:

- Procedimento /attività di trattamento;
- Finalità del trattamento;
- Tipologia di trattamento;
- Interessati;
- Tipologie di dati personali trattati;
- Destinatari delle categorie di dati raccolti;
- Eventuali trasferimenti a soggetti extra UE;
- Base giuridica del trattamento;
- Termini per la conservazione del dato;
- Supporti e banche dati interne utilizzati per il trattamento;
- Supporti e banche dati esterne utilizzati per il trattamento;
- Presenza dell'informativa;
- Co-titolarietà del trattamento;
- Soggetti / settori interni autorizzati al trattamento;
- Responsabili esterni del trattamento;
- Misure di sicurezza informatiche adottate;
- Misure di sicurezza organizzative adottate;
- Eventuale valutazione di impatto.

In accordo con la necessità di avere uno strumento dinamico di responsabilizzazione e corrispondente alla realtà organizzativa, questa banca dati viene popolata e aggiornata periodicamente sia per quanto riguarda i processi documentali che per i trattamenti in essere all'interno di ogni Settore. Con cadenza semestrale i registri sono consolidati, sottoscritti e registrati dal titolare del trattamento (Comune di Padova – Sindaco) e dai responsabili (Settore del Comune di Padova -Caposettore).

## 2.3 Il piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal Comune di Padova siano resi disponibili, autentici e integri;
- i dati personali, le categorie particolari di dati personali (art. 9 del Regolamento EU 2016/679 - *GDPR*) e i dati personali relativi a condanne penali e reati (art. 10 del Regolamento EU 2016/679 - *GDPR*) vengano custoditi in modo da ridurre al minimo, mediante l'adozione di adeguate e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati personali e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune di Padova;
- le modalità di accesso al sistema di protocollo e gestione documentale;
- le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, il Comune di Padova ha adottato le misure tecniche e organizzative di seguito specificate:

- protezione periferica dell'intranet dell'Amministrazione;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio
- piano di continuità del servizio che prevede:
  - l'esecuzione e la gestione delle copie di riserva dei dati e dei documenti effettuate con modalità sincrona e cadenza giornaliera;
  - la capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura dei Servizi informatici, delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- gestione delle situazioni di emergenza informatica attraverso risorse qualificate;
- impiego e manutenzione di un adeguato sistema antivirus;



- uso di soluzioni volte a rendere inintelligibili, a chi non è autorizzato ad accedervi, le particolari categorie di dati personali contenuti in elenchi, registri o banche di dati;
- impiego di adeguate misure di sicurezza anche nel caso di supporti analogici contenenti categorie particolari di dati;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultabili in caso di necessità per controlli da parte delle autorità competenti.

### **2.3.1 Formazione dei documenti - Aspetti di sicurezza**

Le risorse strumentali e le procedure atte a garantire la sicurezza nella formazione dei documenti informatici, con particolare riferimento alla loro immodificabilità e integrità, sono descritte nel capitolo 3 - *Modalità di formazione dei documenti*.

Inoltre, il Comune di Padova utilizza piattaforme di condivisione delle principali regole di formazione del documento informatico che garantiscono anche l'aspetto della sicurezza.

### **2.3.2 Gestione dei documenti informatici - Aspetti di sicurezza**

I documenti del Comune di Padova vengono gestiti attraverso il sistema di protocollo e gestione documentale p@doc, conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

### 2.3.2.1 Componente organizzativa della sicurezza

Tale componente consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte dal sistema informatico p@doc.

In tale contesto la gestione della sicurezza si realizza con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia e con attività di controllo e verifica essenziali ad assicurare l'efficacia nel tempo del sistema informatico.

Conseguentemente vengono adottate le seguenti misure di sicurezza, la cui competenza è posta a carico dei seguenti settori del Comune di Padova:

Misure di sicurezza	Settore responsabile dei controlli
Sicurezza Fisica e infrastrutturale	- Settore Lavori pubblici - Settore Servizi Informatici e Telematici
Sicurezza Logica	- Settore Servizi Informatici e Telematici
Sicurezza Organizzativa	- Settore Servizi Informatici e Telematici - Settore Servizi Istituzionali - Settore Risorse umane

Nello specifico sono individuati i seguenti ruoli:

- Responsabile del protocollo informatico e della gestione documentale;
- Responsabile della conservazione;
- Responsabile della protezione dei dati personali;
- Responsabile delle reti e della sicurezza informatica;
- Amministratore del sistema di protocollo informatico.

Per la gestione organizzativa del sistema di sicurezza il Comune di Padova si avvale inoltre di gruppi di lavoro tematici istituiti formalmente.

### 2.3.2.2 Componente fisica e infrastrutturale della sicurezza

La sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informativo è garantita dalle seguenti misure:

- porte blindate;
- armadi ignifughi;
- impianti elettrici dedicati;
- sistemi di condizionamento per il raffreddamento delle apparecchiature;
- gruppo di continuità elettrica;
- controllo periodico su efficienza del gruppo elettrogeno;
- estintori;
- piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori;

- impianto antincendio nella sala macchine presso il Settore Servizi Informatici e Telematici;
- accesso ai locali mediante sistema d'autenticazione tramite badge e chiave;
- impianto antintrusione autonomo per gli accessi al locale sala macchine.

### 2.3.2.3 Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del sistema di gestione documentale, si realizza attraverso:

- identificazione e autenticazione utente;
- profilazione degli accessi (ACL);
- politica antivirus;
- firma digitale;
- monitoraggio sessioni di lavoro;
- disponibilità del software e dell'hardware.

Nello specifico, p@doc è una *web-application* e come tale presenta una architettura di tipo *client-server*.

Il software è progettato e sviluppato secondo l'architettura *three-tier* (a tre livelli) che prevede la suddivisione dell'applicazione in tre diversi moduli (livelli):

1. interfaccia utente
2. logica funzionale/*business logic* (*application server*)
3. dati persistenti (*database/repository file*)

Le possibili interazioni fra i livelli sono vincolate secondo quanto segue:

- interfaccia utente ↔ logica funzionale
- logica funzionale ↔ dati persistenti

Il livello "interfaccia utente" non può quindi relazionarsi direttamente con il livello "dati persistenti" (e viceversa).

Gli utenti (*clients*) usufruiscono dell'applicazione interagendo con l'interfaccia utente per mezzo di un *browser* installato nella propria postazione di lavoro (PdL) e della rete locale (intranet) del Comune di Padova.

Il software (logica funzionale) e le informazioni gestite (dati persistenti) risiedono in un sistema centralizzato presso il Settore Servizi Informatici e Telematici e costituito da server dedicati e sostanzialmente specializzati nelle seguenti funzioni:

- *application server*;
- *DBMS*;

- *repository file*.

Tale architettura permette di aumentare la modularità ed il livello di sicurezza del sistema.

L'utilizzo delle PdL e della rete intranet è garantito ai soli utenti dotati di credenziali d'accesso (user ID + password) al sistema informatico del Comune di Padova.

L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche autorizzazioni di accesso al sistema p@doc.

L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso; funzioni e dati ai quali l'utente non è autorizzato ad accedere non vengono resi disponibili.

Agli utenti "generici" del Comune di Padova non è quindi consentito:

- interrogare direttamente il DBMS;
- interagire direttamente con il repository dei file;
- accedere direttamente ai server fisici e virtualizzati.

Le precedenti operazioni sono possibili ai soli soggetti autorizzati ed appartenenti al Settore Servizi Informatici e Telematici per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.

Nessun sistema, componente, servizio ed interfaccia inerente al sistema p@doc è direttamente accessibile e fruibile dalla rete pubblica *internet*.

### **2.3.3 Gestione delle registrazioni di protocollo e di sicurezza**

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitati su p@doc o altri indipendenti sistemi di supporto - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza possono essere costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (*Intrusion Detection System (IDS)*, sensori di rete e *firewall*);
- dalle registrazioni di p@doc.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- scrittura su database in modalità asincrona (scrittura logica che coincide con scrittura fisica sul disco);
- copie di backup realizzate su dischi RAID in mirroring e RAID 5;
- consegna di una copia di sicurezza dei back up in un locale diverso come previsto dalla normativa;
- scrittura sincrona dei file su storage ospitato in altra sede;

- accesso alle registrazioni limitato esclusivamente agli amministratori di sistema del sistema di protocollo, al Responsabile della gestione documentale e ai soggetti istruiti e autorizzati;
- conservazione dei supporti con le registrazioni di sicurezza all'interno di un locale con accesso limitato ai soli addetti.

### 2.3.4 Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni del Comune di Padova l'accesso ai servizi previsti, mediante l'adozione di un insieme di misure organizzative e tecnologiche.

Gli utenti interni autorizzati ad utilizzare il software p@doc, operano nel rispetto del "Regolamento per l'utilizzo degli strumenti informatici e telematici del Comune di Padova" approvato con Deliberazione di Giunta Comunale n. 324 del 29/06/2010, che in riferimento alla sicurezza nell'utilizzo delle risorse tecnologiche, prevede quanto segue:

- ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati ai fini istituzionali;
- ogni utente è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali.
- ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. È vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus;
- I dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative;
- La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare con frequenza opportuna i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti;
- Tutti i dati sensibili riprodotti su supporti magnetici (e informatici, *ndr.*), devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto;
- L'account del sistema p@doc è costituito da un codice identificativo personale (username) e da una parola chiave (password);
- La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile;
- Le password dovranno avere le seguenti caratteristiche:
  - lunghezza minima 8 caratteri;

- caratteri di tipo alfanumerico e deve contenere almeno un numero, una lettera minuscola e una lettera maiuscola (non si possono usare simboli);
- non deve essere riconducibile a:
  - nome o cognome proprio o di un collega o di un familiare;
  - identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo;
  - date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione;
- validità 90 giorni.

## 2.4 Trasmissione e interscambio dei documenti informatici - Aspetti di sicurezza

Il Comune di Padova utilizza tecnologie di trasmissione con i seguenti livelli di sicurezza:

Tipologia di trasmissione	Caratteristiche	Livello di sicurezza
Posta elettronica Certificata	<ul style="list-style-type: none"> <li>- identità sicura e accertata del titolare della casella / mittente;</li> <li>- transito del messaggio attraverso il protocollo S-HTTP Mime che garantisce la piena riservatezza;</li> <li>- sicurezza dell'accettazione e consegna del messaggio attraverso l'utilizzo delle ricevute;</li> <li>- tracciamento delle attività nel file di Log a carico del gestore del servizio e conservazione dei registri per 30 mesi.</li> </ul>	Alto
Canali Web - Istanze online	<ul style="list-style-type: none"> <li>- accesso ai servizi previa autenticazione sicura del mittente;</li> <li>- utilizzo del protocollo HTTPS che garantisce la piena riservatezza.</li> </ul>	Alto
Interoperabilità	<ul style="list-style-type: none"> <li>- meccanismo di trasmissione attraverso la Posta elettronica certificata con funzionalità interoperabili.</li> </ul>	Alto
Posta elettronica ordinaria	<ul style="list-style-type: none"> <li>- identità del titolare della casella non accertata da un ISP (Internet server provider) accreditato;</li> <li>- transito del messaggio attraverso un protocollo SMTP che non garantisce la riservatezza della trasmissione.</li> </ul>	Basso

Fax server	- meccanismo di trasmissione che utilizza la tecnologia della posta elettronica ordinaria.	Basso
------------	--	-------

## 2.5 Accesso ai documenti informatici – Aspetti di sicurezza

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso pubblica e privata ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

Per le specifiche relative alla sicurezza per l'accesso degli utenti interni alla AOO al sistema di protocollo e di gestione documentale p@doc, si fa riferimento al capitolo 7 - *Descrizione del sistema di protocollo informatico*.

Attualmente non sono disponibili funzioni per l'accesso al sistema da parte di utenti esterni all'AOO; l'esercizio, per via telematica, del diritto di accesso ai documenti è disponibile attraverso altre modalità descritte nel capitolo 9 – *Procedimenti amministrativi, accesso ai documenti e tutela della riservatezza*

## 2.6 Conservazione dei documenti informatici – aspetti di sicurezza

Per la conservazione dei documenti informatici si rimanda al Manuale della Conservazione del Comune di Padova approvato con Deliberazione del Commissario Straordinario nella competenza della Giunta Comunale n. 2017/0172 del 18/05/2017.

## 2.7 Politiche di sicurezza adottate dall'Ente

Le politiche di sicurezza vengono definite dai documenti citati nel paragrafo 2.1 e periodicamente riesaminate nella procedura di valutazione di impatto sulla protezione dei dati (*Data protection impact assessment*) in conformità al Regolamento EU 2016/679 – *GDPR* e alla norma ISO 29134 – *Information Technology – Security Techniques – Guidelines for privacy impact assessment*.

Il sistema p@doc è soggetto a periodica valutazione di impatto al fine di monitorare la conformità dei trattamenti. Il processo di valutazione di impatto, che si attua quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, permette di identificare i controlli esistenti e pianificati e i rischi legati gli accessi illegittimi, alle modifiche indesiderate e alla scomparsa dei dati.

Come previsto dal provvedimento 393, 2 luglio 2015 del Garante della protezione dei dati personali, le amministrazioni pubbliche sono tenute a comunicare al Garante le violazioni dei dati personali (data breach) che si verificano nell'ambito delle banche dati di cui sono titolari, secondo

la compilazione del modulo predisposto dal Garante (*Allegato 3 - Modello di segnalazione data breach PA*).

## **2.8 Verifica della conformità, miglioramento della sicurezza dei dati e responsabile della protezione dei dati**

La verifica della conformità della sicurezza dei dati viene svolta periodicamente dai soggetti individuati nel paragrafo 2.3.2.1 *Componente organizzativa della sicurezza*. In base al principio di responsabilizzazione, e nell'ambito del sistema di protocollo informatico e di gestione documentale, il Comune di Padova ha previsto la messa in atto di azioni volte alla minimizzazione del rischio al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato.

Queste azioni prevedono il monitoraggio dei dati, dei documenti e dei metadati registrati all'interno del sistema, al fine di minimizzare i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Inoltre, ai sensi dell'articolo 37 del Regolamento UE 2016/679 - *GDPR*, il Comune di Padova ha nominato il responsabile della protezione dei dati, i cui compiti sono descritti nel paragrafo 1.5.4. *Responsabile della protezione dei dati*.



## 3. FORMAZIONE DEI DOCUMENTI

### 3.1 I documenti del Comune di Padova

I documenti del Comune di Padova (d'ora in poi chiamati semplicemente documenti) sono quelli formati, in uno dei modi previsti dalla normativa vigente, dagli organi ed uffici del Comune medesimo nello svolgimento della loro attività istituzionale e costituiscono l'archivio del Comune nel rispetto dei principi archivistici.

In ottemperanza a quanto indicato dal CAD, che prevede l'uso delle tecnologie dell'informazione e della comunicazione per organizzare la propria attività amministrativa, il Comune di Padova forma i suoi documenti originali su supporto informatico.

Per agevolare il processo di formazione da parte dei cittadini di documenti informatici e consentire la trattazione automatica dei dati in essi contenuti, il Comune di Padova rende disponibili moduli accessibili dal sito istituzionale e dalle piattaforme on-line.

### 3.2 Formazione dei documenti - Elementi informativi essenziali

I seguenti elementi informativi essenziali devono essere riportati o associati ai documenti formati dal Comune di Padova:

<b>Autore</b>	<ul style="list-style-type: none"><li>- Stemma e dicitura del Comune di Padova;</li><li>- Unità organizzativa Responsabile / Ufficio e servizio;</li><li>- Dati fiscali (Codice fiscale e partita IVA);</li><li>- Dati di contatto (Indirizzo, recapito telefonico, Indirizzo istituzionale di posta elettronica certificata, indirizzo di posta elettronica certificata, eventuali orari di apertura al pubblico).</li></ul>
<b>Estremi di registrazione</b>	<ul style="list-style-type: none"><li>- Data e numero di registrazione (di protocollo e/o di repertorio);</li><li>- Eventuale indice di classificazione;</li><li>- Eventuali numero e data del documento cui si risponde.</li></ul>
<b>Destinatario (Eventuale)</b>	<ul style="list-style-type: none"><li>- Cognome e Nome / Denominazione / UOR.</li></ul> <p>A seconda dei casi:</p> <ul style="list-style-type: none"><li>- Domicilio digitale (Indirizzo di posta elettronica certificata);</li><li>- Indirizzo per il recapito postale completo (via/piazza, numero civico, cap, città);</li><li>- Indirizzo di posta elettronica precedentemente dichiarato dal destinatario.</li></ul>
<b>Oggetto</b>	<ul style="list-style-type: none"><li>- Indica la funzione del documento in maniera sintetica ma</li></ul>

	esaustiva.
<b>RPA</b>	- Cognome e nome del Responsabile del procedimento amministrativo.
<b>Firma</b>	A seconda dei casi: - firma digitale; - altri tipi di firma.

### 3.3 Formazione dei documenti - aspetti operativi generali

I documenti del Comune di Padova sono prodotti generalmente con adeguati sistemi informatici.

Ogni documento amministrativo:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;
- è associato in modo univoco ad un protocollo e/o repertorio;
- fa riferimento ad uno o più fascicoli.

### 3.4 Formazione del documento informatico e del documento amministrativo informatico

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

Il documento informatico viene formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

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

- sottoscrizione con firma digitale, ovvero con firma elettronica qualificata;
- apposizione di una validazione temporale;
- 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.

### 3.4.1 Metadati

I metadati sono l'insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

Al documento informatico immodificabile e ai documenti soggetti a registrazione particolare vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, previsti dalla normativa, è costituito da:

- Identificativo univoco e persistente
- Riferimento temporale
- Oggetto
- Soggetto che ha formato il documento
- Destinatario
- Impronta del documento informatico
- Metadati aggiuntivi stabiliti dal Comune di Padova a fini gestionali e conservativi

Nel caso specifico del documento amministrativo informatico l'insieme di metadati minimi, associati al documento nel momento della registrazione a protocollo in quanto contenuti nell'impronta .xml della segnatura, è descritto nel paragrafo 5 del capitolo 5 - *La segnatura di protocollo*.

I metadati aggiuntivi stabiliti dal Comune di Padova a fini amministrativi, gestionali e conservativi sono quelli associabili al documento nel momento della sua produzione, attraverso gli strumenti e le opzioni disponibili nel software di editing:

- Dati utente collegati al metadato 'Autore' del documento:

- A. Ente per cui si lavora ('Azienda')
- B. Utente ('Nome', 'Cognome', 'Iniziali')
- C. Indirizzo e contatti del luogo di lavoro ('Via', 'C.A.P.', 'Località', 'Paese/Regione', 'Titolo/posizione', 'Telefono Lavoro', 'E-mail').

- Dati proprietà documento edito:

- A. Autore
- B. Titolo
- C. Oggetto
- D. Parole chiave
- E. commenti (eventuale)

Nel caso di documenti soggetti a registrazione particolare l'insieme minimo di metadati associati al documento nel momento della sua registrazione a repertorio è descritto nell'*Allegato 4 – Metadati dei documenti soggetti a registrazione particolare*.

### **3.4.2 Sottoscrizione dei documenti**

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con processi di firma elettronica conformi alle disposizioni dettate dalla normativa vigente.

Il Comune di Padova utilizza la firma qualificata (firma digitale) come forma di sottoscrizione per garantire i requisiti di integrità, riservatezza e non ripudiabilità nei confronti di entità esterne. Per favorire l'accessibilità e la portabilità dei documenti firmati digitalmente si utilizza il formato PadES, se non previsto diversamente dalla norma.

Il Comune di Padova si avvale dei servizi di un'autorità di certificazione iscritta nell'elenco pubblico dei certificatori accreditati tenuto dall'Agenzia per l'Italia Digitale.

Le verifiche delle firme digitali dei documenti prodotti o ricevuti avviene attraverso l'utilizzo di software rilasciati gratuitamente, secondo la normativa, da enti certificatori.

Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna il Comune di Padova, nella propria autonomia organizzativa, adotta forme diverse dalla firma digitale previste dal Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*.

### **3.4.3 Riferimento temporale**

Per tutte le casistiche per cui la normativa prevede l'apposizione di un riferimento temporale, il Comune di Padova adotta almeno una delle seguenti modalità:

- registrazione di protocollo;
- posta elettronica certificata;
- servizio di marca temporale da Certificatore accreditato.

### 3.4.4 Tipologie di formato del documento informatico

Il Comune di Padova, in considerazione di quanto previsto dal DPCM 3 dicembre 2013 in materia di conservazione, al fine di garantire le caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione, adotta i seguenti formati:

FORMATO	ESTENSIONE	STANDARD DI RIFERIMENTO
PDF - PDF/A	.pdf	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	ISO 12639 ISO 12234
JPG	.jpeg, .jpg	ISO/IEC 10918:1
Office Open XML (OOXML)	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008
Open Document Format	.odt, .ods, .odp, .odg, .odb	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
XML	.xml  derivati da XML: .svg	ISO 8879 - SGML Specifiche W3C
TXT	.txt	/
formati messaggi di posta elettronica	.eml	RFC 2822 - MIME RFC 1847 - S/MIME
AutoCAD DXF	.dxf	proprietario ma con specifiche rilasciate da Autodesk
M4a	.m4a, .m4b, .mp4	ISO/IEC 14496-14
MP3	.mp3	ISO/IEC 11172-3 ISO/IEC 13818-3
WAV	.wav	rilasciato da IBM e Microsoft. estensione del Resource Interchange File Format (.RIFF)

I documenti informatici prodotti dal Comune di Padova, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti nel formato standard PDF/A, salvo nei casi in cui è previsto un formato diverso, al fine di garantirne l'immodificabilità e la corretta archiviazione.

Eventuali integrazioni al presente elenco vengono definite in considerazione di specifiche previsioni normative o tecniche.

Nell'ambito di alcuni specifici contesti operativi vengono definiti alcuni casi eccezionali dove si prevede l'utilizzo di formati diversi da quelli adottati. Queste eccezioni riguardano i documenti sia ricevuti che prodotti dall'ente e si determinano in base ai seguenti criteri:

- **Norma:** una norma, legge o regolamento che definisce l'utilizzo di un particolare formato diverso da quelli adottati;
- **Autenticità del documento:** caratteristica di un documento informatico che fornisce la garanzia che il documento sia ciò che dichiara di essere, senza aver subito alterazioni o modifiche. E' l'insieme di identità (identificazione e provenienza) e integrità;
- **Affidabilità:** livello di fiducia che l'utente ripone nel documento informatico;
- **Rilevanza:** rilevanza e importanza del documento ricevuto;
- **Tipologia e diffusione di formato:** viene valutata la diffusione del formato, la riconoscibilità e l'eventuale minaccia rappresentata dal file (ad esempio per i file .exe).

I casi eccezionali di gestione di ulteriori formati sono definiti dall' *Allegato 5 – Ulteriori formati utilizzati*.

Periodicamente viene svolta una verifica all'interno del sistema volta a rilevare la non conformità dei documenti ricevuti e prodotti. I dati rilevati vengono comunicati al responsabile dell'unità organizzativa.

## 4. SCAMBIO DEI DOCUMENTI

Il presente capitolo fornisce indicazioni per lo scambio di documenti all'interno ed all'esterno dell'AOO. L'assegnazione dei documenti informatici si effettua all'interno di ciascuna UOR competente sotto la responsabilità dirigenziale di cui all'art. 5 comma 2 della L. 241/1990.

Si descrivono di seguito le procedure operative per lo scambio di documenti ricevuti (documenti in entrata), inviati (documenti in uscita) e interni (formali e informali).

### 4.1 Documenti in entrata

I documenti ricevuti su supporto analogico recapitati attraverso:

- **Posta convenzionale e posta raccomandata:** consegna dei documenti analogici ricevuti tramite il servizio postale presso la casella postale del Comune di Padova;
- **Brevi Manu:** consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata allo sportello del Protocollo generale o agli altri uffici delle UOR aperti al pubblico durante l'orario di apertura;

sono sottoposti al processo di registrazione, scansione e inserimento all'interno del sistema di protocollo informatico, tramite il quale sono successivamente smistati.

I documenti informatici trasmessi per mezzo di:

- **caselle di posta elettronica istituzionale:** account di posta elettronica del Protocollo generale e delle UOR del Comune di Padova collegati al sistema di protocollo informatico, disponibili sul sito istituzionale [www.padovanet.it](http://www.padovanet.it);
- **caselle PEC (Posta elettronica certificata):** account di posta elettronica certificata del Protocollo generale e delle UOR del Comune di Padova collegati al sistema di protocollo informatico, disponibili sul sito istituzionale [www.padovanet.it](http://www.padovanet.it);
- **Canali Web:** il Comune di Padova è dotato di un portale web, raggiungibile all'indirizzo <https://istanzeonline.comune.padova.it>, attraverso il quale il cittadino può presentare istanze e richieste;
- **Fax server:** servizio di fax virtuale che utilizza account di posta elettronica collegati al sistema di protocollo informatico;
- **Eventuali canali informativi cooperativi;**

sono sottoposti al processo di registrazione e vengono acquisiti all'interno del sistema di protocollo informatico, attraverso il quale sono successivamente smistati.

## 4.2 Documenti in uscita

Le comunicazioni verso le pubbliche amministrazioni, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese avvengono sempre attraverso la posta elettronica certificata.

Ai sensi dell'art. 3-bis del CAD, in caso di domicilio digitale eletto, le comunicazioni verso i cittadini avvengono attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato.

Per la trasmissione dei documenti prodotti in origine su supporto analogico, ossia i documenti prodotti prima dell'entrata in vigore degli obblighi previsti dall'articolo 17 del Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 – *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni*, si applica il regime delle copie informatiche di documenti originali analogici, ai sensi dell'articolo 22 del CAD.

In sintesi, i documenti originali informatici sono trasmessi attraverso:

- Posta elettronica certificata
- Caselle di Posta elettronica
- Fax server
- Eventuali canali informativi cooperativi

Nel caso in cui il cittadino sia sprovvisto di domicilio digitale, possono utilizzarsi strumenti di trasmissione informatici alternativi e dichiarati dallo stesso. Nel caso in cui il cittadino sia sprovvisto di qualsiasi canale di trasmissione informatico o richieda di ricevere il documento su supporto cartaceo si applica il regime delle copie analogiche dei documenti originali informatici, ai sensi degli articoli 3-bis, 23 e 23-ter del CAD.

Le copie analogiche dei documenti originali informatici sono trasmessi attraverso:

- Posta convenzionale o posta raccomandata
- Brevi Manu
- Notifica

## 4.3 Documenti interni

I documenti interni, cioè i documenti prodotti e destinati all'interno dell' AOO Comune di Padova si distinguono in formali e informali.

I documenti interni sono formati con tecnologie informatiche.



### **4.3.1 Documenti interni formali**

La trasmissione tra UOR di documenti informatici formali avviene per mezzo del sistema di gestione documentale p@doc.

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.

### **4.3.2 Documenti interni informali**

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: Imol, E-ticket, CRM, storage condiviso.

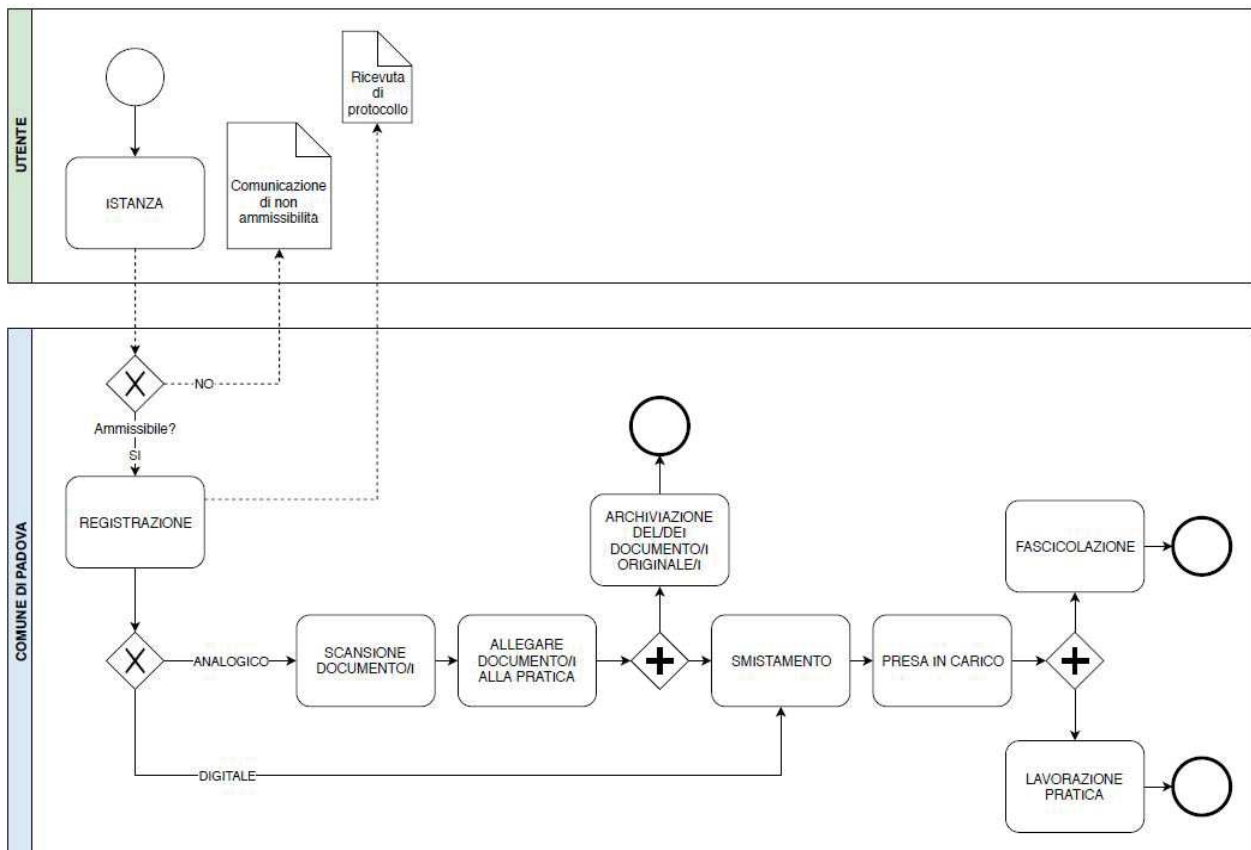
## **4.4 Descrizione del flusso di lavorazione dei documenti**

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni attraverso i diagrammi di flussi riportati nelle pagine seguenti.

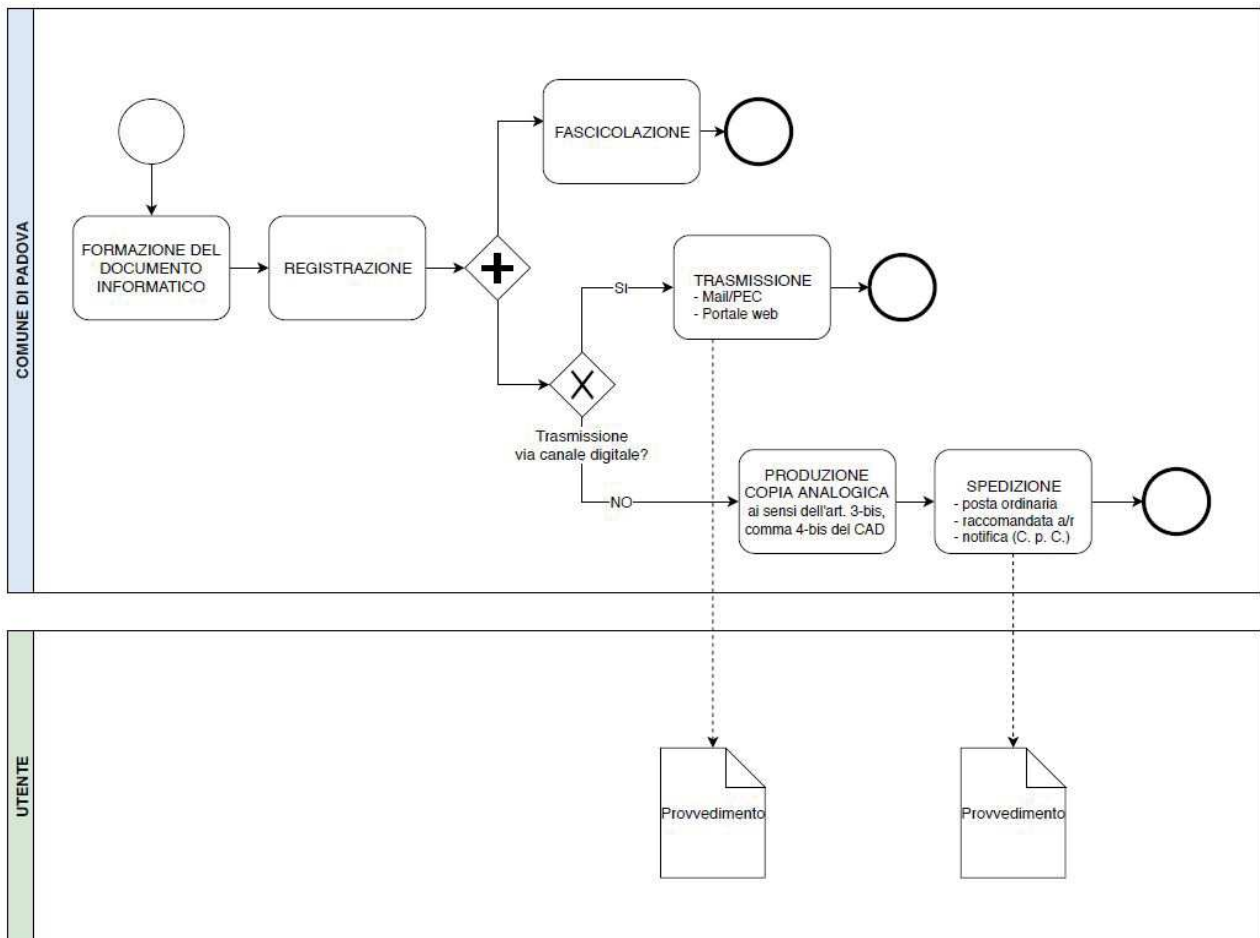
Essi si riferiscono ai documenti:

- ricevuti dal Comune di Padova, dall'esterno
- inviati dal Comune di Padova, all'esterno

#### 4.4.1 Flusso in entrata



## 4.4.2 Flusso in uscita



## **5. PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO**

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni di annullamento o di modifica nell'ambito di ogni sessione di attività di registrazione.

Il Comune di Padova utilizza il sistema di protocollo informatico e di gestione documentale p@doc.

### **5.1 Registrazione dei documenti**

Tutti i documenti del Comune di Padova, dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul sistema di protocollo informatico, con le modalità e le eccezioni di seguito illustrate.

La registrazione è l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, all'autore e alla modalità di trasmissione di un documento.

Tale operazione serve a identificare in modo univoco un documento individuandone data, forma e provenienza certa.

Anche i documenti soggetti a repertoriatura, tipologia particolare di registrazione, possono essere registrati sul sistema di protocollo informatico.

### **5.2 Registro di protocollo**

Il registro di protocollo è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa.

Nell'ambito della AOO Comune di Padova il registro di protocollo è unico e la sua numerazione, unica e progressiva, è costituita da sette cifre numeriche e si chiude al 31 dicembre di ogni anno per ripartire all'anno successivo dal numero 1, come previsto dalle vigenti norme.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

La registrazione a protocollo attesta l'esistenza giuridica di un documento presso l'amministrazione che lo ha prodotto o ricevuto, fatti salvi i casi di annullamento definiti al successivo paragrafo 5.7.5.  
*- Annullamento delle registrazioni di protocollo.*

Non è consentita la registrazione a protocollo di documenti non ancora esistenti, cioè che non siano ancora stati prodotti o perfezionati con la sottoscrizione (nel caso di documenti in uscita), eseguita al solo scopo di “prenotare” un numero di protocollo fissandone la data e l’ora.

Non è consentita la registrazione dei documenti mediante l’assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti.

Non è consentita altresì la protocollazione di un documento già protocollato, salvo casi inevitabili di invii multipli da parte del mittente (per tali casi si veda il successivo paragrafo 5.8.9. - *Trattamento dello stesso documento inviato o consegnato a diverse UOR dell’Ente o pervenuto attraverso canali diversi*).

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell’effettivo ricevimento e spedizione (sia esterna che interna) di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Ai sensi dell’art. 7 comma 5 delle *Regole tecniche per il protocollo informatico*, il registro giornaliero di protocollo deve essere trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l’immodificabilità del contenuto.

Per finalità di consultazione e ricerca interna viene prodotta una stampa annuale e consolidata del registro di protocollo.

## 5.3 Elementi della registrazione di protocollo

Gli elementi obbligatori, in quanto giuridicamente rilevanti della registrazione a protocollo sono:

- data di registrazione;
- numero di protocollo;
- corrispondente (mittente per il documento in entrata/destinatario per il documento in uscita/corrispondente interno per i documenti interni)
- oggetto;
- impronta;
- indice di classificazione.

Gli elementi non obbligatori, ma funzionali qualora disponibili sono:

- livello di riservatezza;
- numero di protocollo del documento ricevuto;
- data del documento ricevuto;
- modalità di trasmissione;
- numero raccomandata;
- data raccomandata;

- annotazioni.

## 5.4 Modalità di registrazione di protocollo e di assegnazione

I documenti pervenuti al Comune di Padova da soggetti esterni sono registrati una sola volta, salvo casi di invii multipli non individuabili da colui che registra il documento in entrata.

I documenti inviati dal Comune di Padova ad altri soggetti esterni sono registrati una sola volta come documenti in uscita.

I documenti interni formali, inviati da una UOR ad un'altra UOR all'interno del Comune di Padova (oppure da un ufficio all'altro all'interno della stessa UOR), devono essere registrati a protocollo una sola volta dalla UOR mittente come documenti interni.

In seguito alla registrazione, i documenti informatici vengono acquisiti nel sistema di protocollo attraverso le modalità descritte nel capitolo 4 – *Scambio dei documenti*; nei casi residuali previsti, i documenti analogici vengono acquisiti nel sistema di protocollo tramite procedura di scansione. In entrambi i casi i documenti vengono assegnati alla UOR competente con le modalità operative descritte al successivo paragrafo 5.10. - *Modalità operative per lo smistamento*.

## 5.5 La segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni minime previste ai sensi del DPCM 3 dicembre 2013 sono:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro;
- progressivo registrazione;
- data di registrazione.

Ulteriori informazioni previste sono:

- indicazione della UOR del Comune di Padova responsabile del documento prodotto;
- 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), 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.

Qualora il documento venga ricevuto in formato analogico, al termine della registrazione viene apposta la segnatura anche tramite timbro o etichetta (le cui informazioni sono il risultato dell'estrazione delle informazioni minime contenute nella segnatura informatica). L'etichetta riporta l'identificazione della AOO, il tipo di protocollo (entrata, uscita o interno), il numero e la data di protocollo, l'anno, la classificazione, la UOR assegnataria e un codice a barre che contiene l'anno ed il numero di protocollo.

## 5.6 Documenti soggetti a registrazione particolare (Repertoriazione)

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare in appositi repertori o registri le tipologie di documenti riportati nell'*Allegato 6 - Documenti soggetti a registrazione particolare*.

Tale tipo di registrazione particolare consente comunque di eseguire sui documenti le operazioni di gestione documentale, quali la classificazione e la fascicolazione.

Questi documenti appartengono al complesso archivistico del Comune di Padova e concorrono al popolamento del sistema di gestione documentale dell'Ente nell'ottica di una gestione uniforme e coordinata.

I registri o repertori 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);
- eventuali dati di classificazione e di fascicolazione;
- annotazioni.

## 5.7 Procedure specifiche nella registrazione di protocollo

### 5.7.1 Protocolli riservati

Sono previste particolare 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 EU 2016/679 - *GDPR*, 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 ai sensi dell'art. 10 del Regolamento EU 2016/679 - *GDPR* (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 dall'art. 24 della L. 241/1990).

I documenti registrati con tali forme appartengono al cosiddetto protocollo riservato, costituito dalle registrazioni sul sistema di protocollo del Comune il cui accesso è consentito solamente alle persone autorizzate, in rapporto alla tipologie di procedimento amministrativo o alle tipologie documentarie dalle stesse trattate.

Di norma le tipologie di documenti da registrare nel protocollo riservato sono codificate all'interno del sistema di protocollo informatico a cura del Responsabile del Servizio archivistico comunale, di concerto con i responsabili delle UOR che producono o ricevono i documenti. In tutti gli altri casi la definizione della riservatezza è demandata a colui che effettua la registrazione di protocollo.

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati sensibili" e successivamente nelle apposite cassettoni dedicate allo smistamento.

Le procedure adottate per la gestione dei documenti e dei procedimenti amministrativi ad accesso riservato sono le stesse adottate per gli altri documenti e procedimenti amministrativi.

Per approfondimenti sulla sicurezza, sulla protezione dei dati e la riservatezza si rimanda al capitolo 2 - *Protezione dei dati personali e piano di sicurezza*.



## 5.7.2 Documenti esclusi dalla registrazione di protocollo

Il DPR 445/2000 prevede che tutti i documenti in entrata e in uscita e tutti i documenti informatici siano registrati a protocollo, con alcune eccezioni. Tra le eccezioni si annoverano i documenti soggetti a registrazione particolare di cui al precedente paragrafo 5.6. - *Documenti soggetti a registrazione particolare (Repertoriazione)* e i documenti di cui all'*Allegato 7 - Documenti esclusi dalla registrazione di protocollo*.

## 5.7.3 Protocollo differito

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 del Servizio archivistico comunale è autorizzato l'uso del protocollo differito.

Il protocollo differito consiste nel differimento dei termini di registrazione, cioè nel provvedimento con il quale vengono individuati i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il responsabile deve descrivere nel provvedimento.

Le operazioni di differimento consistono in:

- provvedimento di differimento con il quale il Responsabile del Servizio archivistico dispone tempi e modalità della successiva registrazione;
- conservazione sicura in luoghi chiusi dei documenti da registrare a protocollo;
- registrazione dei documenti nei tempi indicati nel provvedimento;
- indicazione nel campo "annotazioni" degli estremi del provvedimento di differimento.

## 5.7.4 Correzioni ortografiche e informazioni aggiunte alle registrazioni

Fermo restando che, in base alla vigente normativa, non sono consentite modifiche alle registrazioni di protocollo, è tuttavia consentita la correzione di meri errori ortografici e del tipo di protocollo (entrata, uscita o interno), o l'aggiunta di dati utili ad eventuali successive ricerche, in termini temporali circoscritti e definiti da disposizioni e provvedimenti interni, adeguatamente pubblicizzati sull'area intranet dell'Ente.

Nel caso in cui, invece, le correzioni da effettuare riguardino il contenuto dei campi non modificabili, è necessario procedere all'annullamento della registrazione tramite la procedura descritta al successivo paragrafo 5.7.5.

## 5.7.5 Annullamento delle registrazioni di protocollo

Le informazioni non modificabili delle registrazioni a protocollo sono annullabili ai sensi dell'art. 54 del DPR 445/2000 e vengono memorizzate nel registro informatico di protocollo restando interamente consultabili insieme agli estremi dell'autorizzazione di annullamento. L'annullamento va richiesto ed effettuato generalmente nei casi di mero errore materiale (ad es. la doppia registrazione, la registrazione di documenti non destinati al Comune di Padova, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'Ente, la registrazione a protocollo errata che necessiterebbe di modifiche sostanziali dei campi obbligatori).

La procedura di annullamento è di competenza dell'Ufficio Protocollo Generale che, con cadenza mensile, esegue una verifica di tutte le richieste di annullamento pervenute tramite il canale di posta elettronica supporto.protocollo@comune.padova.it.

Le richieste di annullamento devono essere motivate a cura dei referenti delle UOR.

L'annullamento non è mai consentito né autorizzato nei casi in cui:

- il protocollo di cui si chiede l'annullamento sia pervenuto in entrata attraverso uno o più canali digitali (PEC, mail istituzionali, fax server, portali);
- il protocollo di cui si chiede l'annullamento sia stato spedito in uscita con esito positivo attraverso uno o più canali digitali (PEC, mail istituzionali, fax server);
- riguardi un numero di protocollo registrato da UOR diversa da quella che richiede l'annullamento.

Le richieste accettate sono inserite in apposito elenco dei numeri di protocollo da annullare unitamente alle relative richieste.

L'elenco viene allegato al provvedimento di annullamento che il Responsabile del Servizio archivistico controlla e autorizza e che viene registrato con protocollo interno. In seguito a tale operazione si può procedere all'annullamento delle registrazioni nel sistema di protocollo. Il sistema registra nella traccia la data e l'ora dell'annullamento e gli estremi del provvedimento di autorizzazione, che devono essere preventivamente indicati dall'operatore che esegue la procedura di annullamento.

Nel documento analogico annullato, si deve riportare a margine il numero di protocollo e la data dell'autorizzazione di annullamento. La segnatura (timbro o etichetta) deve essere barrata con la dicitura *"annullato"*.

## 5.8 Casi particolari di registrazioni di protocollo

### 5.8.1 Lettere anonime

La lettera anonima proveniente tramite i canali postali con contenuto diffamatorio, delatorio, ideologico e/o simile, che non rientri tra i procedimenti dell'Ente, deve essere posta all'attenzione del Segretario/Direttore generale o di persona dallo stesso delegata, che fornisce istruzioni in merito al suo trattamento agli addetti del Protocollo, i quali provvedono secondo le indicazioni ricevute, alla sua registrazione (indicando nel campo mittente "anonimo") ovvero alla sua eliminazione.

### 5.8.2 Segnalazioni anonime

La segnalazione anonima proveniente tramite i canali postali che si riferisce ad atti o fatti afferenti ai compiti di vigilanza, garanzia della sicurezza e dell'ordine pubblico e dalla pubblica incolumità o similari, che può attivare procedimenti dell'Ente, viene protocollata indicando nel campo mittente "*anonimo*" e smistata alla UOR competente.

### 5.8.3 Lettere prive di firma

Le lettere prive di firma ma con mittente dichiarato, devono essere protocollate.

La funzione notarile del protocollo (cioè della registratura) è quella di attestare data e provenienza certa di un documento senza interferire su di esso.

È poi compito della UOR di competenza e, in particolare, del RPA valutare se il documento privo di firma debba ritenersi giuridicamente valido e come tale trattato dall'ufficio assegnatario.

### 5.8.4 Corrispondenza da non aprire

Premesso che la corrispondenza che perviene al Comune di Padova riveste carattere istituzionale, rientra nella normalità del trattamento l'apertura delle buste che recano all'esterno l'indicazione del nominativo di un dipendente, funzionario, dirigente o rappresentante istituzionale (sindaco, vicesindaco, assessore, ecc..).

La corrispondenza con dicitura "*personale*", "*riservata*" o "*s.p.m*", destinata a personale dipendente o a figure istituzionali non deve essere aperta; posto il timbro con la data di pervenimento, è consegnata al destinatario, il quale, dopo averne preso visione, decide se dar seguito alla registrazione a protocollo.

La corrispondenza indirizzata al singolo consigliere comunale, al Presidente del Consiglio comunale, alle Commissioni e/o Sottocommissioni consiliari, al Consigliere di fiducia dell'Ente, alla Commissione Pari Opportunità, alla Consulta Femminile, ai Revisori dei Conti, alle Commissioni Elettorali o ad altre persone o organi designati, non deve essere aperta ma recapitata direttamente.

### **5.8.5 Domicili eletti**

In relazione a quanto previsto nella Deliberazione G.C n. 31/1995, si considera e si protocolla come domicilio eletto, utilizzando l'apposito oggetto codificato, solo la corrispondenza e/o gli atti giudiziari che recano nella busta la dicitura "*Via Città di Padova*", "*Domicilio eletto*" o "*c/o Casa Comunale*".

Dev'essere invece restituita al mittente o non accolta la documentazione che rechi la dicitura: "*irreperibile*" o "*c/o Comune*", "*c/o Segreteria Generale*" poiché in questi casi le procedure notificatorie impongono di eseguire una notifica per irreperibilità assoluta.

### **5.8.6 Documenti inviati o presentati allo sportello che non siano afferenti ad alcun procedimento dell'Ente**

In relazione alla presentazione o all'invio di documenti, comunicazioni o dichiarazioni la cui acquisizione non sia richiesta nè prevista nell'ambito dei procedimenti amministrativi dell'Ente, effettuata una verifica con i Settori e gli uffici competenti, si procede alla loro restituzione (direttamente allo sportello o tramite canali postali) o, in caso di impossibilità, alla loro archiviazione in apposito fascicolo. Nel caso in cui questi documenti siano stati registrati a protocollo si dovrà procedere al loro annullamento ai sensi del precedente paragrafo 5.7.5. - *Annullamento delle registrazioni di protocollo.*

### **5.8.7 Integrazioni documentarie**

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, che spetta invece al Responsabile del procedimento amministrativo, ma è tenuto a registrare in ogni caso il documento ed eventuali allegati pervenuti successivamente.

I documenti pervenuti successivamente, ad integrazione di quelli già registrati, sono nuovamente registrati a protocollo indicando nell'oggetto "*integrazione a prot. n. – del --*" ove tale informazione sia desumibile.

### **5.8.8 Documenti pervenuti per errore al Comune di Padova**

I documenti pervenuti per errore al Comune di Padova non devono essere protocollati e devono essere spediti immediatamente al destinatario con la dicitura *“Erroneamente pervenuto al Comune di Padova il ...”*, ad eccezione dei casi previsti dalla normativa sull’accesso.

### **5.8.9 Trattamento dello stesso documento inviato o consegnato a diverse UOR dell’Ente o pervenuto attraverso canali diversi**

Qualora pervenga un documento tramite diversi canali (consegna a mano, invio postale, invio telematico) indirizzati a più UOR, l’addetto alla registrazione, prima di protocollarlo, deve verificare, attraverso il sistema informatico, che esso non sia già stato registrato dagli altri destinatari. Qualora il documento sia già stato registrato si deve riportare la stessa segnatura anche sugli altri esemplari. Nel caso pervenga un unico esemplare di un documento indicante più UOR destinatarie l’addetto alla registrazione provvede allo smistamento a tutte le UOR indicate. Sui documenti pervenuti successivamente si deve apporre la segnatura della registrazione già effettuata.

Nel caso in cui, nei documenti pervenuti telematicamente, siano indicati più indirizzi PEC dell’Ente si deve provvedere alla registrazione e successivo smistamento a tutti i Settori indicati. Per tale attività è necessario un coordinamento tra gli uffici interessati affinché siano evitate registrazioni doppie dei medesimi documenti.

Qualora la verifica sia impossibile perché il documento è stato presentato a sportelli decentrati e quindi protocollato con numeri diversi, il RPA cura la creazione dei collegamenti opportuni tramite il fascicolo informatico. Ai fini del calcolo dei tempi del procedimento amministrativo si tiene conto della data di quello protocollato per primo.

Nel caso di documento analogico pervenuto in un unico esemplare, ma di cui in fase di smistamento si individuano più UOR competenti, nel campo annotazione va riportata la dicitura *“originale cartaceo al settore.....”*.

### **5.8.10 Documenti con pluralità di oggetti**

Nel caso di un documento che tratti una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e, conseguentemente, a fascicoli diversi, l’addetto alla registrazione deve individuare la classifica prevalente e smistare il documento acquisito a sistema alle UOR competenti.

Ogni documento in uscita o interno deve obbligatoriamente trattare un solo oggetto (un solo argomento), deve necessariamente riferirsi ad un solo procedimento e quindi deve essere conservato in un unico fascicolo.

### 5.8.11 Documenti in partenza con più destinatari

Qualora i destinatari del documento siano molteplici nella registrazione di protocollo va riportato il nominativo del primo nel campo “corrispondente” e i nominativi degli ulteriori destinatari nel campo “altri corrispondenti”; se i destinatari sono molti nel campo “corrispondente” si indica: “... ed altri. Vedi elenco allegato alla registrazione”.

É possibile associare alla registrazione il file contenente l’elenco dei destinatari.

## 5.9 Modalità operative per la gestione dei documenti e dei relativi allegati

All’utenza esterna che presenta agli sportelli dell’ente documenti analogici deve essere rilasciata la ricevuta prodotta dal sistema di protocollo informatico. La ricevuta sostituisce l’apposizione della segnatura (timbro/etichetta) di protocollo sulla copie che restano all’utente.

La ricevuta riporta le seguenti informazioni minime:

- numero tipo e data di protocollo;
- mittente;
- indirizzo;
- oggetto;
- data documento;
- UOR competente;
- il nome dell’impiegato addetto alla registrazione.

La ricevuta è firmata elettronicamente dall’addetto alla registrazione.

L’apposizione della segnatura (timbro/etichetta) di protocollo sull’eventuale copia che resta all’utente è consentita solo in casi limitati ed eccezionali. In questo caso la segnatura va barrata e va aggiunta la dicitura “copia per l’utente”.

Si adottano le modalità operative di seguito illustrate:

- Tutti i documenti analogici in entrata o in uscita registrati devono essere acquisiti in copia per immagine e associati alla registrazione di protocollo. Fanno eccezione i documenti che materialmente non possono essere sottoposti a scansione (a titolo meramente esemplificativo: volumi, registri, plichi, planimetrie di formato superiore all’A3, plastici, monete, ecc.). In questi casi si deve segnalare l’assenza della scansione degli allegati, nel campo “Annotazioni” del registro di protocollo, con la dicitura “scansione parziale, segue documentazione cartacea completa”; nel caso in cui se ne ravvisi la necessità sono descritti i singoli allegati tramite le funzioni del sistema.

- Nel caso di documento analogico, l'originale è conservato dal Settore/UOR che ha effettuato la registrazione o dal destinatario finale del documento, fatta salva la trasmissione dell'originale ad altra struttura in base alle procedure in vigore o su espressa richiesta di quest'ultima.
- I documenti informatici sono acquisiti direttamente nel sistema di protocollo.
- La sottoscrizione del documento prodotto e allegato alla registrazione deve necessariamente avvenire prima della sua registrazione a protocollo.

## 5.10 Modalità operative per lo smistamento

L'operazione di smistamento consiste nell'assegnazione di un documento registrato alla UOR competente e al conseguente conferimento di responsabilità del relativo procedimento amministrativo. Ciascun utente registrato nel sistema è pertanto tenuto ad una attività di monitoraggio e controllo costante della/delle scrivanie di lavoro.

Si adottano le modalità operative di seguito illustrate:

- quotidianamente gli operatori e/o i responsabili devono aprire la scrivania di lavoro, attraverso la quale verificano i documenti pervenuti e ne monitorano i movimenti. Le scrivanie di lavoro sono uno strumento di gestione e di controllo dei documenti acquisiti, presi in carico o assegnati;
- il responsabile della UOR, verificati i documenti, li assegna al RPA competente sulla materia oggetto dei documenti;
- il RPA provvede alla visione e alla gestione del documento assegnato e mediante una delle seguenti azioni:
  - Assegnazione: assegnazione ad altro ufficio o ad utenti del proprio ufficio;
  - Rifiuto: restituzione del documento a UOR mittente per errata assegnazione;
  - Fascicolazione: inserimento del documento nel fascicolo informatico.
- E' prevista una forma di assegnazione per conoscenza per i soli documenti a carattere conoscitivo privi di adempimenti per le UOR (come le circolari di contenuto informativo).

Il sistema p@doc memorizza tutti i passaggi, conservando l'identificativo dell'utente che effettua l'operazione, il tipo di operazione effettuata, la data e l'ora di esecuzione.

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

La traccia risultante attesta le responsabilità, i tempi e le modalità di gestione del flusso documentale.

## 6. IL REGISTRO DI EMERGENZA

### 6.1. Situazioni che prevedono l'utilizzo del Registro di emergenza

L'utilizzo del Registro di emergenza è disciplinato dall'art. 63 del DPR 445/2000.

Nelle situazioni di emergenza nelle quali per cause tecniche non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato Registro di emergenza (*Allegato 8 - Modello del Registro di emergenza*).

Per emergenza si intende una situazione in cui la sospensione del servizio si protragga oltre le due 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, ecc...).

L'utilizzo del registro di emergenza, deve essere autorizzato dal Responsabile del Servizio archivistico; in caso di sua assenza o impedimento vi provvede il Capo Settore Servizi Istituzionali o un suo delegato.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana.

### 6.2. Modalità di utilizzo del Registro di emergenza

Per la registrazione di emergenza si utilizza:

- nel caso di disponibilità dei PC un modulo in formato excel disponibile tra la modulistica presente in intranet; il modulo 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 modulo allegato al Manuale di gestione che verrà compilato manualmente.

Sul registro di emergenza devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, la data e l'ora di ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti.

Prima di autorizzare l'avvio della procedura, il Responsabile del Servizio archivistico deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza.

Il Responsabile del Servizio archivistico dovrà annotare nel protocollo informatico unico i periodi di attivazione del Registro di emergenza.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, UOR, anno di registrazione, numero di protocollo nel formato stabilito; ad esempio:



La segnatura del protocollo di emergenza deve essere apposta mediante timbro o altro dispositivo e riportare le informazioni desunte dal relativo registro (es. RE01-2019-0000005).

Una volta ripristinata la piena funzionalità del sistema, il Responsabile del Servizio archivistico provvede alla chiusura dei registri di emergenza, annotando su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura.

In seguito l'operatore adibito alla protocollazione provvederà a inserire nel sistema informatico p@doc tutte le registrazioni già eseguite sul registro di emergenza. Ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo, seguendo la numerazione del protocollo informatico unico raggiunta al momento dell'interruzione del servizio senza soluzioni di continuità.

Di conseguenza i documenti prodotti in situazioni di emergenza e trasferiti nel protocollo informatico unico riceveranno due numeri: uno del protocollo di emergenza e uno del sistema di protocollo informatico p@doc. Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

## **7. DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO**

### **7.1 Descrizione funzionale ed operativa**

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico p@doc con particolare riferimento alle modalità di utilizzo nel contesto organizzativo dell'Ente.

La struttura modulare, che risponde ad esigenze di organizzazione e razionalizzazione delle componenti del sistema, è stata concepita per essere in grado di affrontare successive implementazioni, aggiornamenti o modifiche senza comprometterne l'impianto di base e le funzionalità già realizzate.

Il sistema consente di informatizzare l'attività amministrativa del Comune di Padova e possiede funzioni di amministrazione (per la gestione della struttura organizzativa e degli utenti) e funzioni operative (protocollazione e gestione dei flussi documentali).

Ai sensi della normativa vigente sono disponibili funzioni:

- per la produzione delle registrazioni di protocollo e relative ricerche, stampe, statistiche e reportistica anche ai fini del controllo di gestione;
- per la gestione della scrivania di lavoro e dell'ufficio;
- per la produzione dei fascicoli informatici, del relativo repertorio e delle connesse funzionalità di ricerca e visibilità;
- per la gestione dell'albo on-line e del registro delle pubblicazioni.

Il sistema è integrato con tutti i canali di trasmissione informatica dei documenti previsti dall'Ente (posta elettronica, posta elettronica certificata, fax server, istanze on-line), dai quali i documenti informatici vengono acquisiti a protocollo.

#### **7.1.1. Il sistema di protocollo generale all'interno del piano di formazione dell'Ente**

All'interno del piano di formazione dell'Ente è previsto un processo di condivisione delle procedure relative al sistema di protocollo e gestione documentale, condotto in presenza dal personale addetto su richiesta dei Settori (per esigenze formative straordinarie, ad esempio dovute a cambi organizzativi e/o di ruolo, o per un supporto alle attività ordinarie di gestione documentale).

E' inoltre disponibile nell'area Intranet - accessibile ai dipendenti - un corso on-line in modalità FAD (formazione a distanza) volto ad approfondire le principali funzionalità del sistema di gestione documentale adottato dall'Ente.

## 7.2 Rilascio delle abilitazioni di accesso

Il presente paragrafo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso ad utenti interni al sistema di protocollo informatico e gestione documentale p@doc.

L'accesso ad utenti esterni al sistema non è consentito.

Gli utenti di p@doc hanno autorizzazioni di accesso differenziate (ruoli) in base alle tipologie di attività da svolgere nell'ufficio di appartenenza, comunicate dal Responsabile della UOR. I ruoli all'interno del sistema sono definiti dal Responsabile del Servizio archivistico.

Ogni utente viene registrato all'interno di p@doc :

- con le medesime credenziali di accesso assegnate dal sistema informativo che utilizza per accedere a tutti i servizi personali quali pc, imol, posta elettronica:
  - *nome utente* pubblico che permette l'identificazione da parte del sistema
  - *password* privata o riservata di autenticazione
- con una autorizzazione di accesso (profilo), che limita 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.

I diversi livelli di autorizzazione sono assegnati agli utenti dal Responsabile del Servizio archivistico, che si avvale di un profilo di amministratore. Gli utenti del sistema, una volta identificati, sono suddivisi in profili d'accesso sulla base delle rispettive competenze. La profilazione degli utenti avviene mediante il modulo per la gestione dell'organigramma.

L'organigramma si compone di una serie di entità che possono essere combinate per rappresentare la struttura organizzativa del Comune di Padova.

Gli elementi costitutivi principali dell'organigramma sono :

- Amministrazione;
- Area Organizzativa;
- Unità Organizzativa;
- Carica (ACL);
- Persona;
- Gruppo Interno (raggruppamento di ACL).

Alcuni di questi elementi servono per definire la tipologia del quadro organizzativo (Amministrazione, AOO, UOR, persona), altri (come Cariche e Gruppo interno) definiscono nello specifico compiti e ruoli delle «Persone» che operano all'interno del programma.

La successione logica nella definizione dell'organigramma è la seguente:

- Amministrazione;
- Area organizzativa;
- Unità organizzativa;
- Gruppo Interno;

- Carica;
- Persona.

Da tale struttura logica discende il sistema di creazione delle entità nell'organigramma e di visibilità gerarchica che consente l'accesso ai documenti limitatamente a ciascuna UOR di appartenenza.

Le abilitazioni all'utilizzo delle funzionalità del sistema, ovvero l'identificazione delle unità organizzative e delle persone abilitate sono sottoposte a periodica verifica, modifica, gestione e aggiornamento da parte dell'amministratore del sistema.

### 7.2.1 Abilitazioni interne ad accedere al sistema

Per accedere è necessaria la registrazione effettuata dall'amministratore di sistema, previa richiesta da parte del responsabile della UOR.

L'utente registrato, mediante apposita icona sul sito intranet, si autentica a p@doc con le stesse credenziali assegnate dalla gestione centralizzata delle utenze tramite LDAP.

Tutte le utenze dell'AOO sono configurate con un time-out che provvede a disconnettere automaticamente l'applicazione dopo un periodo di inattività.

Le sessioni multiple con la stessa user ID sono impedita da p@doc.

### 7.2.2 Modalità di creazione e gestione delle utenze e dei relativi profili d'accesso

Come anticipato nel paragrafo 7.1. - *Descrizione funzionale ed operativa*, attraverso lo strumento di gestione dell'organigramma è possibile definire i ruoli e i livelli di autorizzazione per utenti o gruppi di utenti. Gli elementi dell'organigramma da impostare per una corretta profilazione degli utenti sono:

- **Gruppo Interno (raggruppamento di ACL):** Il gruppo interno permette di creare entità intese come insieme di permessi attribuiti alle persone inserite nel gruppo e di gestire i permessi di un consistente numero di persone.
- **Carica:** rappresenta il ruolo della persona all'interno dell'organizzazione ed è fondamentale per garantire un ottimo livello di astrazione e longevità al programma; tutte le registrazioni sono collegate alla carica e all'ufficio di appartenenza, garantendo così il presidio sulla visibilità dei documenti. Alla carica sono associati i permessi alle diverse funzioni del sistema.
- **Persona:** coincide con l'utente che accede al programma con le credenziali assegnate.

I principali gruppi interni del sistema p@doc sono:

GRUPPO	FUNZIONI
ALBO	utente che gestisce la pubblicazione all'albo pretorio on-line del proprio Settore (pubblicazione, defissione, ricerca)
CAPO SETTORE	utente con livello avanzato di abilitazioni, ha visibilità gerarchica su tutta la struttura di sua competenza
FATTURA ELETTRONICA	utente che riceve e protocolla la fattura elettronica
RESPONSABILE	utente con livello avanzato di abilitazioni, ha visibilità gerarchica sulla UO di sua competenza
SEGRETERIA	utente con livello medio di abilitazioni che gestisce la segreteria di Settore (protocollo entrata, uscita, interno, PEC entrata e uscita, mail entrata e uscita, fax entrata e uscita, protocollo riservato, modifica campi opzionali e campi obbligatori, cruscotto personale e di struttura, certificati INPS, fascicolazione, ricerca limitata ai documenti di settore)
UTENTI PROTOCOLLATORI	utente con livello base di abilitazioni (protocollo entrata, uscita, interno, modifica campi opzionali)
UTENTI PROTOCOLLO GENERALE	utente con visibilità completa su tutto il registro di protocollo, gestione pec in entrata e uscita, fattura elettronica, modifica dati obbligatori e opzionali, stampe registro di protocollo
VISUALIZZATORI	utente con livello minimo di abilitazioni, visibilità dei documenti assegnati alla propria UOR o a loro stessi, fascicolazione

Sono inoltre stati creati ulteriori gruppi interni utili alla gestione di particolari attività.

Al singolo utente possono essere aggiunte ulteriori abilitazioni necessarie allo svolgimento della propria attività che non sono comprese nella carica assegnata:

- protocollo riservato;
- mail , fax o pec istituzionale in entrata e/o uscita;
- pratiche assegnate (moduli on-line).

### 7.2.3 Abilitazione alle registrazioni di protocollo riservato

L'utente del sistema può gestire (registrare, visualizzare, assegnare) documenti riservati solo se autorizzato tramite apposita abilitazione.

In fase di registrazione gli utenti autorizzati sono chiamati a definire la tipologia di riservatezza, individuando le particolari categorie di dati sulla scorta del registro delle attività di trattamento. Il sistema consente la scelta tra:

- 0 - Non riservato
- 1 - Privacy - D.Lgs 196/2003
- 2 - Riservato – L. 241/1990

Tale scelta incide conseguentemente sulla possibilità di visibilità e di gestione di un documento da parte di un utente e consente la creazione del protocollo riservato, il cui accesso è autorizzato alle persone con appositi permessi.

L'utente non abilitato alla gestione dei protocolli riservati può registrare un documento che appartiene alle categorie sopracitate qualora questo sia preventivamente codificato.

Dopo la registrazione l'utente non autorizzato avrà visibilità sui seguenti dati: numero e data di protocollo, mittente/destinatario, UOR competente. I dati contenuti nei campi oggetto e classifica saranno sostituiti dal carattere asterisco e gli allegati non saranno visibili.

Tutte le registrazioni a carattere riservato formano il registro dei protocolli riservati.

## 8. GESTIONE E CONSERVAZIONE DEI DOCUMENTI

Il presente capitolo riporta il sistema di classificazione dei documenti e le modalità di formazione, consultazione e movimentazione dei fascicoli; descrive inoltre gli strumenti di gestione che consentono una corretta conservazione dei documenti con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto.

### 8.1 Sistema di classificazione

La classificazione dei documenti ha come obiettivo la corretta organizzazione dell'archivio e si avvale del Titolare o Piano di classificazione prodotto dal Gruppo di lavoro per gli Archivi dei comuni, adottato dal Comune di Padova e riportato all'*Allegato 09 – Piano di classificazione*.

Il Titolare può essere aggiornato su proposta del Servizio archivistico e le eventuali modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno seguente, previa informazione a tutti i soggetti abilitati all'operazione di classificazione dei documenti.

La classificazione viene effettuata su tutti i documenti ricevuti e prodotti dalle UOR del Comune di Padova ed è presupposto indispensabile per l'attività di fascicolazione.

Il Titolare di classificazione è collegato al Piano di conservazione prodotto dal Gruppo di lavoro per gli Archivi dei comuni di cui all'*Allegato 10 - Piano di conservazione*.

### 8.2 Attività di fascicolazione

Tutti i documenti registrati a protocollo e classificati nel sistema informatico sono inseriti in fascicoli. Tramite apposita funzione del sistema di protocollo sono descritti e inseriti nei fascicoli anche i documenti non protocollati.

Il sistema di protocollo informatico e gestione documentale genera e aggiorna automaticamente il repertorio dei fascicoli all'apertura di un nuovo fascicolo.

All'interno del fascicolo informatico i documenti sono inseriti in ordine cronologico e visualizzati a partire dal più recente.

Gli elementi identificativi del fascicolo sono:

- anno;
- indice di classificazione, (composto da titolo e classe);
- numero del fascicolo;
- oggetto del fascicolo;
- data di apertura del fascicolo;
- AOO e UOR;
- nominativo del responsabile.

Per esigenze pratiche all'interno del fascicolo possono essere creati i sottofascicoli, la cui numerazione è parimenti gestita dal sistema informatico.

Per l'organizzazione e gestione dei fascicoli si fa riferimento a diversi strumenti, quali le Linee guida per l'organizzazione dei fascicoli e delle serie prodotte dal Gruppo di lavoro per gli Archivi dei comuni (*Allegato 11 – Linee guida per l'organizzazione dei fascicoli e delle serie*) e il Censimento delle istanze e dei documenti, che definiscono i criteri e i metodi per costituire le aggregazioni documentarie. Dal punto di vista metodologico, per la creazione dei fascicoli, è opportuno far riferimento alle seguenti tipologie:

- *fascicoli per persona fisica/giuridica*: aggregazioni in cui l'elemento unificante è il soggetto del quale vengono raccolti i documenti, identificato mediante una chiave univoca quale: il numero di matricola, il codice fiscale, la partita IVA, il numero di registrazione, ecc.
- *fascicoli per affare/procedimento*: aggregazioni di documenti che fanno riferimento ad un determinato procedimento amministrativo
- *fascicoli per attività*: aggregazioni di documenti uguali per tipologia e riferite ad attività limitatamente complesse, raccolte in ordine cronologico o con altri criteri per un periodo di tempo determinato (fascicoli annuali, semestrali, trimestrali, ecc...).

Il fascicolo deve avere una chiusura che è effettuata dal Responsabile dello stesso al termine dell'attività (termine del rapporto dell'Ente con la persona fisica/giuridica nel primo caso; termine del procedimento amministrativo o esaurimento dell'affare nel secondo caso; termine del periodo di raccolta nel terzo caso).

La data di chiusura è la data dell'ultimo documento prodotto. Il fascicolo è ordinato dal sistema in base al repertorio.

### **8.2.1 Processo di assegnazione dei fascicoli**

Quando un nuovo documento viene acquisito dall'amministrazione, l'UOR abilitata all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo, 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, il soggetto preposto:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato.
- 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.

### **8.2.2 Repertorio dei fascicoli**

Lo strumento di gestione e organizzazione dei fascicoli è il Repertorio dei fascicoli, i cui elementi costitutivi sono:



- l'anno di apertura;
- l'indice di classificazione completo (titolo e classe);
- il numero di fascicolo o del sottofascicolo;
- la data di apertura;
- la data di chiusura;
- l'oggetto del fascicolo o del sottofascicolo;
- l'annotazione sullo stato del fascicolo, cioè se è aperto o chiuso;
- eventuali ulteriori annotazioni.

## **8.3 Documenti repertoriati**

Come previsto dall'art. 53 del DPR 445/2000, i documenti informatici prodotti o ricevuti dal Comune di Padova sono registrati nel sistema di protocollo generale dell'Ente o in uno dei repertori previsti dal Titolare di classificazione.

I registri o repertori informatici dell'Ente sono formati, gestiti e trasferiti in conservazione ai sensi delle norme attualmente vigenti, assicurando la corretta sedimentazione dei documenti e la predisposizione delle aggregazioni documentarie per la conservazione permanente.

Ciascuna tipologia di documento soggetto a registrazione particolare costituisce una serie archivistica; i documenti repertoriati possono altresì essere inseriti nel fascicolo archivistico di pertinenza.

L'elenco dei documenti esclusi dalla registrazione di protocollo generale e quello dei documenti soggetti a registrazione particolare sono riportati nei rispettivi allegati.

## **8.4 Gestione documenti cartacei degli archivi di deposito**

### **8.4.1 Gli archivi di deposito delle Unità organizzative**

Le UOR devono garantire, fino al versamento dei documenti cessati in Archivio generale, una gestione corretta della documentazione presente nei loro archivi di deposito, attraverso: la tenuta dei locali idonea alla conservazione materiale dei documenti; il condizionamento dei documenti e il mantenimento del loro ordinamento; la redazione di elenchi di consistenza aggiornati; la registrazione dei movimenti del materiale documentario eventualmente prelevato.

### **8.4.2 Il versamento dei fascicoli**

Il versamento dei fascicoli relativi ad affari e procedimenti amministrativi conclusi o comunque non più utili ad una trattazione corrente avviene su autorizzazione del Responsabile del Servizio archivistico comunale.

Prima di eseguire qualsiasi intervento sulla documentazione è obbligatorio contattare il personale archivistico dell'Archivio generale, il quale provvede ad effettuare un sopralluogo presso la sede dove sono conservati i fascicoli da versare.

In seguito, sulle indicazioni fornite dall'Archivio generale stesso, si procede alla redazione dell'elenco di versamento su supporto informatico utilizzando il modello adottato dal Comune di Padova (*Allegato 12 - Modello di Elenco di versamento*).

### **8.4.3 La movimentazione dei fascicoli**

Una volta che i fascicoli sono stati versati all'Archivio Generale, possono essere richiesti in consultazione e, se indispensabile prelevati su autorizzazione del personale archivistico; la consultazione e il prelievo avvengono solamente su richiesta scritta.

Il prelievo di fascicoli è annotato su un apposito registro informatico dal personale dell'Archivio generale che periodicamente può verificarne lo stato e richiedere la restituzione dei fascicoli affidati temporaneamente.

Il richiedente non può estrarre i documenti originali dal fascicolo, né alterarne l'ordine.

## **8.5 Conservazione dei documenti**

Il Comune di Padova conserva i documenti analogici presso gli archivi presenti nelle UOR e presso l'Archivio generale, mentre i documenti informatici sono affidati ad uno o più conservatori accreditati, pubblici o privati.

In entrambi i casi, i documenti sono conservati in modo permanente ovvero per un determinato periodo di anni, in base al Piano di conservazione.

Periodicamente il Servizio archivistico comunale predispone una proposta di scarto attraverso una determinazione del Responsabile del Servizio con l'elenco del materiale documentario da scartare, al fine di ottenere la necessaria autorizzazione della Soprintendenza archivistica competente.

Per quanto riguarda i documenti analogici, il personale archivistico redige gli elenchi di scarto in base alla selezione effettuata sui documenti conservati presso l'Archivio generale stesso e, in accordo con le UOR, sulla documentazione conservata presso le loro sedi.

Per i documenti informatici si fa riferimento al Manuale di conservazione.

## **8.6 Gestione dell'archivio storico**

L'Archivio generale adempie, per i documenti che costituiscono l'archivio storico del Comune di Padova, agli obblighi conservativi stabiliti per legge, garantendo la conservazione dei documenti in locali a norma e redigendo elenchi ed inventari delle serie e dei fondi attraverso schedature analitiche di diverso livello.

L'accesso per la consultazione dell'archivio storico del Comune di Padova è regolato dalle norme riportate all'*Allegato 13 - Norme generali per l'accesso alla Sala di studio*.

## 9. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

### 9.1 Regolamenti

Il Comune di Padova, recependo le prescrizioni e i principi espressi dalla normativa in materia, adotta e aggiorna appositi regolamenti in merito alle attività e ai procedimenti amministrativi. Inoltre, garantisce l'accesso il più ampio possibile ai documenti amministrativi e la tutela dei dati personali - soprattutto quelli particolari - riconoscendo in tal modo i diritti entrambi costituzionalmente fondati nel rispetto del principio del bilanciamento di interessi.

Nello specifico, sono adottati i seguenti regolamenti:

- *Regolamento sull'attività e i procedimenti amministrativi ;*
- *Regolamento sul diritto di accesso ai dati e ai documenti amministrativi;*
- *Regolamento per il trattamento dei dati personali.*

Al fine di assolvere agli obblighi di pubblicità legale ai sensi della Legge 18 giugno 2009, n. 69, il Comune di Padova ha attivato un sistema di gestione dell'Albo on-line integrato nel sistema di protocollo e gestione documentale p@doc e conforme ai requisiti previsti, e ha regolamentato le modalità, le forme e i limiti con i quali deve essere organizzato e gestito (*Regolamento per la disciplina dell'Albo pretorio informatico*).

### 9.2 Amministrazione trasparente

In adempimento alla recente normativa in tema di trasparenza e accesso civico (Decreto legislativo n. 33 del 14 marzo 2013 e successive modifiche - *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*), il Comune di Padova ha costituito apposita sezione di "Amministrazione trasparente" nel sito istituzionale, nella quale sono pubblicati dati, informazioni e documenti che riguardano l'organizzazione e le attività dell'amministrazione. Attraverso apposita sottosezione di Amministrazione trasparente è possibile consultare l'elenco dei procedimenti amministrativi del Comune di Padova mediante funzionalità di ricerca per unità organizzativa responsabile o per argomento.

Nelle forme previste dalla normativa pubblica, l'Amministrazione comunale pubblica ed aggiorna annualmente il Programma triennale per la trasparenza e l'integrità ed il relativo stato di attuazione, indicando i responsabili della trasmissione e della pubblicazione dei documenti, delle informazioni e dei dati.

## 9.3 Procedure di accesso ai documenti e di tutela della riservatezza

### 9.3.1 Accesso dei documenti per fini amministrativi

Tutta la documentazione prodotta dal Comune di Padova nell'esercizio della sua attività amministrativa, ivi compresa quella conservata nell'archivio storico, è accessibile per fini amministrativi nel rispetto della normativa vigente e dello specifico regolamento comunale.

### 9.3.2 Accesso dei documenti per fini di ricerca storico-scientifica

La consultazione è disciplinata dal Capo III del *Codice dei Beni Culturali e del Paesaggio*, in base al quale tutti i documenti del Comune di Padova sono liberamente consultabili, ad eccezione:

- di quelli di carattere riservato relativi alla politica estera o interna dello Stato, che divengono consultabili 50 anni dopo la chiusura del fascicolo che li contiene;
- di quelli contenenti dati particolari, che diventano consultabili 40 anni dopo la chiusura del fascicolo che li contiene;
- di quelli contenenti taluni dati particolari, idonei a rivelare lo stato di salute o la vita sessuale o i rapporti riservati di tipo familiare, che diventano consultabili 70 anni dopo la chiusura del fascicolo che li contiene.

La consultazione dei documenti contenenti categorie particolari di dati personali e dati personali relativi a condanne e reati può essere autorizzata dalla Soprintendenza archivistica competente per territorio anche prima della scadenza dei termini prescritti dalla legge.

## **10. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI**

### **10.1 Modalità di approvazione e aggiornamento del Manuale**

Il presente Manuale è approvato dalla Giunta comunale con propria deliberazione ed è aggiornato, su proposta del Responsabile del servizio archivistico o del gruppo di progetto incaricato della revisione, con le medesime modalità.

Gli aggiornamenti potranno rendersi necessari a seguito di:

- adeguamenti normativi che rendano superate le prassi definite nel Manuale;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Gli allegati al presente Manuale, che contengono indicazioni di dettaglio sulle procedure operative e sulle modalità di funzionamento dei sistemi gestionali, sono modificati con Determinazione dirigenziale o con provvedimento del Responsabile del Servizio archivistico, sentiti il Capo Settore Servizi Istituzionali e il Capo Settore Servizi Informatici.

Entra in vigore alla data di esecutività della deliberazione che lo approva. Con l'entrata in vigore del presente Manuale viene abrogato il Manuale di gestione già approvato con Deliberazione di Giunta Comunale n. 2015/0658 del 6 ottobre 2015.

### **10.2 Pubblicità del presente Manuale**

In ottemperanza a quanto disposto dal comma 3 dell'art. 5 delle *Regole tecniche per il protocollo informatico*, il Manuale di gestione è reso pubblico dal Comune di Padova mediante la pubblicazione sul proprio sito istituzionale.

Al fine di assicurarne adeguata conoscenza al personale dell'Ente il Manuale di gestione è pubblicato sulla rete Intranet del Comune di Padova e la sua conoscenza è inserita nei percorsi di formazione in tema di gestione documentale.

## ELENCO DEGLI ALLEGATI

NUMERO	NOME ALLEGATO	NOME FILE
1	Definizioni	Allegato 01 - Definizioni.pdf
2	Organigramma	Allegato 02 - Organigramma.pdf
3	Modello di segnalazione data breach PA	Allegato 03 - Modello segnalazione data breach PA.pdf
4	Metadati dei documenti soggetti a registrazione particolare	Allegato 04 - Metadati dei documenti soggetti a registrazione particolare.pdf
5	Ulteriori formati utilizzati	Allegato 05 - Ulteriori formati utilizzati.pdf
6	Documenti soggetti a registrazione particolare	Allegato 06 - Documenti soggetti a registrazione particolare.pdf
7	Documenti <sup>esclusi</sup> dalla registrazione di protocollo	Allegato 07 - Documenti esclusi dalla registrazione di protocollo.pdf
8	Modello di registro protocollo di emergenza	Allegato 08 - Modello di registro protocollo di emergenza.pdf
9	Piano di classificazione	Allegato 09 - Piano di classificazione.pdf
10	Piano di conservazione	Allegato 10 - Piano di conservazione.pdf
11	Linee guida per fascicoli e serie	Allegato 11 - Linee guida per fascicoli e serie.pdf
12	Elenco di versamento	Allegato 12 - Elenco di versamento.pdf
13	Norme generali per l'accesso alla sala studio	Allegato 13 - Norme generali per l'accesso alla sala di studio.pdf