



Città di Abano Terme

Manuale di Gestione e Conservazione

del protocollo informatico, dei flussi
documentali e degli archivi



Aggiornato alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti
informatici in vigore dal 01/01/2022.



Approvato con Deliberazione di G.C. n. 106 del 19/06/2025

INDICE GENERALE

1. PRINCIPI GENERALI

- 1.1 Premessa
- 1.2 Ambito d'applicazione
- 1.3 Normativa di riferimento e definizioni
- 1.4 Struttura organizzativa (Area Organizzativa Omogenea e Unità Organizzativa)
 - 1.4.1 Accreditamento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA)
- 1.5 Ruoli e responsabilità
 - 1.5.1 Responsabile della gestione documentale
 - 1.5.2 Responsabile della conservazione
 - 1.5.3 Responsabile della protezione dei dati

2. PROTEZIONE DEI DATI PERSONALI E PIANO DI SICUREZZA

- 2.1 Contesto
- 2.2 Le politiche di sicurezza adottate dall'Ente
 - 2.2.1 Aspetti di sicurezza relativi alla formazione dei documenti
 - 2.2.2 Aspetti di sicurezza relativi alla gestione dei documenti
 - 2.2.2.1 Componente organizzativa della sicurezza
 - 2.2.2.2 Componente fisica e infrastrutturale della sicurezza
 - 2.2.2.3 Postazioni di lavoro
 - 2.2.2.4 Componente logica della sicurezza
 - 2.2.3 Gestione delle registrazioni di protocollo e di sicurezza
 - 2.2.4 Criteri di utilizzo degli strumenti tecnologici
- 2.3 Aspetti di sicurezza connessi a trasmissione e interscambio dei documenti informatici
- 2.4 Aspetti di sicurezza relativi all'accesso ai documenti informatici
- 2.5 Aspetti di sicurezza connessi alla conservazione dei documenti

3. FORMAZIONE DEI DOCUMENTI

- 3.1 I documenti del Comune di Abano Terme
- 3.2 Elementi formativi essenziali dei documenti analogici
- 3.3 Formazione dei documenti informatici e dei documenti amministrativi informatici
 - 3.3.1 Metadati associati ai documenti informatici e ai documenti amministrativi informatici
 - 3.3.2 Sottoscrizione dei documenti informatici
 - 3.3.2.1 Tipologie di firme elettroniche
 - 3.3.2.1.1 La firma elettronica semplice
 - 3.3.2.1.2 La firma elettronica avanzata
 - 3.3.2.1.3 La firma elettronica qualificata
 - 3.3.2.1.4 Il Sigillo Elettronico Qualificato
 - 3.3.2.2 Sottoscrizione dei documenti informatici
 - 3.3.3 Tipologie di formato del documento informatico
 - 3.3.4 Copie, duplicati ed estratti
 - 3.3.4.1 Duplicati del documento informatico e analogico
 - 3.3.4.2 Copia del documento informatico e analogico
 - 3.3.4.3 Copia informatica del documento amministrativo analogico

- 3.3.4.4 Estratto informatico di un documento amministrativo informatico
- 3.3.4.5 Copia analogica di un documento amministrativo informatico

4. SCAMBIO DI DOCUMENTI

- 4.1 Documenti in entrata
- 4.2 Documenti in uscita
- 4.3 Documenti interni
 - 4.3.1 Documenti interni formali
 - 4.3.2 Documenti interni informali
- 4.4 Descrizione del flusso di lavorazione dei documenti
 - 4.4.1 Flusso in entrata
 - 4.4.1.1 Ricezione di documenti informatici nella casella di posta elettronica istituzionale del Comune
 - 4.4.1.2 Ricezione dei documenti informatici tramite PEC del Comune
 - 4.4.2 Flusso in uscita
 - 4.4.3 Flusso dei documenti interni formali

5. PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

- 5.1 Registrazione dei documenti
- 5.2 Registro di protocollo
- 5.3 Elementi della registrazione di protocollo
- 5.4 Modalità di registrazione di protocollo e di assegnazione
 - 5.4.1 La segnatura di protocollo
 - 5.4.2 Documenti soggetti a registrazione particolare, repertoriatura e documenti esclusi
 - 5.4.3 Modalità operative per la gestione dei documenti e dei relativi allegati
 - 5.4.4 Procedure specifiche nella registrazione a protocollo
 - 5.4.4.1 Protocolli riservati
 - 5.4.4.2 Documenti esclusi dalla registrazione a protocollo
 - 5.4.4.3 Protocollo differito
 - 5.4.4.4 Correzioni ortografiche e informazioni aggiunte alle registrazioni
 - 5.4.4.5 Annullamento delle registrazioni di protocollo
 - 5.4.5 Casi particolari di registrazioni di protocollo
 - 5.4.5.1 Lettere anonime
 - 5.4.5.2 Segnalazioni anonime
 - 5.4.5.3 Lettere prive di firma
 - 5.4.5.4 Corrispondenza da non aprire
 - 5.4.5.5 Domicili eletti
 - 5.4.5.6 Procedura per la gestione delle Pec e mail ordinarie contenenti link esterni per l'accesso agli allegati
 - 5.4.6 Documenti inviati o presentati allo sportello che non siano afferenti ad alcun procedimento dell'Ente
 - 5.4.7 Integrazioni documentarie
 - 5.4.8 Documenti pervenuti per errore al Comune
 - 5.4.9 Trattamento dello stesso documento inviato o consegnato a diverse UO dell'Ente o pervenuto attraverso canali diversi
 - 5.4.10 Documenti con pluralità di oggetti

- 5.4.11 Documenti informatici contenenti macroistruzioni
- 5.4.12 Modalità operative per lo smistamento

6. REGISTRO DI EMERGENZA

7. DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

- 7.1 Descrizione funzionale e operativa
- 7.2 Rilascio delle abilitazioni d'accesso

8. GESTIONE DEI DOCUMENTI

- 8.1 Archivio corrente
 - 8.1.1 Sistema di classificazione
 - 8.1.2 Fascicolazione
 - 8.1.3 Documenti repertoriati
- 8.2 Archivio di deposito
 - 8.2.1 Gli archivi di deposito delle UO
 - 8.2.2 Il versamento
 - 8.2.3 Movimentazione e prelievo dei fascicoli
 - 8.2.4 Selezione e scarto

9. CONSERVAZIONE DEI DOCUMENTI

- 9.1 Conservazione dei documenti analogici
- 9.2 Conservazione dei documenti digitali
 - 9.2.1 Ruoli e responsabilità
 - 9.2.2 Oggetti conservati
 - 9.2.3 Procedure di conservazione e di monitoraggio effettuate dal Comune

10. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

- 10.1 Regolamenti
- 10.2 Amministrazione trasparente e Albo online
- 10.3 Tutela della trasparenza e accesso ai documenti
 - 10.3.1 Accesso ai documenti amministrativi
 - 10.3.2 Accesso civico e accesso civico generalizzato
 - 10.3.3 Accesso ai documenti per fini di ricerca storico-scientifica

11. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

- 11.1 Modalità di approvazione e di aggiornamento del Manuale
- 11.2 Pubblicità del presente Manuale

12. ALLEGATI

- 1. Glossario
- 2. Organigramma del Comune
- 3. Documenti soggetti a registrazione particolare
- 4. Metadati dei documenti soggetti a registrazione particolare

5. Documenti esclusi dalla registrazione di protocollo
6. Formati
7. Modello di registro di protocollo di emergenza
8. Piano di classificazione
9. Prontuario per la classificazione
10. Piano di conservazione
11. Linee guida per fascicoli e serie
12. Modello di elenco di versamento
13. Registro di prelievo
14. Modello di elenco di scarto per SAB-VTA
15. Appendice normativa
16. Eccezioni al piano di classificazione
17. Il sistema documentale di protocollazione adottato dall'Ente
18. Servizio di conservazione a norma
19. Nomine ed incarichi
20. Metadati minimi del documento informatico
21. Metadati minimi dell'aggregazione documentale

1. PRINCIPI GENERALI

1.1. Premessa

Le *Linee guida sulla formazione, gestione e conservazione di documenti informatici*, pubblicate da dall'Agenzia per l'Italia digitale (AgID) prevedono per tutte le pubbliche amministrazioni l'adozione del Manuale di gestione che, secondo quanto disposto dal paragrafo 3.5 “descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi¹.

In tale ambito è previsto che ogni pubblica amministrazione individui una o più Aree Organizzative Omogenee, per le quali sia stato nominato un Responsabile della gestione documentale, così come già disposto dall'art. 50, comma 4, del Decreto del Presidente della Repubblica del 28 dicembre 2000 n. 445 - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*.

Lo scopo principale del Manuale di gestione (d'ora in avanti Manuale) è la descrizione del sistema documentale a partire dall'attività di protocollazione e delle ulteriori funzionalità disponibili. Inoltre, fornisce dettagliate istruzioni per una corretta esecuzione delle operazioni di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti nel Comune di Abano Terme.

1.2. Ambito di applicazione

Il presente documento, a cui devono fare riferimento non solo gli operatori di protocollo ma, in generale, tutti i dipendenti e i soggetti esterni che interagiscono con l'Amministrazione, ha lo scopo di raggiungere corrette e omogenee metodologie per:

- a) il trattamento dei documenti analogici e digitali;
- b) le procedure condivise per gestire i vari procedimenti amministrativi;
- c) l'accesso ad atti e informazioni;
- d) l'archiviazione e la conservazione della documentazione.

Più nel dettaglio, nel Manuale sono trattati:

- a) le politiche di protezione dei dati e il piano di sicurezza;
- b) le metodologie di formazione e scambio dei documenti;
- c) l'utilizzo del software di protocollo informatico e di gestione dei documenti;
- d) la gestione dei flussi documentali;
- e) l'utilizzo del piano di classificazione e la formazione e gestione delle aggregazioni

¹ Le Linee guida sono state pubblicate da AgID secondo la procedura di cui all'art. 71 del Decreto legislativo 7 marzo 2005, n. 82 e successive modifiche – Codice dell'amministrazione digitale (d'ora in poi CAD) con determinazione del 9 settembre 2020, n. 407. La determinazione AgID n. 371 del 17 maggio 2021 ha poi introdotto alcuni correttivi alle Linee guida e nello specifico agli allegati 5 e 6, estendendo poi i termini per l'applicazione al 1° gennaio 2022.

- documentali;
- f) le modalità di gestione dei documenti;
 - g) le modalità di conservazione dei documenti;
 - h) l'accesso ai documenti e alle informazioni e le annesse responsabilità;
 - i) la gestione dei procedimenti amministrativi.

1.3. Normativa di riferimento e definizioni

Il Manuale è redatto sulla base dei principi risiedenti nelle norme e negli standard nazionali e internazionali in materia di amministrazione digitale e gestione documentale, procedimenti e documenti amministrativi, tutela e conservazione degli archivi, sia analogici che digitali, e protezione dei dati personali.

Il dettaglio dell'apparato normativo di riferimento è contenuto nell'*Appendice normativa (Allegato 15)*, mentre le definizioni sono riportate nell'*Allegato 1 – Glossario*.

1.4. Struttura organizzativa (Area Organizzativa Omogenea e Unità Organizzative)

Per la gestione unitaria dei documenti il Comune di Abano Terme è costituito da un'unica Area Organizzativa Omogenea (d'ora in poi AOO), formalmente istituita con Deliberazione del Commissario straordinario n. 101 del 13 dicembre 2005.

All'interno dell'AOO il sistema di protocollo è unico e permette un'autonoma gestione documentale ad ogni Unità Organizzativa (d'ora in poi UO).

Le UO di cui si compone l'AOO sono presenti nell'*Organigramma del Comune (Allegato 2 – Organigramma del Comune di Abano Terme)*.

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le informazioni che individuano l'amministrazione stessa e le unità organizzative in cui è articolata.

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità tutti i dati.

1.4.1. Accredimento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA)

Nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;

- l'indirizzo della sede principale della amministrazione;
- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:
 - della denominazione;
 - del codice identificativo;
 - della casella di posta elettronica;
 - del nominativo del RSP;
 - della data di istituzione;
 - dell'eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'AOO.
- i dati relativi alla fatturazione elettronica
- i dati relativi al Responsabile della Transizione digitale

Per assicurare la comunicazione tra AOO le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

1.5. Ruoli e responsabilità

Con provvedimento dell'organo competente sono individuati i seguenti ruoli, prescritti dalla vigente normativa di riferimento:

- a) Responsabile della gestione documentale²;
- b) Responsabile della conservazione³;
- c) Responsabile della protezione dei dati⁴.

1.5.1. Responsabile della gestione documentale

Il Comune istituisce, nell'ambito del Settore Servizi amministrativi, l'ufficio denominato Servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi⁵, le cui funzioni fanno capo al Responsabile della gestione documentale.

Come riferito nel par. 3.4 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*, il Responsabile della gestione documentale “predisporre il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali e in coerenza con quanto previsto nel manuale di conservazione” ed è preposto al servizio di cui all'art. 61 del DPR 445/2000.

² Cfr. art. 61 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 – *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* (d'ora in poi DPR 445/2000) e art. 44, comma 1-bis, del CAD.

³ Cfr. par. 4.5 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*.

⁴ Cfr. art. 37 del Regolamento Europeo del 27 aprile 2016, n. 679 – *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* (d'ora in poi GDPR).

⁵ Si fa riferimento alla delibera del Commissario straordinario n. 102 del 13 dicembre 2005.

1.5.2. Responsabile della conservazione

Il Comune istituisce il Responsabile della conservazione⁶ il quale:

- a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11 delle *Linee guida*;
- j) assicura 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 a medesimo attribuite;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;
- m) predispone il manuale di conservazione di cui al par. 4.7 delle *Linee guida* e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Parte delle attività descritte sono affidate, nel Comune di Abano Terme, al Responsabile del servizio di conservazione.

⁶ Ai sensi del par. 4.5 delle *Linee guida*.

1.5.3. Responsabile della protezione dei dati

Il Responsabile della protezione dei dati personali svolge le seguenti attività⁷:

- a) fornire consulenze al titolare del trattamento, al responsabile del trattamento o ai dipendenti che si occupano del trattamento in merito agli obblighi derivanti dal presente Regolamento;
- b) se necessario, fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati e vigilarne lo svolgimento;
- c) collaborare coll'autorità di controllo.

2. Protezione dei dati personali e Piano di Sicurezza

Ai sensi delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*, con riferimento specifico al par. 3.9, il presente capitolo descrive le misure di sicurezza impiegate per la formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti.

2.1. Contesto

La normativa di riferimento è il Regolamento UE 2016/679 – GDPR che, in ambito italiano, ha portato all'armonizzazione del Decreto legislativo 30 giugno 2003, n. 196 – *Codice in materia di protezione dei dati personali* attraverso il Decreto legislativo 10 agosto 2018, n.101 – *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679* favorendo un nuovo approccio in tema di sicurezza e privacy con l'impiego del termine *accountability*, ovvero sia la responsabilizzazione del titolare di un trattamento dati.

In questo modo, tale figura non è più un mero esecutore di un elenco di misure imposte da una norma, ma il responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque idonee a salvaguardare i dati che tratta.

Nella cornice appena descritta, il Comune di Abano Terme ha provveduto, in data 7 dicembre 2000, alla pubblicazione di un Documento Programmatico per la Sicurezza, il quale ha fornito una serie di informazioni relativamente a:

- a) elenco dei trattamenti di dati personali;
- b) individuazione delle tipologie di dati personali trattati;
- c) descrizione delle aree, dei locali e degli strumenti con cui vengono effettuati tali trattamenti;
- d) distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- e) analisi dei rischi;
- f) misure da adottare per garantire l'integrità e disponibilità dei dati e la protezione delle aree e dei locali;
- g) descrizione dei criteri e delle modalità per il ripristino della disponibilità di dati ed informazioni in seguito a distruzione e danneggiamento;
- h) interventi formativi degli incaricati del trattamento;
- i) descrizione delle strategie da adottare in caso di trattamenti di dati personali affidati

⁷ Così come previsto dagli artt. 37-39 del GDPR.

all'esterno.

A partire dal 2018⁸, il Comune ha assegnato ad una ditta esterna l'incarico di Responsabile della protezione dei dati (DPO), nonché gli incarichi di:

- a) stesura e aggiornamento del Registro delle attività di trattamento;
- b) stesura e aggiornamento delle misure minime di sicurezza ICT;
- c) manutenzione della piattaforma SaaS Privacy X-GDPR;
- d) assistenza per la stesura di una valutazione annuale d'impatto sulla protezione dei dati⁹;
- e) formazione in ambito privacy tramite una serie di videolezioni;
- f) fornitura di modelli organizzativi per la privacy;
- g) assistenza e manutenzione da remoto;
- h) mantenimento del ruolo di *Data Protection Officer* (DPO);
- i) attività di *audit* in ambito privacy, con lo scopo di verificare:
 - il grado di conformità alla normativa vigente;
 - il grado di conformità alle *privacy policy* aziendale che tutti i dipendenti sono tenuti ad osservare;
 - l'efficacia di azioni correttive a seguito di non conformità.

Per quanto concerne nello specifico i punti a) e d) del precedente elenco, è stata prevista la predisposizione di un Registro delle attività di trattamento¹⁰ contenente:

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, comma 2, del GDPR, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

⁸ A seguito dell'emanazione della circolare dell'Agenzia per l'Italia Digitale del 18 aprile 2017, n.2 – *Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante misure minime di sicurezza ICT per le pubbliche amministrazioni*, in base alla quale entro il 31 dicembre 2017 le amministrazioni avrebbero dovuto adottare le misure minime per la sicurezza ICT al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.

⁹ La *Valutazione d'impatto sulla protezione dei dati*, così come prevista dall'art. 35 del GDPR, deve comprendere i seguenti elementi:

- a) una sistematica descrizione dei trattamenti e delle corrispondenti finalità oltre che, ove possibile, il legittimo interesse del titolare;
- b) considerate le finalità del trattamento, una valutazione della proporzionalità e delle necessità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati;
- d) considerati i diritti e i legittimi interessi degli interessati, le misure previste per affrontare i rischi includendo le necessarie garanzie di *data protection* e *compliance* previste dal GDPR.

¹⁰ Cfr. art. 30 del GDPR.

2.2. Le politiche di sicurezza adottate dall'Ente

Il Piano della Sicurezza del sistema di gestione informatica dei documenti¹¹, di seguito descritto, ha lo scopo di:

- a) garantire che informazioni e documenti trattati dal Comune siano resi disponibili, autentici e integri;
- b) assicurare che i dati personali, le tipologie di dati personali particolari¹² e i dati giudiziari relativi a reati e condanne penali¹³ siano preservati in modo tale da ridurre al minimo i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito.

Definito sulla base dello studio delle tipologie dei documenti trattati e delle direttive strategiche stabilite dai vertici dell'Amministrazione, il Piano di Sicurezza si articola nei seguenti punti, regolando:

- a) le politiche di sicurezza da adottare all'interno del Comune di Abano Terme;
- b) le norme d'accesso al sistema di protocollo informatico e di gestione documentale;
- c) le misure di sicurezza adottate dal punto di vista organizzativo, procedurale e tecnico;
- d) l'insieme delle procedure che disciplinano il monitoraggio periodico delle misure di sicurezza adottate.

In tal senso, nel 2018 il Comune ha implementato i propri sistemi server, adottando un'infrastruttura virtuale e un software impiegato giornalmente nell'attività di backup incrementale, garantendo così la generazione di una copia dei dati su un apposito server fisico.

Inoltre, è stato creato un nuovo server fisico avente la capacità di replicare l'intero sistema informaticocomunale in caso di indisponibilità dei server principali. Lo scopo è di allestire un'unità di crisi immediatamente utilizzabile in casi di emergenza. Attualmente tale sistema è ubicato in Municipio. Inoltre, col fine di assicurare la sicurezza del sistema tecnologico, la riservatezza delle informazioni custodite nelle banche dati e l'identificazione univoca degli utenti, sono state adottate le seguenti procedure tecniche ed organizzative:

- a) protezione periferica dell'Intranet dell'Amministrazione;
- b) assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti di un ID, di una password e di un profilo di autorizzazione;
- c) predisposizione di un piano di continuità del servizio che prevede:
 - l'esecuzione e la gestione delle copie di riserva di informazioni e documenti con modalità sincrona e a cadenza giornaliera;
 - la possibilità di ripristinare il sistema informativo entro sette giorni in caso di disastro o emergenza;
- d) gestione dei casi di emergenza informatica attraverso risorse qualificate;
- e) utilizzo e manutenzione di un adeguato sistema antivirus;

¹¹ Secondo quanto disposto dall'art. 51 del CAD e par. 3.4 delle *Linee guida*.

¹² Cfr. art. 9 del GDPR.

¹³ Cfr. art. 10 del GDPR.

- f) impiego di soluzioni grazie alle quali sono rese inintelligibili, a chi non ha diritto d'accesso, le particolari tipologie di dati personali presenti in elenchi, registri o banche dati;
- g) archiviazione giornaliera, in modo permanente e non modificabile, delle copie del registro di protocollo, dei file di log con le informazioni sulle operazioni compiute da ciascun utente nell'arco di una giornata lavorativa, compresi i processi di backup e di manutenzione del sistema;
- h) protezione e controllo dei sistemi di accesso alle informazioni;
- i) la conservazione, da parte del Servizio informatico comunale, 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.

Nei capitoli successivi saranno illustrati più dettagliatamente gli aspetti di sicurezza relativamente a:

- a) formazione dei documenti;
- b) gestione dei documenti informatici;
- c) gestione delle registrazioni di protocollo e di sicurezza;
- d) criteri di utilizzo degli strumenti tecnologici.

2.2.1. Aspetti di sicurezza relativi alla formazione dei documenti

Come già sottolineato al par. 2.1.1 delle *Linee guida* le caratteristiche di immutabilità e di integrità dei documenti prodotti dall'Ente sono garantite da una o più delle seguenti procedure, dipendenti dalla modalità stessa di formazione dei documenti informatici:

- a) Apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- b) trasferimento del documento a soggetti terzi attraverso l'impiego della PEC o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS;
- c) memorizzazione del documento all'interno del sistema di protocollo informatico e di gestione documentale che adottino idonee misure di sicurezza;
- d) registrazione dei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure di protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- e) riversamento del documento all'interno di un sistema di conservazione.

2.2.2. Aspetti di sicurezza relativi alla gestione dei documenti

I documenti del Comune di Abano Terme sono gestiti:

- a) analogicamente: attraverso la formazione di fascicoli, all'interno dei quali devono confluire in modo omogeneo e secondo regole condivise i documenti relativi ad una persona fisica o giuridica, ad un affare o ad un procedimento. I suddetti fascicoli, contenenti documenti disposti cronologicamente secondo l'ordine di sedimentazione, dovranno a loro volta essere

inseriti all'interno di faldoni recanti le informazioni necessarie al loro rapido reperimento¹⁴.
Le buste dovranno essere:

- formate dai responsabili del procedimento;
- conservate in locali idonei e accessibili al solo personale addetto alla consultazione all'interno degli uffici di competenza o comunque presso una delle sedi comunali;
- descritte in un elenco di censimento avente lo scopo di tenere traccia della produzione documentaria corrente e di favorirne un rapido reperimento.

Terminato il periodo di utilità corrente per l'ufficio, i fascicoli non dovranno più giacere inutilizzati presso una delle sedi comunali, bensì essere versati nella nuova sede d'Archivio in attesa di essere scartati o ulteriormente riordinati per la conservazione permanente.

- b) digitalmente: attraverso il sistema di protocollo informatico e di gestione documentale attualmente in uso.

2.2.2.1. Componente organizzativa della sicurezza

La componente organizzativa della sicurezza, legata alla gestione del protocollo e della documentazione, si riferisce principalmente alle attività svolte attraverso l'attuale software di protocollo informatico.

In tale contesto, la gestione della sicurezza informatica dei dati si concretizza attraverso interventi tecnici e organizzativi atti a prevenire o ridurre gli effetti di una minaccia e con controlli e verifiche per assicurare la stabilità nel tempo del sistema informatico. Il settore che, all'interno del Comune, è incaricato di salvaguardare i dati del sistema informatico è il Centro di Elaborazione Dati (CED). Una ditta esterna, invece, è incaricata alla sicurezza in termini di accesso e backup, all'aggiornamento, alla manutenzione e allo sviluppo dell'applicativo in versione Cloud.

Nella tabella seguente sono elencati i settori responsabili dei controlli in relazione alle varie tipologie di misure di sicurezza da adottare in casi di rischi o minacce:

Misure di sicurezza	Settore responsabile dei controlli
Sicurezza fisica e infrastrutturale	Ufficio tecnico
Sicurezza logica	CED
Sicurezza organizzativa	Segreteria Generale

2.2.2.2 Componente fisica e infrastrutturale della sicurezza

Per componente fisica e infrastrutturale della sicurezza s'intende la sicurezza fisica degli accessi ai luoghi in cui risiedono le risorse del sistema informativo. Essa è garantita attraverso l'impiego di:

- a) impianti elettrici dedicati;
- b) sistemi di condizionamento per il raffreddamento delle apparecchiature;

¹⁴ Per i dettagli relativi alle informazioni da riportare sulle coperte dei fascicoli e sui dorsi delle buste si rimanda alla lettura del capitolo 8 – *La gestione dei documenti*.

- c) gruppo di continuità elettrica;
- d) controllo periodico su efficienza del gruppo elettrogeno;
- e) estintori;
- f) piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori;
- g) accesso ai locali mediante sistema d'autenticazione tramite badge e chiave.

Nell'allegato A - *Misure di sicurezza tecniche ed organizzative* del citato Registro delle attività di trattamento sono forniti in forma tabellare i dati dettagliati relativamente a quanto sopra elencato.

2.2.2.3 Postazioni di lavoro

La gestione e manutenzione delle postazioni di lavoro dei dipendenti per l'utilizzo del sistema di protocollo informatico rientra nell'ambito di competenze del CED. Infatti, il Comune, attraverso i propri informatici, dev'essere in grado di verificare il corretto funzionamento delle postazioni di lavoro e di allestire le necessarie infrastrutture *hardware* e *software* per favorirne la necessaria sicurezza informatica.

I requisiti che tutte le postazioni di lavoro devono soddisfare comprendono:

- a) l'aggiornamento del sistema operativo;
- b) la dotazione di un programma antivirus con funzionalità automatica di aggiornamento periodico;
- c) la protezione dell'accesso al sistema operativo delle postazioni di lavoro attraverso l'immissione di una *password* di adeguata complessità, cambiata con cadenza regolare;
- d) la connessione solo all'interno della rete del Comune.

Sulle postazioni di lavoro non è permesso:

- a) utilizzare modem o dispositivi mobili per l'accesso da o verso l'esterno della rete del Comune, fatte salve espresse autorizzazioni;
- b) installare programmi non attinenti all'attività lavorativa e/o privi di licenze d'uso;
- c) copiare dati di titolarità dell'Amministrazione comunale su dispositivi esterni personali.

2.2.2.4 Componente logica della sicurezza

Lo scopo principale di tale componente è di garantire i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. È assicurata dall'impiego di:

- a) identificazione e autenticazione degli utenti;
- b) profilazione degli accessi (ACL);
- c) politica antivirus;
- d) firma digitale;
- e) monitoraggio delle sessioni di lavoro.

Nell'allegato A del Registro delle attività di trattamento¹⁵ sono riportate più dettagliatamente le strategie attualmente predisposte dall'Ente per il mantenimento di tale aspetto della sicurezza informatica.

2.2.3. Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono formate da dati o transazioni presenti o transitate sul software di protocollo o su sistemi di supporto indipendenti, che è essenziale conservare sia in caso di controversie legali, sia per esaminare le matrici da cui possono discendere incidenti di sicurezza.

Le registrazioni di sicurezza possono essere rappresentate da:

- a) log di sistema generati dal sistema operativo;
- b) log dei dispositivi di protezione periferica del sistema informatico;
- c) registrazioni del software di protocollo informatico attualmente in uso.

Inoltre, per tali registrazioni essendo il software in versione Cloud e ospitato in hostig qualificato e approvato da AGID e ANC, si elencano di seguito le caratteristiche di sicurezza offerte:

- a) CSP (cloud service provider) dal 12/12/2018
- b) SaaS (software as a service) dal 25/01/2019
- c) Certificazione Iso27001 sulla sicurezza informatica, Iso27017, Iso27018
- d) Certificazione sul sistema CLOUD : iso 20000
- e) Certificazione sul sistema di qualità : iso 9001
- f) Certificazione sulla gestione ambientale : iso 14001

¹⁵ Registro delle attività di trattamento, allegato A – Misure di sicurezza tecniche ed organizzative

2.2.4. Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni del Comune l'accesso ai diversi servizi attraverso l'adozione di una serie di misure organizzative e tecnologiche. Le principali regole che ogni utente deve rispettare in tal senso sono le seguenti:

- a) è responsabile, civilmente e penalmente, del corretto utilizzo dei dispositivi informatici, dei servizi e dei programmi e canali a cui ha accesso, nonché dei dati trattati ai fini istituzionali;
- b) è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute ai fini istituzionali, anche in riferimento alla riservatezza dei dati ivi contenuti;
- c) deve garantire il buon funzionamento degli strumenti, anche col fine di ridurre i rischi legati alla sicurezza del sistema informatico. Dunque, non è possibile utilizzare supporti per la memorizzazione dei dati non sicuri o provenienti dall'esterno;
- d) è responsabile della tutela dei dati e dei documenti archiviati, per garantire i quali dovrà effettuare regolarmente salvataggi su supporti idonei e conservare gli stessi in luoghi adatti;
- e) è responsabile in modo esclusivo della password affidata, che quindi non è cedibile né tantomeno divulgabile;
- f) è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
- g) è tenuto a trattare i dati sensibili riprodotti su supporti magnetici con particolare cautela. Per quanto concerne tale tipologia di dati e quelli di natura giudiziaria, si rinvia al *Regolamento per il trattamento di dati sensibili e giudiziari* del Comune.

2.3. Aspetti di sicurezza connessi a trasmissione e interscambio dei documenti informatici

Il Comune di Abano Terme utilizza le tecnologie della trasmissione con i seguenti livelli di sicurezza:

Tipologia di trasmissione	Caratteristiche	Livello di sicurezza
PEC	Sicurezza dell'accettazione e consegna del messaggio attraverso l'utilizzo delle ricevute	Medio-basso
Canali web – Istanze online	Utilizzo del protocollo HTTPS che garantisce la piena riservatezza	Medio
Posta elettronica ordinaria	Transito del messaggio attraverso un protocollo SMTPS che non garantisce la riservatezza della trasmissione	Basso
Fax server	Meccanismo di trasmissione che utilizza la posta elettronica ordinaria	Medio

2.4. Aspetti di sicurezza relativi all'accesso ai documenti informatici

I dettagli relativi alla sicurezza degli accessi al sistema di protocollo informatico da parte degli utenti interni al Comune sono descritti nel capitolo 7 – *Descrizione del sistema di protocollo informatico*.

Il capitolo 10 – *Procedimenti amministrativi, accesso ai documenti e tutela della riservatezza*, invece, tratta il tema del diritto d'accesso ai documenti.

2.5. Aspetti di sicurezza connessi alla conservazione dei documenti

Per gli aspetti di sicurezza relativi alla conservazione dei documenti informatici si rimanda alla lettura del paragrafo 9.2.3 – *Procedure di conservazione e di monitoraggio effettuate dal Comune*.

3. FORMAZIONE DEI DOCUMENTI

3.1. I documenti del Comune di Abano Terme

I documenti sono formati dai rispettivi organi e uffici durante lo svolgimento della loro attività amministrativa e, sedimentandosi progressivamente, costituiscono l'Archivio comunale.

Le modalità di formazione dei documenti sono determinate dai dirigenti e dai responsabili delle UO e da quanto riportato nel presente Manuale.

L'Ente forma gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici¹⁶ riservandosi di formare documenti originali analogici nelle situazioni di necessità e secondo gli elementi descritti nel capitolo seguente.

3.2. Elementi formativi essenziali dei documenti analogici

Nell'attività amministrativa, il documento analogico è formato su un supporto analogico e con strumenti analogici (es.: documento scritto a mano) o informatici (es.: documento prodotto a PC) e successivamente stampato su carta. L'originale analogico è il documento nella sua redazione definitiva, perfetta e autentica negli elementi formali (carta intestata, formulario amministrativo) e sostanziali, comprende tutti gli elementi di garanzia e di informazione, del mittente, del destinatario ed è dotato di firma autografa.

Qui di seguito vengono elencati gli elementi obbligatori da riportare o associare a tale tipologia di documenti:

Autore:

- a) stemma e dicitura del Comune di Abano Terme;
- b) Unità Organizzativa Responsabile;
- c) dati fiscali (codice fiscale e partita IVA);
- d) dati di contatto, ovverosia:
 - indirizzo e recapito telefonico;
 - PEC istituzionale del Comune;
 - indirizzo PEC dell'UOR, ufficio o servizio responsabile del procedimento.

Estremi di registrazione:

- a) numero e data di registrazione di protocollo/repertorio;
- b) classificazione;
- c) eventuale numero e data del documento cui si risponde.

Destinatario (nel caso in cui dovesse esserci). A seconda dei casi, almeno una delle seguenti opzioni:

- a) domicilio digitale, ovverosia PEC;
- b) indirizzo per il recapito postale completo (via/piazza, numero civico, CAP, città);
- c) altro indirizzo di posta elettronica precedentemente dichiarato.

¹⁶ In conformità a quanto disposto dall'art. 40 del CAD.

Oggetto: descrizione sintetica ma esaustiva della funzione/materia del documento.

Responsabile del Procedimento (RPA): cognome e nome del Responsabile del procedimento amministrativo.

Sottoscrizione. A seconda dei casi:

- a) firma digitale;
- b) altri tipi di firma.

Inoltre, si ricorda che ai sensi del DPCM 21 marzo 2013¹⁷, per particolari tipologie di documenti analogici originali unici sussiste l'obbligo di conservazione dell'analogico originale, oppure, in casi di conservazione sostitutiva, la conformità all'originale dev'essere autenticata da un pubblico ufficiale a ciò autorizzato.

Pertanto, tutti i documenti su cui vengono apposti manualmente i dati di registrazione a protocollo, le sigle e la firma autografa sono da considerarsi documenti amministrativi analogici.

3.3. Formazione dei documenti informatici e dei documenti amministrativi informatici

Il documento informatico è il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti¹⁸.

I documenti amministrativi informatici sono gli atti formati dalle pubbliche amministrazioni con l'ausilio di strumenti informatici, nonché i dati e documenti informatici dalle stesse detenuti, e costituiscono informazione primaria e originale da cui è possibile effettuare, su diversi o medesimi tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge¹⁹.

Secondo quanto disposto dal par. 2.1.1 delle *Linee guida*, i documenti informatici possono essere formati secondo una delle seguenti modalità:

- a) Creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle *Linee guida*;
- b) acquisizione 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. Rientrano in questa categoria i messaggi di posta elettronica e posta elettronica certificata (PEC), il servizio elettronico di recapito certificato e le immagini ottenute con processi di digitalizzazione degli originali analogici;

¹⁷ Decreto del Presidente del Consiglio dei Ministri del 21 marzo 2013 - *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente e allegata al documento informatico*, ai sensi dell'art. 22, comma 5, del CAD.

¹⁸ CAD, art. 1, comma 1 lett. p).

¹⁹ CAD, art. 23-ter, comma 1, e par 2.4 delle *Linee guida*.

- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi eseguiti su computer, oppure dalla presentazione telematica di dati attraverso moduli o formulari online resi disponibili all'utente;
- d) 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.

Il documento informatico assume la caratteristica di immodificabilità se formato in modo tale che forma e contenuto non siano alterabili durante le fasi di gestione e accesso e ne sia garantita la staticità nella fase di conservazione.

Inoltre, lo stesso, identificato univocamente e in modo persistente, è memorizzato all'interno di un sistema di gestione informatica dei documenti o di conservazione, la cui tenuta può anche essere delegata a terzi.

Il mantenimento nel tempo delle caratteristiche di sicurezza, integrità e immodificabilità dei documenti informatici, così come disposto dall'art. 20, comma 1-bis, del CAD, è determinato da una o più delle seguenti operazioni:

- a) sottoscrizione con firma digitale, ovvero con firma elettronica qualificata;
- b) apposizione di una validazione temporale;
- c) trasferimento a soggetti terzi con PEC con ricevuta completa;
- d) memorizzazione su sistemi di protocollo e di gestione documentale con idonee politiche di sicurezza;
- e) versamento in un sistema di conservazione.

I documenti formati dagli uffici possiedono le caratteristiche elencate e, con lo scopo di semplificare la gestione dei procedimenti amministrativi, il Comune di Abano Terme ha inserito all'interno del proprio sito istituzionale un'apposita sezione denominata *Servizi online*, all'interno della quale i cittadini e le imprese possono adempiere ad una serie di procedure in modalità unicamente telematica. Infine, nelle sezioni del sito relative alle varie Unità Organizzative comunali sono resi disponibili moduli da compilare e inviare unicamente in modalità telematica.

3.3.1 Metadati associati ai documenti informatici e ai documenti amministrativi informatici

I metadati sono definibili come l'insieme dei dati associati a un documento informatico, ad un fascicolo o ad un'aggregazione documentale informatici, con lo scopo di identificarlo e di descriverne il contesto, il contenuto e la struttura e di assicurarne la gestione nel tempo all'interno del sistema di conservazione.

L'insieme minimo di metadati da associare al documento informatico immodificabile e anche ai documenti soggetti a registrazione particolare è costituito da:

- a) identificativo univoco e persistente;
- b) riferimento temporale rappresentato dall'informazione contenente la data e l'ora sincronizzata con il tempo coordinato universale (UTC);
- c) oggetto;
- d) soggetto che ha provveduto alla formazione del documento;

- e) eventuale destinatario;
- f) impronta del documento informatico²⁰;
- g) ulteriori ed eventuali metadati aggiuntivi stabiliti dal Comune a fini gestionali e conservativi.

Nel caso di documenti amministrativi informatici, invece, l'insieme minimo dei metadati inseriti nell'allegato 5 delle *Linee guida* comprende:

- a) codice identificativo dell'amministrazione;
- b) codice identificativo dell'area organizzativa omogenea;
- c) codice identificativo del registro nel quale sono annotati i documenti;
- d) data di protocollo generata automaticamente dal software di protocollo;
- e) numero progressivo di protocollo generato automaticamente dal software di protocollo;
- f) oggetto del documento²¹;
- g) dati identificativi del mittente per i documenti ricevuti o del destinatario/i per i documenti spediti;
- h) data e numero di protocollo del documento ricevuto, qualora disponibili;
- i) impronta del documento informatico, qualora trasmesso telematicamente;
- j) indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- k) indice di classificazione;
- l) identificazione degli allegati (numero e descrizione);
- m) informazioni sul procedimento a cui afferisce e sul trattamento da applicare al documento.

Ulteriori metadati, per ogni tipologia di documento, sono definiti dall'Amministrazione.

3.3.2 Tipologie di Firme e Sottoscrizione dei documenti informatici

3.3.2.1 Tipologie di firme elettroniche

La normativa vigente in materia, individua e disciplina cinque diverse tipologie di sottoscrizione elettronica (persone fisiche) attraverso le seguenti definizioni:

- a) firma elettronica – dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
- b) firma elettronica avanzata – insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da

²⁰ L'impronta del documento informatico è una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta con il contenuto originale.

²¹ Per la redazione dell'oggetto del documento e la descrizione di mittente e destinatario, è possibile adottare le raccomandazioni elaborate dal progetto Amministrazioni unite per la redazione degli oggetti e delle registrazioni anagrafiche nel protocollo informatico (Aurora) elaborate da un gruppo di lavoro coordinato dall'Archivio Generale dell'Università degli Studi di Padova. Le informazioni sopra riportate sono consultabili al seguente link: <http://www.unipd.it/archivio/progetti/aurora>, febbraio 2018.

consentire di rilevare se i dati stessi siano stati successivamente modificati

c) firma elettronica qualificata – una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche

d) firma digitale – un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

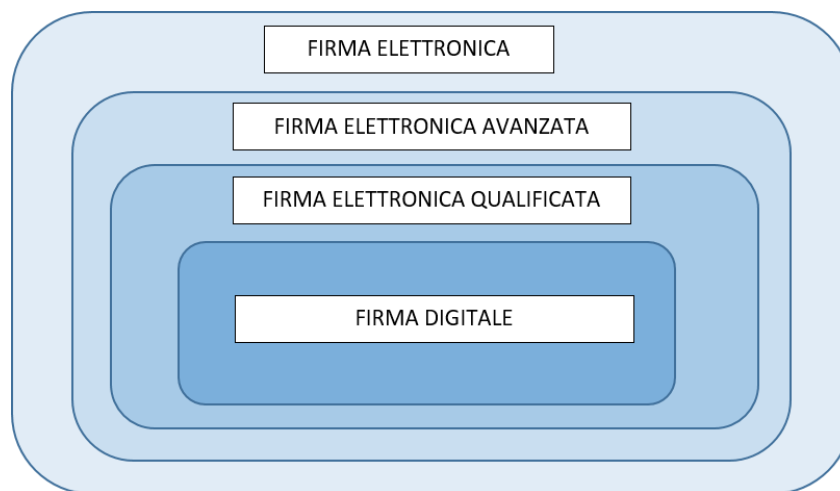


Figura 1 Le diverse firme elettroniche.

Come si evince dalla Figura 1, la firma digitale è del genere “firma elettronica qualificata.” Ai fini del presente documento, le locuzioni “firma elettronica qualificata” (o FEQ) e “firma digitale” sono pertanto utilizzati come sinonimi.

I documenti informatici sottoscritti elettronicamente possono essere distinti in tre categorie:

- documenti sottoscritti con firma elettronica (“semplice”),
- documenti sottoscritti con firma elettronica avanzata,
- documenti sottoscritti con firma elettronica qualificata (o firma digitale).

3.3.2.1.1 La firma elettronica semplice

La firma elettronica cosiddetta semplice può essere costituita da molteplici elementi che consentono di ricondurre degli atti o fatti giuridicamente rilevanti a una persona fisica. Un esempio è l’invio di un messaggio di posta elettronica che, in alcune circostanze, è stato considerato costituire prova in tribunale. Altro esempio di firma elettronica è la firma a stampa (il nome e cognome in calce a un documento). È evidente che, per sua natura, non è adeguatamente robusta.

3.3.2.1.2 La firma elettronica avanzata

La firma elettronica avanzata possiede i requisiti di cui all'art. 26 del Regolamento eIDAS e dell'art. 56 del DPCM 22 febbraio 2013. Fra i requisiti più importanti troviamo l'immodificabilità del documento dopo la firma, la riconducibilità della firma ad una persona garantendo alla stessa l'uso esclusivo degli strumenti di firma. Buoni esempi di firma elettronica avanzata sono diverse implementazioni basate sulla cosiddetta firma "grafometrica". Si tratta di soluzioni di firma che raccolgono le caratteristiche comportamentali e tipiche della firma autografa (attraverso l'uso di tavolette molto evolute) quali la velocità, l'inclinazione, la pressione, l'accelerazione (e rallentamenti), i tratti aerei.

Tutte queste informazioni legate in maniera certa al documento, consentono di raggiungere il risultato voluto.

Da notare che, ai sensi dell'art. 61 del DPCM 22 febbraio 2013, queste soluzioni possono essere utilizzabili limitatamente per i rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che rende disponibile la soluzione. Un tipico esempio è la struttura ospedaliera che rende disponibile presso i propri sportelli soluzioni di firma elettronica avanzata ai fruitori delle prestazioni sanitarie.

3.3.2.1.3 La firma elettronica qualificata

Questa tipologia di firma elettronica è oggetto di normativa comunitaria, in particolare, del Regolamento eIDAS e della Decisione di Esecuzione (UE) N°1506/2015 della Commissione dell'8 settembre 2015. Queste firme sono generabili esclusivamente con gli strumenti resi disponibili dai soggetti qualificati a tale scopo. L'elenco dei soggetti stabiliti in Italia è disponibile nella apposita sezione del sito dell'Agenzia. La Commissione Europea mette a disposizione un servizio che consente di conoscere tutti i prestatori di servizi fiduciari qualificati accreditati nell'Unione Europea (nel seguito, per brevità, "certificatori accreditati," altrimenti indicati come QTSP).

3.3.2.1.4 Il Sigillo Elettronico Qualificato

Il sigillo elettronico qualificato è stato introdotto nel nostro ordinamento con l'emanazione del già citato Regolamento eIDAS. Sostanzialmente è equivalente a una firma elettronica qualificata, con la differenza che non afferisce a una persona fisica, bensì a una persona giuridica. In altri termini, mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice fiscale ecc., da un sigillo possiamo risalire con certezza ad una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, ma non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.

3.3.2.2 Sottoscrizione dei documenti informatici

Quando previsto, il processo di sottoscrizione dei documenti informatici si svolge attraverso l'utilizzo della firma digitale conformemente a quanto disposto dalla vigente normativa.

Come riportato nell'art. 1, comma 1, del CAD, tale tipologia di firma è basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Come per le firme elettroniche qualificate, per generare una firma digitale è necessario

disporre di un dispositivo di firma sicuro e di un certificato qualificato di firma elettronica, entrambi rilasciati da un prestatore di servizi fiduciari qualificato. La coppia di chiavi di cui sopra è generata all'interno del dispositivo di firma, costituito da una *smart card* o una *business key* con porta USB, allo scopo di assicurare l'assoluta segretezza della chiave privata. All'interno del dispositivo è memorizzato anche il certificato qualificato, in cui viene riportata la chiave pubblica per creare il collegamento inscindibile tra questo codice e i dati identificativi del titolare.

Grazie all'utilizzo della firma digitale sono soddisfatti i requisiti di riservatezza, integrità, non ripudiabilità.

In aggiunta, i formati di firma impiegati sono CADES e PAdES.

CADES: attraverso il quale il documento firmato e il file con la firma digitale sono inseriti insieme in una busta. Tale busta, contenente il documento e il file della firma, è anch'essa un file con estensione .p7m. Infatti, tutti i file firmati digitalmente con modalità CADES hanno una seconda estensione .p7m. Le principali caratteristiche di questa modalità di firma sono:

- la possibilità di firmare qualsiasi tipo di documento (docx, .xlsx, ecc.), anche se è comunque raccomandabile firmare file in formato .pdf;
- la modifica del nome del documento dopo essere stato firmato. Volendo fare un esempio: un documento Prova.docx, una volta firmato digitalmente con modalità CADES, modificherà il suo nome in Prova.docx.p7m.;
- l'utilizzazione di specifici SW per verificare una firma digitale e per visualizzare il documento firmato.

PAdES: Nel caso di firma digitale apposta con modalità PAdES, invece, vengono sfruttate le caratteristiche dei documenti in formato .pdf e il file contenente la firma digitale viene inglobato insieme al documento stesso. Ecco le principali caratteristiche di questa modalità di firma:

- la modalità PAdES consente di firmare solo documenti in formato .pdf;
- un documento, una volta firmato con modalità PAdES, mantiene il suo nome;
- per verificare una firma digitale apposta con modalità PAdES e per visualizzare il documento firmato, è possibile utilizzare un qualsiasi software per la lettura dei file .pdf, come ad esempio Acrobat Reader.

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

Inoltre, le verifiche delle firme digitali dei documenti prodotti o ricevuti avvengono mediante l'impiego di software rilasciati da appositi enti certificatori, così come previsto dalla normativa di settore.

Infine, è necessario sottolineare l'esigenza di attribuire ai documenti informatici un riferimento temporale opponibile a terzi, sia per collocarli in un determinato contesto giuridico e istituzionale sia per verificare la loro valenza giuridica in rapporto alle caratteristiche e al livello di sicurezza dei sistemi utilizzati in fase di produzione. Definito all'interno del Regolamento *eIDAS validazione temporale*²², esso può essere definito come un insieme di dati in forma elettronica che collega altri dati in forma elettronica ad una particolare ora e data, così da provare che questi ultimi esistevano in quel momento. Se tale validazione:

²² Cfr. DPCM 22 febbraio 2013 - *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*, art. 1, comma 1 lett. m), e art. 41 del Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE – *eIDAS*.

- a) collega data ed ora ai dati in modo da escludere la possibilità di modifiche non rilevabili deidati;
- b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato (UTC);
- c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente, allora è da considerarsi qualificata e gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.

Per l'applicazione di una validazione temporale, il Comune ha l'obbligo di adottare almeno una delle seguenti modalità:

- a) registrazione di protocollo;
- b) PEC;
- c) servizio di marca temporale da certificatore accreditato;
- d) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- e) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica;
- f) il riferimento temporale contenuto nella segnatura del repertorio informatico gestito all'interno del sistema di gestione documentale.

3.3.3 Tipologie di formato del documento informatico

La leggibilità di un documento informatico dipende dalla possibilità²³ e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del documento informatico nel suo ciclo di vita.

La scelta dei formati dipende dalle caratteristiche proprie del formato e dei programmi che lo gestiscono. Le principali caratteristiche che è necessario tenere in considerazione nella scelta sono:

- a) apertura e standardizzazione: un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente;
- b) non proprietario;
- c) stabilità;
- d) inammissibilità di macroistruzioni;
- e) robustezza: possibilità di recuperare il più possibile un file corrotto;
- f) sicurezza: dipende da due elementi, ovvero sia il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno;

²³ Si vedano le *Linee guida* e in particolare il *Glossario* all'allegato 1.

- g) accuratezza e usabilità: la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili;
- h) funzionalità: la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico;
- i) supporto allo sviluppo: modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.);
- j) diffusione: è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Tale elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

I documenti informatici prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale, devono essere convertiti in uno dei formati standard riportati nell'allegato 2 delle *Linee guida*, al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo della loro forma e del loro contenuto. I documenti ricevuti in un formato diverso da quelli prescritti dal Manuale, se sottoscritti con firma digitale, sono recepiti dal sistema e convertiti in uno dei formati standard previsti. In caso di migrazione di documenti informatici, la corrispondenza fra il formato originale e quello migrato è garantita dal responsabile del servizio competente.

3.3.4 Copie, duplicati ed estratti

3.3.4.1 Duplicati del documento informatico e analogico

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento in grado di assicurare che il documento informatico contenga la medesima sequenza binaria del documento informatico originario da cui è tratto. Inoltre, il duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto, se prodotto conformemente alla regolamentazione tecnica, per cui non è necessario attestare la conformità all'originale da parte di un notaio o di un pubblico ufficiale. Il duplicato di un documento analogico, invece, è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti di legge.

3.3.4.2 Copia del documento informatico e analogico

La copia di un documento informatico è un documento informatico che, attraverso l'impiego di appositi processi e strumenti, assicura la corrispondenza della copia alle informazioni del documento informatico originario mediante l'utilizzo di uno dei formati idonei previsti dalla normativa vigente.

La copia del documento informatico ha la medesima valenza probatoria dell'originale da cui è

tratta, se la sua conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta, fermo restando l'obbligo di conservare l'originale informatico. La copia del documento analogico è definibile come la trascrizione o la riproduzione dell'originale da cui è tratta. Inoltre, si distingue in:

- a) **copia semplice**: è la mera trascrizione dell'originale, senza il rispetto dei suoi elementi formali;
- b) **copia imitativa**: riproduce il contenuto e la forma dell'originale da cui è tratta (es.: fotocopia);
- c) **copia conforme**: è la copia certificata in qualità di conforme all'originale da un pubblico ufficiale a ciò autorizzato.

3.3.4.3 Copia informatica del documento amministrativo analogico

La copia informatica di un documento analogico ha lo stesso valore dell'originale analogico da cui è tratta, se la sua conformità è regolarmente attestata da un funzionario a ciò preposto.

L'attestazione di conformità può essere:

- a) inserita nel documento informatico che contiene la copia informatica;
- b) prodotta come un documento separato, che, tuttavia, deve contenere un riferimento temporale e l'impronta informatica della copia.

Per entrambi i casi l'attestazione di conformità dev'essere sottoscritta digitalmente da un notaio o da un pubblico ufficiale a ciò deputato.

Per copia informatica di un documento analogico, invece, s'intende:

- a) una copia per immagine su supporto informatico di un documento analogico (scansione)²⁴, in cui forma e contenuto sono uguali all'originale. Inoltre, ha la stessa efficacia probatoria dell'originale, se:
 - la sua conformità è attestata da un notaio o da un altro pubblico ufficiale a ciò deputato, con dichiarazione allegata al documento informatico e asseverata secondo le *Linee guida*;
 - è formata nel rispetto delle *Linee guida* e se la sua conformità all'originale non è espressamente disconosciuta.
- b) una copia informatica del documento analogico, data dal documento informatico avente contenuto identico a quello del documento analogico da cui è tratta, ma diversa nella forma. Essa ha la medesima efficacia probatoria dell'originale, se ad essa è apposta o associata, da parte della persona che la spedisce o la rilascia, una firma digitale o un'altra firma elettronica qualificata e dichiarazione di conformità.

3.3.4.4 Estratto informatico di un documento amministrativo informatico

²⁴ Come disposto all'art. 22, comma 1-bis, del CAD, la scansione dei documenti analogici dev'essere prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

La copia che riproduce solo parzialmente il contenuto del documento è definita *estratto*. Esso, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l'estratto, ha la medesima efficacia probatoria dell'originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Qualora sia richiesta dalla natura dell'attività, l'attestazione di conformità può essere inclusa nello stesso documento informatico contenente l'estratto, oppure può essere generata come documento informatico separato; in entrambi i casi l'attestazione dev'essere firmata digitalmente o con firma elettronica qualificata da un notaio o da un pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, quest'ultimo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto di attestazione.

3.3.4.5 Copia analogica di un documento amministrativo informatico

La copia analogica di un documento amministrativo informatico corrisponde normalmente alla sua stampa cartacea.

La copia su supporto analogico di un documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la medesima efficacia probatoria dell'originale da cui è tratta, dev'essere certificata come conforme all'originale da un pubblico ufficiale deputato all'esecuzione di tale attestazione nello svolgimento delle proprie funzioni, salvo che la conformità allo stesso non sia espressamente disconosciuta. Una copia analogica estratta dal sistema di gestione documentale è da ritenersi conforme all'originale secondo quanto disposto dall'art. 23-ter, comma 5, del CAD.

Comunque, ove previsto, resta obbligatoria la conservazione dell'originale informatico.

4. SCAMBIO DI DOCUMENTI

Questo capitolo fornisce delle prescrizioni relative allo scambio dei documenti all'interno e all'esterno del Comune. In particolare, sono trattate le procedure operative per lo scambio dei documenti in entrata, in uscita e interni, a loro volta suddivisi in formali e informali.

4.1 Documenti in entrata

I documenti ricevuti su supporto analogico pervengono attraverso la consegna a mano, fax o servizio postale. In questi casi, si provvede alla protocollazione della documentazione, indicandola modalità di ricezione della stessa, l'oggetto, il mittente, la classificazione, l'assegnazione alla/eUO competente/i. Successivamente, se possibile, i documenti vengono scansionati. Infine, qualora il documento sia presentato a mano in duplice copia, sulla copia da restituire viene apposto il timbro recante la seguente dicitura: "Comune di Abano Terme – data – pervenuto al protocollo".

In caso di presentazione del solo originale, viene preferibilmente concordata la trasmissione della ricevuta di avvenuta protocollazione a mezzo mail/PEC oppure si procede immediatamente alla protocollazione e si consegna ricevuta cartacea.

I documenti informatici, invece, pervengono attraverso:

- a) **Posta elettronica semplice**: in tal caso, è da tenere presente che la mail inviata attraverso tale tipologia di posta elettronica è da considerarsi sottoscritta con firma elettronica debole ed è soggetta alla registrazione a protocollo, solo nel caso in cui il suo contenuto sia rilevante ai fini giuridico-probatori. Se così fosse, il software acquisisce un file del testo della mail in formato EML al momento della registrazione;
- b) **PEC**: essa rappresenta un mezzo di trasmissione con cui inviare comunicazioni e documenti in modo pienamente valido agli effetti di legge. Dunque, viene impiegata nei casi in cui si rivela necessario avere la prova opponibile a terzi dell'invio e della consegna del messaggio di posta. A differenza della posta elettronica semplice, la PEC presenta le seguenti peculiarità:
- identifica il mittente, se coincidente con l'autore del documento;
 - garantisce l'integrità e la riservatezza dei messaggi;
 - garantisce la data certa di spedizione e di consegna dei messaggi;
 - rilascia la ricevuta di avvenuta consegna o di avviso di mancato recapito;
 - il gestore si cura della tracciatura dei messaggi.

Nel Comune di Abano Terme, lo scarico e la protocollazione di mail e PEC sono effettuati dall'apposito software. Qualora l'oggetto risulti incompleto, viene completato manualmente dal personale del Protocollo.

Infine, è bene ricordare che, nel caso in cui la comunicazione/istanza sia costituita dal mero corpo di testo della PEC, è necessario procedere alla registrazione del messaggio sul software di protocollo informatico solo se il contenuto risulta rilevante ai fini giuridico-probatori;

- c) **Supporti rimovibili**: questa casistica comprende, nella fattispecie, il deposito di pratiche da parte di ditte o professionisti incaricati della realizzazione ed esecuzione di progetti di edilizia pubblica o di viabilità e, fino al momento di entrata in vigore del nuovo Regolamento edilizio, tale situazione è prevista anche per gli elaborati di edilizia privata. In tal caso, vengono consegnati al Protocollo dei supporti magnetici o dei supporti ottici contenenti la copia informatica di documenti o elaborati originariamente cartacei, su cui viene apposta l'etichetta recante la segnatura di protocollo.
- d) **Ricezione di documenti informatici tra PA tramite cooperazione applicata**

Come previsto dall'allegato 6 delle Linee Guida, per dare seguito alla comunicazione tra AOO mittente e AOO destinataria della P.A., dal 01/01/2022 è possibile utilizzare la modalità di trasmissione dei protocolli in cooperazione applicativa utilizzando il Simple Object Access Protocol (SOAP/o preferibilmente REST).

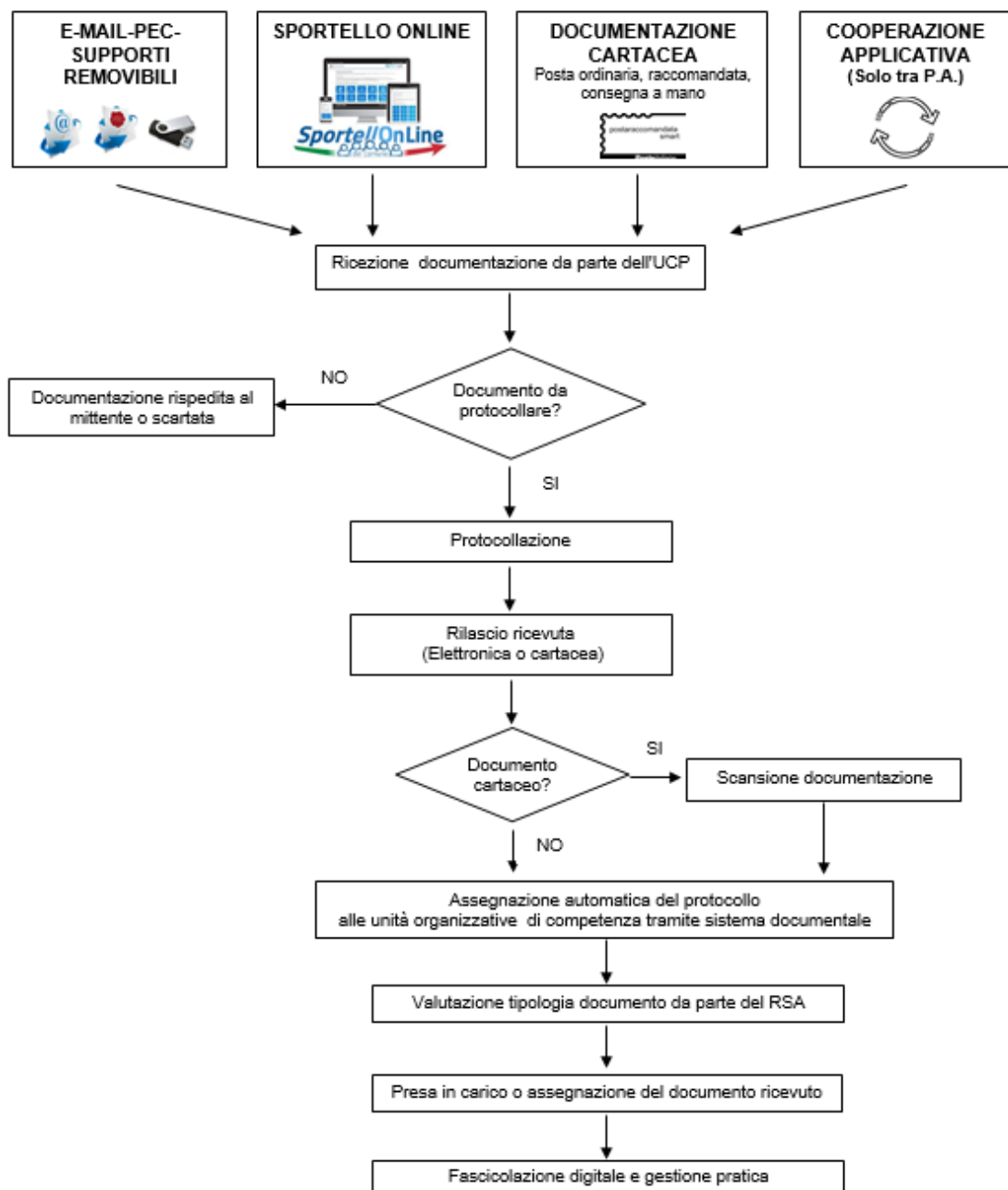
Per assicurare la comunicazione tra AOO in cooperazione applicativa, le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) con il prefisso condiviso dagli endpoint di esposizione dei servizi indicati nell'Appendice B dell'Allegato 6 delle Linee Guida.

Le AOO mittente e AOO destinataria assicurano il non ripudio della comunicazione,

provvedendo alla firma dei messaggi scambiati ed al loro trasposto su canale TLS tramite SOAP coerentemente alla specifica WS-Security.

e) **Ricezione di documenti informatici da portale web dell'Ente**

I documenti digitali possono anche essere ricevuti dall'Ente dal sito internet istituzionale, tramite apposito servizio web. Il cittadino, dopo essersi autenticato al portale con SPID o CIE, può avviare on line la procedura di erogazione dei servizi messi a disposizione dall'Ente. Al termine dell'operazione, verrà rilasciata all'utente una ricevuta attestante l'avvenuta presa in carico della sua richiesta.



4.2 Documenti in uscita

Le comunicazioni con le altre pubbliche amministrazioni, i professionisti aventi l'obbligo d'iscrizione in albi ed elenchi e i soggetti tenuti ad iscriversi nel registro delle imprese si svolgono attraverso l'utilizzo della PEC.

Le comunicazioni con i cittadini avvengono attraverso:

- a) l'utilizzo della PEC o di un servizio elettronico di recapito certificato qualificato, qualora individuato;
- b) posta ordinaria;
- c) messo comunale;
- d) consegna a mano della documentazione.

I documenti in uscita sono generalmente firmati dal Responsabile del Procedimento Amministrativo e successivamente trasmessi al destinatario dopo essere stati registrati autonomamente dagli uffici.

Il Comune di Abano Terme è tenuto alla produzione di documenti originali digitali, come già ribadito. Qualora fosse necessario trasmettere ad altre pubbliche amministrazioni o a cittadini dei documenti su supporto analogico, l'originale dovrà comunque essere formato con gli strumenti informatici in uso ed essere registrato. La copia analogica del documento informatico estratta dal sistema²⁵ sarà oggetto di trasmissione secondo le modalità convenute con il destinatario.

4.3 Documenti interni

Per documenti interni s'intendono tutti quelli prodotti e destinati all'interno del Comune di Abano Terme e sono suddivisibili in interni formali e informali.

I documenti interni sono formati attraverso l'utilizzo di tecnologie informatiche, ma possono essere eccezionalmente sottoscritti con firma autografa.

4.3.1 Documenti interni formali

Assumono la definizione di interni formali i documenti redatti dai Responsabili del Provvedimento nello svolgimento delle proprie funzioni con lo scopo di documentare fatti inerenti alle attività svolte e alla regolarità dell'azione amministrativa, qualora ritengano abbiano carattere giuridico-probatorio.

La trasmissione tra le UO di documenti informatici interni formali deve avvenire tramite immissione e contestuale registrazione degli stessi all'interno del sistema di protocollo informatico. I documenti devono essere protocollati come interni ed essere successivamente assegnati alle altre UO coinvolte.

4.3.2 Documenti interni informali

La trasmissione tra le UO di documenti interni informali avviene attraverso l'utilizzo di:

- a) Intranet comunale;

²⁵ Identificata con contrassegno, secondo le modalità descritte nell'art. 23-ter, comma 5, del CAD.

- b) posta elettronica interna al Comune.

4.4 Descrizione del flusso di lavorazione dei documenti

4.4.1 Flusso in entrata

All'interno del Comune l'Ufficio Protocollo ha il compito di ricevere e registrare tutti i documenti, digitali e analogici, in entrata che rivestono un valore giuridico-probatorio.

I documenti amministrativi informatici da protocollare in entrata pervengono secondo una delle modalità descritte al paragrafo 4.1.

Nel caso in cui le UO del Comune prevedano l'arrivo di notevoli quantità di documenti da protocollare entro un ristretto arco temporale e relativi a selezioni, gare o ad altri procedimenti, i competenti RPA sono tenuti ad informare quanto prima il Protocollo, anche via mail, al seguente indirizzo: protocollo@abanoterme.net.

Gli addetti alla protocollazione, per i documenti da loro trattati, eseguono di norma la classificazione sulla base del Titolario di classificazione adottato presso l'AOO e provvedono ad inviarli tramite il sistema documentale all'unità organizzativa di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, ritrasmette il documento all'ufficio protocollo;
- in caso di verifica positiva, esegue l'operazione di presa in carico e fascicolazione digitale;
- assegna le eventuali visibilità ulteriori rispetto a quelle attribuite automaticamente in base alla classificazione;
- gestisce il documento

Terminata la fase di protocollazione, i documenti sono portati automaticamente nella disponibilità dei soggetti competenti alla loro trattazione grazie al sistema documentale adottato dall'Ente. Il sistema consente comunque di assegnare la visibilità dei documenti ad altri soggetti singoli, uffici o gruppi trasversali di addetti configurati sul sistema. Questa modalità operativa consente di portare il documento all'attenzione di tutti i soggetti interessati, attraverso la condivisione interna del sistema documentale. Si tratta di una modalità particolarmente utile per favorire la conoscenza, e la disponibilità diffusa, di tipologie documentali quali circolari, manualistica, disposizioni operative, documenti di interesse generale ecc.

Viceversa, i documenti risultano inesistenti per i soggetti ai quali non è stata assegnata, automaticamente o meno, la visibilità specifica. Si tratta di un meccanismo semplice ed affidabile per garantire la corretta gestione dei documenti riservati, contenenti dati sensibili o giudiziari, o comunque particolarmente delicati.

Nel caso di assegnazione errata, l'unità organizzativa che riceve il documento comunica l'errore all'ufficio protocollo che ha assegnato il documento, affinché proceda ad una nuova assegnazione

Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'unità organizzativa competente attraverso il sistema di gestione documentale al

termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione.

I documenti ricevuti dall'amministrazione in formato cartaceo, di regola acquisiti in formato immagine o altro formato standard non modificabile con l'ausilio di scanner, una volta concluse le operazioni di registrazione segnatura e assegnazione sono fatti pervenire al Servizio di competenza per via informatica attraverso il sistema di gestione documentale. L'originale cartaceo viene anch'esso trasmesso alla struttura di competenza, mediante collocazione nell'apposita cartella presso l'Ufficio Protocollo.

L'unità organizzativa competente ha notizia dell'arrivo del documento tramite apposita "notifica" generata automaticamente dal sistema documentale.

4.4.1.1 Ricezione di documenti informatici nella casella di posta elettronica istituzionale del Comune

Come già anticipato, la mail è un mezzo di trasmissione che può costituire anche un documento informatico nel caso in cui il messaggio sia contenuto nel corpo della stessa. Il corpo della mail e gli eventuali allegati su cui non sia stata apposta una firma digitale possono in ogni caso essere considerati come sottoscritti dal mittente, ma con firma elettronica semplice.

Sarà compito del RPA della UO verificarne la provenienza, valutare l'accettazione o il rigetto della firma elettronica semplice e, in aggiunta, chiedere al mittente un documento informatico sottoscritto digitalmente, da cui scaturirà una nuova registrazione con un diverso numero di protocollo rispetto al precedente.

4.4.1.2 Ricezione dei documenti informatici tramite PEC del Comune

La PEC è un canale di trasmissione attraverso cui inviare o ricevere un documento informatico, il quale può essere allegato o costituito dal corpo stesso della PEC.

Presso il Comune di Abano Terme la PEC è integrata all'interno del sistema di protocollo informatico attualmente in uso ed è configurata per la ricezione di documenti informatici solamente da/a altre caselle di posta elettronica certificate.

Una volta effettuata la registrazione, la UO a cui viene assegnato il documento informatico dovrà provvedere, come già anticipato precedentemente, alla sua fascicolatura.

Inoltre, il software di protocollo informatico genera tutte le ricevute previste dalla normativa vigente in materia di posta elettronica certificata.

Nel caso in cui il documento sia pervenuto in un formato diverso da quelli ammessi nell'Allegato 6 - *Formati*, con o senza firma digitale, deve comunque essere registrato a Protocollo. Sarà poicura del RPA:

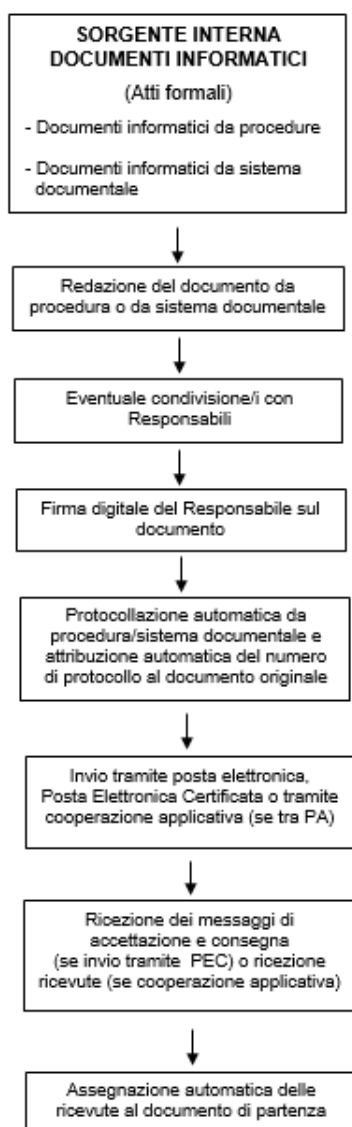
- a) valutare l'accettazione o meno del documento informatico assegnato non sottoscritto o non conforme alle prescrizioni sui formati degli standard internazionali;
- b) richiedere il documento al mittente nel formato prescritto dalla normativa vigente.

4.4.2 Flusso in uscita

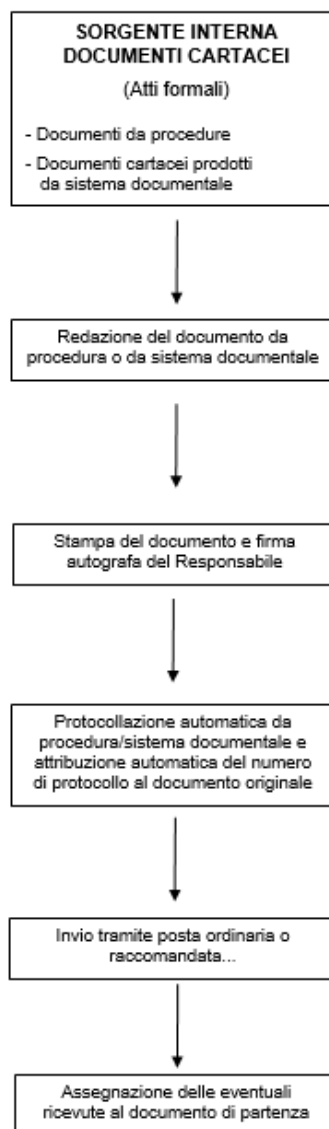
Il documento informatico prodotto dai vari settori del Comune dev'essere:

- a) preferibilmente redatto nel formato PDF/A o in uno degli altri formati previsti dalla normativa vigente;
- b) redatto seguendo le indicazioni riportate nel paragrafo 3.3 - *Formazione dei documenti informatici e dei documenti amministrativi informatici*;
- c) protocollato;
- d) correttamente fascicolato.

SORGENTE INTERNA - DOCUMENTI INFORMATICI



SORGENTE INTERNA - DOCUMENTI CARTACEI



4.4.3 Flusso dei documenti interni formali

I documenti interni scambiati tra le UO del Comune possono essere costituiti da:

- a) documenti redatti attraverso l'impiego di specifici *software* e firmati digitalmente;
- b) documenti informatici formati per mezzo dell'acquisizione della scansione di un documento originariamente analogico;
- c) documenti costituiti dal corpo di una mail.

Nei casi a) e b), il flusso risulta analogo rispetto a quanto descritto per i documenti in partenza (vedi paragrafo 4.4.2 – *Flusso in uscita*), ma selezionando la casella *interni* nel software di protocollo informatico.

5. PRODUZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

Il presente capitolo tratta i criteri e le modalità di produzione delle registrazioni a protocollo informatico. Inoltre, le operazioni di seguito descritte riguardano la conservazione delle registrazioni e le procedure di modifica e di annullamento delle informazioni che concernono le attività di registrazione.

Sono trattate sia le modalità generali di registrazione che quelle particolari, quali la repertoriatura.

5.1 Registrazione dei documenti

La registrazione consiste nell'attività obbligatoria della memorizzazione delle informazioni fondamentali relative al documento e nello specifico nei termini del contenuto, dell'autore e della modalità di trasmissione.

La registrazione, quindi, riguarda tutti i documenti del Comune di Abano Terme dai quali derivano diritti o doveri in capo ad esso o a terzi coinvolti.

La registrazione dei documenti sul sistema di protocollo informatico consente di identificare il singolo documento in modo univoco, individuando informazioni certe come data, forma e provenienza.

5.2 Registro di protocollo

Il registro di protocollo è un documento informatico prodotto e redatto secondo le modalità previste dalla vigente normativa e nello specifico secondo l'art. 53, comma 1, del DPR 445/2000.

Nell'ambito della AOO Comune di Abano Terme, il registro di protocollo è unico e la sua numerazione è univoca, progressiva e costituita da una serie di sette cifre numeriche che parte all'inizio di ogni anno solare per concludersi il 31 dicembre.

Ogni numero di protocollo individua un unico documento e, ne deriva, che ogni documento ha apposto o associato un solo numero di protocollo.

L'inserimento dei dati di un documento nel registro di protocollo attesta l'esistenza giuridica del

documento stesso per l'amministrazione che lo ha prodotto o ricevuto. Esiste, tuttavia, la possibilità di annullamento della registrazione, come descritto nel paragrafo dedicato.

È assolutamente proibita la registrazione a protocollo di documenti non ancora esistenti, specie nei casi di documenti in uscita. La prescrizione vale sia per i documenti non ancora prodotti sia per quelli non perfezionati da una sottoscrizione. La prenotazione di un numero di protocollo al fine di fissare la data e l'ora, infatti, si qualifica come falso in atto pubblico.

Non è consentita la protocollazione multipla di un documento. A questa norma basilare, tuttavia, si applicano delle eccezioni, specie in occasione di invii multipli da parte del mittente, che sono descritte nei paragrafi successivi.

Il registro di protocollo è un atto pubblico di fede privilegiata che attesta l'esistenza e l'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso. In funzione di tale caratteristica, il registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Ai fini della permanenza dei requisiti di immutabilità, in ambito di protocollo informatico, il registro giornaliero di protocollo deve essere trasmesso al sistema di conservazione entro la giornata lavorativa successiva alla sua produzione, come ribadito nel par. 3.1.6 delle *Linee guida*. Le eventuali modifiche apportate alle registrazioni di protocollo, sempre tracciate, vengono trasmesse al sistema di conservazione con il registro giornaliero della data della loro produzione. La stampa periodica del registro di protocollo su supporto cartaceo è stata sospesa.

5.3 Elementi della registrazione di protocollo

La registrazione di protocollo è formata da diversi elementi. Una parte di questi elementi sono **obbligatori**, in quanto la loro presenza è giuridicamente rilevante:

- data di registrazione;
- numero di protocollo;
- corrispondente (può trattarsi del mittente del documento in entrata, il destinatario del documento in uscita e il corrispondente interno per i documenti interni formali);
- oggetto;
- impronta del documento informatico;
- indice di classificazione.

Inoltre, esistono diversi **elementi non obbligatori** che possono essere oggetto dell'attività di registrazione:

- tipologia (documenti in arrivo, partenza o interni);
- riservatezza;
- numero di protocollo del documento ricevuto;
- data del documento ricevuto;
- formato o modalità di trasmissione;
- tipo di documento;
- data e ora di arrivo (campo obbligatorio per documenti in arrivo che riguardano appalti e concorsi);
- numero degli allegati (campo compilato automaticamente per le PEC);
- annotazioni.

5.4 Modalità di registrazione di protocollo e di assegnazione

I documenti che pervengono dall'esterno al Comune di Abano Terme sono registrati tempestivamente e una sola volta come documento in entrata.

I documenti prodotti e inviati dal Comune di Abano Terme ad altri soggetti devono essere registrati solo quando perfezionati e costituiscono documenti in uscita.

I documenti interni a carattere formale, normalmente scambiati tra UO diverse del Comune o tra uffici diversi della medesima UO, devono essere registrati solo una volta dall'ufficio mittente.

I documenti informatici vengono acquisiti nel sistema di protocollo tramite le procedure descritte nel capitolo che segue, mentre i documenti analogici possono essere sottoposti al procedimento di scansione ottica per acquisirne una copia nel sistema.

5.4.1 La segnatura di protocollo

La segnatura di protocollo consiste nell'apposizione o nell'associazione dei dati della registrazione di protocollo rispettivamente al documento analogico e a quello digitale. I dati sono associati in forma permanente e non modificabile e consentono l'identificazione univoca del documento.

Le informazioni apposte o associate ai documenti, ai sensi degli artt. 9, 20 e 21 del DPCM 3 dicembre 2013 sul protocollo informatico (confermati dalle *Linee guida*), sono le seguenti:

- il codice identificativo dell'ente;
- il codice identificativo dell'AOO;
- il codice identificativo del registro;
- data di registrazione;
- numero progressivo del protocollo.

Inoltre, nella segnatura sono indicati anche i seguenti elementi:

- indicazione della UO dell'Ente produttore del documento;
- titolo del Piano di classificazione;
- classe.

I dati descritti sono associati al documento trasmesso dal Comune di Abano Terme e immessi nello stesso messaggio in un file conforme al linguaggio di marcatura XML, compatibile con un file XML Schema.

Il file XML deve contenere anche le seguenti informazioni:

- l'oggetto;
- il mittente;
- il destinatario.

Sul documento in formato analogico, in seguito alla registrazione, viene apposta la segnatura con una etichetta adesiva. L'etichetta è prodotta da una stampante e generata a partire dai dati inseriti nel sistema. L'etichetta riporta il nominativo dell'Ente, il numero di protocollo, la data di registrazione e la classificazione.

5.4.2 Documenti soggetti a registrazione particolare e a repertoriazione

Alcuni documenti prodotti dal Comune di Abano Terme non vengono registrati nel registro di protocollo, ma in appositi registri. Tali tipologie di documenti sono elencate nell'*Allegato 3 – Documenti soggetti a registrazione particolare*.

Per i documenti soggetti a forme di registrazione particolare sono previste, ad ogni modo, le stesse operazioni contemplate per la gestione degli altri documenti. Per esempio, è sempre possibile eseguire la registrazione, la classificazione e la fascicolazione dei documenti.

Di conseguenza anche i registri o repertori, declinati secondo la tipologia del documento, contengono i dati che seguono:

- tipologia di registro o repertorio;
- numero di registro o di repertorio;
- data;
- elementi identificativi del soggetto;
- elementi identificativi dell'oggetto;
- dati di classificazione e fascicolazione;
- annotazioni.

5.4.3 Modalità operative per la gestione dei documenti e dei relativi allegati

Al termine delle operazioni di registrazione, il sistema di protocollo informatico produce una ricevuta di registrazione che contiene i seguenti elementi:

- numero e data di protocollo;
- indicazione dell'AOO che ha acquisito il documento;
- mittente;
- oggetto;
- numero e descrizione degli allegati se presenti;
- indicazione di responsabilità, cioè l'indicazione dell'UO/RPA competente a cui il documento è assegnato;
- operatore che ha effettuato la registrazione di protocollo.

In caso di registrazione di documento digitale acquisito via PEC, la ricevuta di protocollazione è generata dal sistema e trasmessa attraverso le sue funzionalità. Nel caso in cui il documento digitale sia pervenuto attraverso posta elettronica ordinaria, la ricevuta può essere analogamente generata e trasmessa.

In caso di ricezione allo sportello di un documento analogico direttamente dal mittente, o da una persona delegata a tale funzione, che faccia esplicita richiesta di una ricevuta di consegna del documento, sarà cura dell'operatore di Protocollo rilasciare la ricevuta prodotta dal sistema che può essere ritirata o trasmessa via posta elettronica o PEC dichiarate al momento della consegna. Se il mittente è in possesso della copia della documentazione, sulla stessa verrà apposto il timbro di ricevuta.

L'Ufficio Protocollo, infine, non rilascia ricevute di registrazione per documenti che non sono soggetti a protocollazione né rilascia fotocopia del documento analogico con segnatura di

protocollo, in quanto tale procedura non produce alcun effetto giuridico.

5.4.4 Procedure specifiche nella registrazione a protocollo

5.4.4.1 Protocolli riservati

Il Comune di Abano Terme produce e riceve documenti che, in funzione ai dati contenuti, sono considerati come riservati e per i quali sono previste forme controllate di accesso. In base alla normativa vigente, i documenti riservati sono:

- i documenti che contengono una particolare categoria di dati personali atti a rilevare «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona», come riportato dall'art. 9 del GDPR;
- i documenti che rilevano i dati personali relativi «alle condanne penali o ai reati e a connesse misure di sicurezza», previsti all'art. 10 del GDPR;
- i documenti coperti da segreto statistico;
- i documenti di carattere politico e di indirizzo e nello specifico quelli relativi alle misure di sicurezza attuate nell'ambito del Comune di Abano Terme.

I documenti registrati che hanno queste caratteristiche, in base ai criteri utilizzati al momento dell'assegnazione, sono accessibili solo alle persone autorizzate in funzione della tipologia di documento e al procedimento amministrativo innescato. La riservatezza, quindi, è individuata dai responsabili delle UO che producono i documenti e codificata nel *Registro delle attività di trattamento* e l'operazione è demandata agli operatori del protocollo.

I documenti contenenti le citate categorie di dati o ritenuti riservati che pervengono all'Ufficio Protocollo in forma analogica, dopo essere stati registrati e scansati, devono essere inseriti in una busta chiusa fino allo smistamento.

5.4.4.2 Documenti esclusi dalla registrazione a protocollo

Tutti i documenti informatici prodotti o ricevuti dal Comune di Abano Terme sono soggetti a registrazione, come previsto dal DPR 445/2000. **Le eccezioni previste sono quelle ricordate nel paragrafo 5.4.2 – Documenti soggetti a registrazione particolare e a repertoriazione, cui si aggiungono i documenti esclusi dalla registrazione riportati nell'Allegato 5.**

Al fine di garantire la conformità alle normative in materia di documentazione amministrativa e gestione informatica dei documenti, il documento è considerato ricevuto solo se perviene direttamente come allegato; collegamenti a repository esterni non garantiscono la riferibilità e la conservabilità del contenuto.

Per la gestione, i rischi operativi e le azioni operative si rimanda alla lettura del del paragrafo 5.4.5.6 - *Procedura per la gestione delle Pec e mail ordinarie contenenti link esterni per l'accesso agli allegati.*

Al di fuori di queste categorie, non sono ammesse eccezioni all'obbligo di protocollazione, segnatura e corretta gestione dei documenti se non espressamente autorizzate dal Responsabile del Protocollo o dal Responsabile della Transizione Digitale (RTD).

5.4.4.3 Protocollo differito

L'uso del protocollo differito è consentito solo in alcuni casi eccezionali e solo con motivato provvedimento del responsabile del servizio di Protocollo, qualora non sia possibile evadere la corrispondenza ricevuta e qualora dalla mancata registrazione a protocollo del documento entro la giornata lavorativa di arrivo derivasse la lesione di diritti di terzi. Si cita, a titolo esemplificativo, l'arrivo di un'ingente mole di corrispondenza in prossimità della scadenza dei termini di presentazione di una domanda per un bando.

La registrazione differita di protocollo informatico è consentita solo per i documenti in arrivo.

Il provvedimento motivato indica espressamente la data alla quale è stata rinviata la registrazione e la causa del differimento ed è emesso dal Responsabile del Servizio di Protocollo per i documenti che arrivano al Protocollo, mentre per i documenti ricevuti dalla UO competente il differimento deve essere chiesto dalla UO stessa al responsabile del Protocollo, dichiarando la motivazione e la data dell'effettivo ricevimento. Il provvedimento, dunque, deve sempre contenere l'individuazione dei documenti per i quali la registrazione è differita, il motivo e la data termine in cui la registrazione si deve effettuare.

5.4.4.4 Correzioni ortografiche e informazioni aggiunte alle registrazioni

L'intervento di correzione sulle registrazioni di protocollo è consentito, secondo normativa, per intervenire su errori ortografici o per aggiungere informazioni funzionali alla ricerca del documento. Il sistema traccia automaticamente le correzioni, memorizzando il dipendente che le ha effettuate, l'ora e la data di intervento e mantenendo anche le informazioni precedenti alla correzione.

Qualora la correzione dovesse riguardare campi non modificabili, si dovrà, invece, procedere all'annullamento della registrazione di protocollo.

5.4.4.5 Annullamento delle registrazioni di protocollo

In base all'art. 54 del DPR 445/2000, le registrazioni di protocollo possono essere annullate, quando uno o più campi non modificabili della registrazione vengono annullati per motivate e verificate ragioni. I motivi che possono portare all'annullamento della registrazione sono:

- il mero errore di inserimento delle informazioni registrate in modo immodificabile ma riportate correttamente nel documento;
 - il documento non doveva essere prodotto, ovvero le motivazioni per cui il documento è stato prodotto sono venute meno. In tal caso, la registrazione può essere annullata solo se il documento non è già stato diffuso.

La necessità di modificare anche un solo campo tra quelli obbligatori e immodificabili della

registrazione di protocollo per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare la registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, insieme a data, ora e autore dell'annullamento e agli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.

In tale ipotesi la procedura riporta l'annotazione di annullamento. Il sistema inoltre registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Solo il Responsabile della gestione documentale e del Servizio di Protocollo informatico ad annullare, direttamente o delegando gli addetti, una registrazione di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile della gestione documentale e del Servizio di Protocollo informatico, contenente il numero di protocollo da annullare, i motivi dell'annullamento e, se il documento è stato riprotocollato correttamente, l'indicazione del nuovo numero di protocollo attribuito al documento.

L'annullamento avviene attraverso una funzione specifica del sistema, che consente, comunque la lettura delle informazioni registrate.

Il documento, quindi, acquisisce una nuova segnatura che fa riferimento alla corretta registrazione.

Nel caso di documenti analogici, la nuova segnatura deve essere apposta senza rimuovere la precedente, sulla quale occorre annotare la dicitura "annullato" e gli estremi del provvedimento di annullamento.

Qualora l'annullamento riguardasse un documento che non doveva essere protocollato dal Comune di Abano Terme, il responsabile del servizio di Protocollo provvederà comunque alla conservazione del documento registrato e annullato, anche fotoriprodotta o acquisita dal sistema tramite immagine. Tutte le procedure di annullamento saranno registrate nel registro giornaliero di protocollo e mandate in conservazione entro la giornata lavorativa successiva alla loro produzione.

Il numero di protocollo annullato non potrà più essere utilizzato.

L'annullamento della registrazione è una procedura distinta dall'annullamento del provvedimento come previsto dalla L. 241/1990: in questo caso non si provvede all'annullamento della registrazione, ma all'emanazione di un nuovo provvedimento che sostituisce e annulla il precedente, richiamandolo e motivando le cause. Anche la nuova registrazione di protocollo deve riportare in nota gli estremi del documento sostituito.

Il documento la cui registrazione è annullata, fatto salvo il caso di restituzione ad altra persona fisica o giuridica per non afferenza a procedimenti amministrativi del Comune di Abano Terme, deve essere comunque conservato nel fascicolo corrispondente.

In nessun caso è possibile annullare la registrazione di un documento ricevuto o diffuso via PEC, in quanto il corrispondente è già in possesso del documento originale. In presenza di documento in partenza, sarà dunque necessario redigere un nuovo documento che richiami il numero di protocollo del precedente annullato.

5.4.5 Casi particolari di registrazioni di protocollo

Esistono casi di documenti particolari quanto alla tipologia o alle modalità di ricezione che richiedono specifiche strategie di registrazione e di gestione.

5.4.5.1 Lettere anonime

Le lettere trasmesse all'Ufficio Protocollo tramite posta convenzionale che contengono dichiarazioni anonime o con firma illeggibile o non idonea all'identificazione del mittente vengono registrate nel sistema, indicando nel campo del corrispondente la dicitura "Anonimo" o annotando le specifiche "Lettera non firmata" o "Mittente illeggibile".

La registrazione di questi documenti pervenuti all'Ufficio è subordinata al ricevimento di specifiche istruzioni espresse dal Segretario o da persona da esso delegata, in particolar modo se il contenuto della lettera è di tipo diffamatorio o delatorio e non rientri espressamente nei procedimenti dell'Ente.

5.4.5.2 Segnalazioni anonime

Parimenti la segnalazione anonima riguardante questioni di sicurezza o di ordine pubblico che può avviare procedimenti dell'Ente e perviene attraverso i canali di posta convenzionale senza firma viene protocollata, indicando "anonimo" nel campo mittente e in seguito assegnata alla UO competente.

5.4.5.3 Lettere prive di firma

Le lettere prive di firma pervenute al Protocollo da mittente noto devono, così come le PEC, essere protocollate attestando data e provenienza certa del documento.

È compito del RPA della UO assegnataria del documento stabilire se lo stesso è giuridicamente valido ai fini del procedimento.

5.4.5.4 Corrispondenza da non aprire

Normalmente la corrispondenza pervenuta all'Ufficio Protocollo viene aperta per consentire le operazioni di registrazione e lo smistamento. I plichi e le buste non vengono aperte, ma smistate direttamente alle UO assegnatarie:

- se presentano le diciture "personale", "s.p.m." o analoghe e diciture quali "riservato" o "segreto" e destinate a personale dipendente o figure istituzionali;
- se si tratta di corrispondenza legata a procedure di gara.

Nel primo caso l'Ufficio appone il timbro con la data di ricevimento e il documento potrà essere registrato in seguito al parere del destinatario. Nel secondo caso l'Ufficio potrà procedere con la registrazione dei dati ricavabili dalla busta, da completare a cura della UO assegnataria per quanto concerne il numero e la tipologia di allegati e l'acquisizione ottica degli stessi.

5.4.5.5 Domicili eletti

Per la corrispondenza o gli atti giudiziari ricevuti con la dicitura “Domicilio eletto” o “c/o Casa comunale” non sussiste l’obbligo di protocollazione. Sulla busta viene apposto il timbro per attestare la data di ricezione e/o pervenimento da parte dell’Ufficio Protocollo.

Il Comune si è dotato di un Registro interno (non protocollo ufficiale) per documentare la consegna di posta al cittadino.

Non è consentito registrare al protocollo la corrispondenza per la quale è prevista la procedura notificatoria di irreperibilità.

5.4.5.6 Procedura per la gestione delle Pec e mail ordinarie contenenti link esterni per l’accesso agli allegati

La presente procedura disciplina le modalità di gestione, protocollazione e conservazione delle comunicazioni pervenute via PEC o mail che contengono collegamenti ipertestuali (link) per l’accesso a documenti allegati, al fine di garantire la conformità alle normative in materia di documentazione amministrativa e gestione informatica dei documenti.

L'utilizzo di link esterni non garantisce:

- La persistenza dei contenuti nel tempo (i link possono scadere o essere rimossi).
- La provenienza certa e la non alterabilità dei documenti allegati.
- La validità legale e probatoria del documento informatico ai sensi delle norme vigenti.

Tale pratica espone l’Amministrazione a rischi quali:

- Perdita di documentazione ai fini della conservazione digitale a norma.
- Inammissibilità giuridica di documenti presentati in procedimenti amministrativi.
- Violazione del principio di immodificabilità e integrità del documento amministrativo informatico.

A partire dalla data di adozione del presente provvedimento:

- È fatto obbligo ai mittenti esterni di trasmettere direttamente via PEC tutti gli allegati inclusi nella comunicazione, anche in più invii separati, purché con riferimento chiaro all’oggetto e in ordine crescente numerico (es. "oggetto:.... – Invio 1/3, . "oggetto:.... – Invio 2/3", ecc.).
- Il documento è considerato ricevuto solo se perviene direttamente come allegato; collegamenti a repository esterni non garantiscono la riferibilità e la conservabilità del contenuto.
- Eventuali eccezioni dovranno essere autorizzate esplicitamente dal Responsabile del Protocollo o dal Responsabile della Transizione Digitale (RTD).

Gli Uffici destinatari di PEC o mail contenenti link dovranno:

1. Verificare l’eventuale presenza di allegati direttamente nella PEC o mail.
2. Se il messaggio contiene solo un link, verrà protocollata esclusivamente al fine di attestare l’avvenuta corrispondenza in entrata per l’Ente. Tuttavia, i documenti ivi collegati saranno considerati regolarmente ricevuti solo se perverranno come allegati diretti al messaggio PEC o mail. Collegamenti a repository esterni non garantiscono la riferibilità, l’integrità, né la conservabilità a norma del contenuto documentale.
3. Rispondere al mittente richiedendo la trasmissione diretta degli allegati in PEC, eventualmente suddivisi in più invii numerati.
4. Segnalare eventuali anomalie al Responsabile della gestione documentale.

La presente procedura entra in vigore immediatamente e sarà oggetto di revisione in caso di aggiornamenti normativi o tecnologici.

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

Qualora siano presentati allo sportello dei documenti non richiesti o previsti dall'Ente per l'espletamento di alcuna attività procedimentale, il Servizio Protocollo, sentiti gli altri Settori o Servizi, deve restituire il documento al mittente prima della registrazione o, eventualmente, archivarlo in apposito fascicolo annuale. Nel caso in cui la registrazione sia già stata effettuata, si procede come previsto nel paragrafo 5.4.3.5 - *Annullamento delle registrazioni di protocollo*.

5.4.7 Integrazioni documentarie

I documenti giunti a Protocollo, successivamente alla registrazione del documento che devono integrare, sono registrati con un nuovo numero, indicando, nel campo *Oggetto*, "integrazione a prot. n. ... del ...".

Spetta al RPA l'inserimento nel fascicolo del procedimento e, soprattutto, la valutazione dell'ammissibilità della documentazione integrativa.

5.4.8 Documenti pervenuti per errore al Comune

Nel caso di documenti pervenuti per errore al Comune di Abano Terme, l'Ufficio Protocollo procede secondo il tipo di documento:

- nel caso di documenti analogici, i documenti in busta chiusa vanno restituiti o inviati all'Ente destinatario con la dicitura "pervenuto per errore al Comune di Abano Terme". Nel caso in cui la busta sia stata aperta, il documento registrato deve essere anche registrato in partenza compilando, in nota, la dicitura "documento pervenuto per errore" e apponendo sulla busta la dicitura "Pervenuta e aperta per errore";
- nel caso di documenti digitali pervenuti per errore alla casella di posta elettronica istituzionale o PEC del Comune, il documento deve essere rispedito al mittente con il messaggio "Documento pervenuto per errore" o "Documento non di competenza del Comune di Abano Terme".

5.4.9 Trattamento dello stesso documento inviato o consegnato a diverse UO dell'Ente o pervenuto attraverso canali diversi

Nel caso di un documento trasmesso anche attraverso diversi canali e indirizzato a diverse UO, l'addetto al Protocollo deve verificare, prima di registrarlo, che il documento non sia già stato registrato.

Nel caso di documento pervenuto in esemplare unico e destinato a diverse UO, la registrazione a sistema avviene una sola volta e il documento viene trasmesso a tutti i destinatari. Nel caso di documento digitale attraverso l'assegnazione il documento è subito disponibile alle diverse UO. Nel caso di documento analogico il documento è disponibile a tutti i destinatari nel sistema tramite acquisizione per immagine mentre l'addetto al Protocollo dovrà consultarsi con le UO coinvolte per trasmettere l'originale cartaceo al RPA. Le eventuali copie cartacee, inviate alle altre UO competenti, devono riportare la dicitura "originale cartaceo al settore ...".

Nel caso in cui, anche a seguito di verifica, il documento risulti già registrato con protocolli diversi spetta al RPA richiamare le registrazioni nello stesso fascicolo informatico. La data di inizio del procedimento amministrativo è quella della prima registrazione.

5.4.10 Documenti con pluralità di oggetti

Nel caso di documento trasmesso con pluralità di oggetti che afferiscono a procedimenti diversi, l'addetto alla registrazione deve individuare la classifica prevalente e di conseguenza smistare il documento. La ricevuta di registrazione attesta la trasmissione del documento alla UO responsabile del procedimento individuato.

La responsabilità della tenuta del documento spetta esclusivamente alla UO che ha competenza prevalente sul procedimento amministrativo, come individuato al momento della registrazione, ed è a cura del RPA aprire il fascicolo e rendere disponibile il contenuto alle altre UO coinvolte. Ogni altro procedimento innescato dal documento ricevuto produrrà documenti interni o in uscita aggregati in un fascicolo diverso da quello aperto con il documento ricevuto, che sarà invece richiamato nei documenti generati senza essere inserito nel fascicolo.

Il Comune di Abano Terme ha individuato, per molti dei suoi procedimenti, una modulistica specifica per limitare l'arrivo di documenti con molti oggetti e canali web per l'espletamento di alcune tipologie di servizi.

5.4.11 Documenti informatici contenenti macroistruzioni

Qualora il documento in entrata contenga macroistruzioni in grado di modificare il contenuto del documento, la firma digitale perde efficacia probatoria, quindi, nel caso di ricezione di questa tipologia di documenti, è opportuno richiedere l'invio di un'integrazione documentaria in formato stabile.

5.4.12 Modalità operative per lo smistamento

L'operazione di smistamento consiste nell'assegnazione di un documento alla UO competente e quindi il conferimento di responsabilità relative sia al procedimento che alla gestione e conservazione del documento stesso. Gli utenti del sistema sono tenuti al monitoraggio costante della propria postazione di lavoro e alla verifica dei documenti recapitati nelle caselle di posta convenzionale.

Gli addetti alla protocollazione, per i documenti da loro trattati, eseguono di norma la classificazione sulla base del Titolario di classificazione adottato presso l'AOO e provvedono ad

inviarli tramite il sistema documentale all'unità organizzativa di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, ritrasmette il documento all'ufficio protocollo;
- in caso di verifica positiva, esegue l'operazione di presa in carico e fascicolazione digitale;
- assegna le eventuali visibilità ulteriori rispetto a quelle attribuite automaticamente in base alla classificazione;
- gestisce il documento

Terminata la fase di protocollazione, i documenti sono portati automaticamente nella disponibilità dei soggetti competenti alla loro trattazione grazie al sistema documentale adottato dall'Ente. Il sistema consente comunque di assegnare la visibilità dei documenti ad altri soggetti singoli, uffici o gruppi trasversali di addetti configurati sul sistema. Questa modalità operativa consente di portare il documento all'attenzione di tutti i soggetti interessati, attraverso la condivisione interna del sistema documentale. Si tratta di una modalità particolarmente utile per favorire la conoscenza, e la disponibilità diffusa, di tipologie documentali quali circolari, manualistica, disposizioni operative, documenti di interesse generale ecc.

Viceversa, i documenti riservati risultano inesistenti per i soggetti ai quali non è stata assegnata, automaticamente o meno, la visibilità specifica. Si tratta di un meccanismo semplice ed affidabile per garantire la corretta gestione dei documenti riservati, contenenti dati sensibili o giudiziari, o comunque particolarmente delicati.

Nel caso di assegnazione errata, l'unità organizzativa che riceve il documento comunica l'errore all'ufficio protocollo che ha assegnato il documento, affinché proceda ad una nuova assegnazione

Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'unità organizzativa competente attraverso il sistema di gestione documentale al termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione.

I documenti ricevuti dall'amministrazione in formato cartaceo, di regola acquisiti in formato immagine o altro formato standard non modificabile con l'ausilio di scanner, una volta concluse le operazioni di registrazione segnatura e assegnazione sono fatti pervenire al Servizio di competenza per via informatica attraverso il sistema di gestione documentale. L'originale cartaceo viene anch'esso trasmesso alla struttura di competenza, mediante collocazione nell'apposita cartella presso l'Ufficio Protocollo.

L'unità organizzativa competente ha notizia dell'arrivo del documento tramite apposita "notifica" generata automaticamente dal sistema documentale.

6. IL REGISTRO DI EMERGENZA

Come prescritto all'art. 63 del DPR 445/2000, il responsabile del Protocollo autorizza allo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica.

Sul registro di emergenza devono essere riportati:

- a) numero progressivo della registrazione di emergenza, che deve garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- b) data e ora di registrazione;
- c) data e ora di arrivo della documentazione;
- d) tipologia del documento pervenuto (in arrivo, in partenza, interno);
- e) mittente e destinatario (corrispondente);
- f) oggetto;
- g) allegati;
- h) modalità di trasmissione;
- i) classificazione;
- j) eventuali note.

Qualora l'impossibilità di utilizzare la procedura informatica si protrasse oltre le ventiquattro ore per eccezionali gravità, il responsabile del Protocollo può autorizzare all'uso del registro di emergenza per periodi successivi di non più di una settimana.

Per ogni giornata di registrazione di emergenza dev'essere altresì riportato il numero totale di operazioni registrate manualmente.

Per la registrazione di emergenza si utilizza:

- a) in caso di disponibilità di PC, il modello in formato Excel allegato al presente Manuale (Allegato 7 – *Modello di registro di protocollo di emergenza*), che potrà essere implementato tramite l'immissione dei dati sulla tabella e che dovrà essere successivamente salvato;
- b) in caso di indisponibilità d'utilizzo di PC, il modello di cui al punto precedente dovrà essere stampato e compilato manualmente.

Inoltre, il responsabile del Protocollo avrà il compito di annotare in un'apposita sezione del software di protocollo informatico i periodi di attivazione del registro di emergenza.

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

Successivamente sarà compito dell'operatore di protocollo inserire nel sistema di protocollo informatico tutte le registrazioni del registro di emergenza. Ad ognuna di esse sarà attribuito un nuovo numero di protocollo, il quale costituirà la prosecuzione della numerazione di protocollo raggiunta al momento dell'interruzione del servizio.

7. DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

7.1 Descrizione funzionale e operativa

Per la descrizione operativa del sistema di protocollo informatico attualmente utilizzato dal Comune di Abano Terme si rimanda alla lettura del manuale operativo del software di protocollo informatico attualmente in uso.

7.2 Rilascio delle abilitazioni d'accesso

L'utente accede al sistema di protocollo informatico attraverso l'infrastruttura di autenticazione centralizzata del Comune.

L'accesso è subordinato all'abilitazione a cura del CED. È necessario che il controllo degli accessi sia assicurato attraverso l'assegnazione di differenti livelli di autorizzazione all'utilizzo del sistema di protocollo informatico in relazione alle diverse tipologie di ruoli ricoperti da ciascun utente.

Le richieste di abilitazione o di modificazione del livello di abilitazione, da formulare per iscritto tramite apposita procedura informatica, devono pervenire dai responsabili delle UO al Responsabile dell'Ufficio Protocollo, il quale, a sua volta, trasmetterà il contenuto di tale richiesta al CED oppure al gestore del software per l'espletamento della procedura.

All'interno dell'Amministrazione, la visibilità completa del registro di protocollo e dei flussi documentali in partenza, in arrivo e interni è permessa solamente a:

- a) Sindaco;
- b) Capo Gabinetto;
- c) Segretario comunale;
- d) Ufficio protocollo;
- e) Responsabili delle UO (PO/EQ).

Il profilo di ciascun utente è generato mediante la personalizzazione dei modelli predefiniti quindi seguito elencati:

- a) **protetto**: non si possiede nessun diritto, i dati non possono essere visualizzati e le funzionalità non possono essere eseguite;
- b) **sola lettura**: è concessa la visualizzazione e la lettura delle informazioni, ma non è possibile modificarne il contenuto;
- c) **lettura e scrittura**: è possibile sia la visualizzazione, sia la modifica dei dati ma non è consentita la cancellazione;
- d) **tutti i diritti**: sono concessi tutti i privilegi, ovvero sia visualizzazione, modifica ed eliminazione dei dati;
- e) nel caso in cui si voglia che il nuovo profilo goda dei diritti di Amministratore di protocollo, è necessario aggiungere una spunta al campo *Amministratore*. Infine, per confermare il nuovo profilo, bisogna scegliere l'opzione *Applica le modifiche* e digitare il nome che si desidera attribuire al nuovo profilo creato.

Inoltre, il CED dovrà periodicamente verificare la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione per l'intera AOO.

Il sistema di protocollo informatico in uso²⁶:

- a) assicura l'univoca identificazione e autenticazione degli utenti;
- b) protegge le informazioni di ciascun utente nei confronti degli altri;
- c) garantisce l'accesso alle risorse solamente agli utenti abilitati;
- d) garantire la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- e) assicura la corretta registrazione a protocollo dei documenti in entrata e in uscita;
- f) fornisce informazioni sul collegamento esistente tra ogni documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine di adottare il provvedimento finale;
- g) consente di reperire le informazioni riguardanti i documenti registrati;
- h) garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione e dell'archivio adottato;
- i) organizza e gestisce l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'art. 40-ter del CAD;
- j) consente il tracciamento di qualsiasi evento di modifica delle informazioni, associandolo all'autore;
- k) rispetta le misure di sicurezza in materia di protezione dei dati personali.

Durante lo svolgimento delle proprie mansioni all'interno del sistema, gli utenti interni hanno l'obbligo di riservatezza relativamente alla comunicazione e/o divulgazione di qualsivoglia dato sensibile e/o personale.

²⁶ Secondo quanto disposto dall'art. 52 del DPR 445/2000 e dagli art. 44, commi 1 e 1-bis, del CAD.

8. GESTIONE DEI DOCUMENTI

8.1 Archivio corrente

Il capitolo che riguarda la gestione dei documenti descrive le modalità di formazione, consultazione e movimentazione dei documenti e delle aggregazioni di documenti (fascicoli). La descrizione fa riferimento al contesto attuale di produzione documentale in presenza di un archivio ibrido, composto da documenti originali analogici e documenti originali digitali, sottolineando altresì le peculiarità della formazione, consultazione e movimentazione dei documenti di entrambe le tipologie e determinando l'uso degli strumenti di gestione dei flussi documentali, quali il sistema di classificazione, le modalità di fascicolazione e la repertoriatura.

8.1.1 Sistema di classificazione

La classificazione dei documenti serve a realizzare una corretta organizzazione degli atti nell'archivio ed è prevista dall'ordinamento vigente come una delle operazioni necessarie e sufficienti per la tenuta del sistema di gestione documentale al pari delle operazioni di registrazione e segnatura di protocollo.²⁷ L'operazione di classificazione avviene, quindi, attraverso il sistema del protocollo informatico e contestualmente alle due operazioni correlate. Il Comune di Abano Terme ha adottato il *Piano di classificazione per gli archivi dei comuni italiani* (seconda edizione – dicembre 2005) elaborato dal Gruppo di lavoro per la formulazione di proposte e modelli per l'organizzazione dell'archivio dei Comuni, che è riportato nel presente Manuale all'*Allegato 8 – Piano di classificazione*. Tale strumento è integrato al sistema di protocollo informatico in uso. Al Piano di classificazione è collegato il Prontuario di classificazione, organizzato in ordine alfabetico e a sua volta allegato al presente Manuale (*Allegato 9 – Prontuario per la classificazione*). Al Piano di classificazione è integrato, inoltre, il *Piano di conservazione* di cui si tratterà più diffusamente nel capitolo successivo.

Il *Piano di classificazione* può essere aggiornato su proposta del Responsabile della gestione documentale in considerazione degli adeguamenti normativi e nei termini di condivisione degli strumenti che permettano l'interoperabilità dei sistemi. Le eventuali modifiche e aggiornamenti entreranno in vigore dal 1° gennaio dell'anno successivo alla loro approvazione.

Al termine dell'operazione di classificazione, al documento informatico viene associata la segnatura di protocollo. Qualora il documento fosse analogico, la segnatura di protocollo sarà apposta applicando una etichetta autoadesiva al supporto.

Nel caso di documento ricevuto dal Comune di Abano Terme, viene, infine, assegnato al RPA per la fascicolazione e l'espletamento dell'azione amministrativa. Il sistema di protocollo, integrato con i canali di comunicazione ufficiali dell'Ente, genera una ricevuta che viene inviata al mittente del documento in cui sono indicati la segnatura del documento, la data e la UO competente.

Nel Comune di Abano Terme ogni UO assegnataria del documento è abilitata alla fascicolazione secondo due modalità:

- se il documento si ricollega ad un fascicolo aperto, il soggetto preposto seleziona il fascicolo relativo attraverso le funzioni di ricerca del sistema di protocollo e collega la registrazione di protocollo del documento al fascicolo selezionato;

²⁷ Artt. 50 e 56 del DPR 445/2000.

- se il documento non è collegabile ad alcun fascicolo aperto il soggetto preposto crea un nuovo fascicolo e collega la registrazione di protocollo del documento al fascicolo selezionato.

8.1.2 Fascicolazione

I documenti registrati e classificati con il programma di protocollo informatico sono inseriti nei fascicoli informatici²⁸ e in altre aggregazioni documentali informatiche²⁹ attraverso l'apposita funzione del sistema. I fascicoli creati nel sistema rimandano a tutti i documenti loro assegnati e sedimentati in ordine cronologico e sono visualizzati a partire dal più recente.

Al momento dell'apertura di ogni fascicolo il sistema di protocollo informatico aggiorna automaticamente il repertorio dei fascicoli che contiene i dati identificativi di ogni fascicolo:

- anno;
- indice di classificazione (composto da titolo e classe);
- numero del fascicolo o numero di repertorio (numero sequenziale generato all'interno dell'ultimo grado divisionale del titolare);
- oggetto del fascicolo;
- data di apertura del fascicolo;
- AOO e UO;
- nominativo del responsabile;
- elenco dei documenti contenuti;
- data di chiusura del fascicolo.

Il fascicolo può presentarsi suddiviso in sottofascicoli, qualora fosse necessario per esigenze pratiche. I sottofascicoli presentano dei dati identificativi simili a quelli del fascicolo e sono gestiti dal sistema di protocollo informatico in modo automatico attraverso la generazione di una numerazione che ha progressione cronologica.

Come previsto dalle *Linee guida*³⁰, per l'organizzazione dei fascicoli integrata con il Piano di conservazione il Comune di Abano Terme adotta come Piano di organizzazione delle aggregazioni documentali³¹ lo strumento delle *Linee guida per l'organizzazione dei fascicoli e delle serie* proposto dal Gruppo di lavoro per gli archivi dei Comuni (*Allegato 11*).

Dal punto di vista logico, la creazione dei fascicoli rispetta le necessità di creazione di aggregazioni di documenti secondo le seguenti tipologie:

- **fascicolo per persona fisica/giuridica**: si tratta di una aggregazione di documenti per la quale l'elemento unificante è il soggetto di cui vengono raccolti i documenti. Il soggetto è identificato secondo una chiave univoca quale il numero di matricola, il codice fiscale, la partita IVA, il numero di registrazione;
- **fascicolo per affare/procedimento**: aggregazione di documenti che fanno riferimento ad un singolo procedimento amministrativo;
- **fascicolo per attività**: aggregazione di documenti uguali per tipologia e riferiti ad attività

²⁸ Art. 41, comma 2, del CAD.

²⁹ Par. 3.3 delle *Linee guida*.

³⁰ Par. 3.1.3

³¹ Definito all'allegato 1 delle *Linee guida*. - *Glossario*

limitatamente complesse, raccolti secondo un ordine cronologico nell'arco dell'anno solare.

La chiusura del fascicolo è determinata dal responsabile del fascicolo stesso al concludersi di ogni specifica attività e quindi dipendente dalla tipologia di fascicolo, secondo i criteri appena descritti. La data di chiusura del fascicolo corrisponde alla data dell'ultimo documento prodotto e il fascicolo resta ordinato in funzione del suo numero di repertorio (generato al momento dell'apertura). L'attività conclusiva in capo al RPA consiste nello sfoltimento del fascicolo analogico da tutto il materiale non documentario utile al procedimento ma non destinato alla conservazione (fotocopie, normativa, appunti e quant'altro).

Il fascicolo informatico, che si costituisce come aggregazione logica all'interno del sistema di protocollo, può essere composto anche da documenti analogici che saranno sedimentati in ordine cronologico all'interno di una camicia di carta rigida che riporta gli stessi dati prescritti per il fascicolo informatico.

I dati che identificano il fascicolo si riportano secondo la struttura che segue:

- l'anno va separato dalla classificazione con un trattino (-);
- i gradi divisionali della classificazione (titolo e classe) vanno separati da una barra (/) indicando prima il titolo con numeri romani e di seguito la classe con numeri arabi;
- il numero progressivo del fascicolo che segue la classificazione è separato da un punto;
- l'oggetto chiude la segnatura archivistica ed è scritto tra virgolette caporali (« »).

Es.: 0000 – I/1.1 «Abcdefgh»

8.1.3 Documenti repertoriati

In ottemperanza alla normativa vigente³², i documenti informatici prodotti o ricevuti dal Comune sono registrati nel sistema di Protocollo generale o in uno dei repertori previsti.

La repertoriazione avviene attraverso specifiche funzioni previste dal sistema di Protocollo nel rispetto delle norme generali in materia di conservazione. Tali aggregazioni documentali costituiscono serie archivistiche.

L'elenco dei documenti esclusi dalla registrazione nel sistema di Protocollo generale e per i quali è prevista una forma di registrazione particolare sono riportati negli allegati 3 e 5.

³² Art. 53 del DPR 445/2000.

8.2 Archivio di deposito

Questa sezione del Manuale riguarda esclusivamente la gestione della documentazione cartacea.

8.2.1 Gli archivi di deposito delle UO

I fascicoli conclusi sono gestiti dalle rispettive UO fino al versamento in Archivio comunale. I fascicoli conservati presso gli uffici sono conservati negli armadi esistenti e nei vani d'archivio preposti in maniera ordinata e le Unità si occupano di redigere e aggiornare elenchi di consistenza oltre che di registrare il prelievo e la movimentazione dei fascicoli. Le UO, inoltre, si occupano di condizionare i fascicoli in una busta idonea alla conservazione, sul dorso della quale si deve indicare l'UO, la classificazione e gli estremi cronologici della documentazione contenuta. Infine, il dorso può riportare un codice di identificazione univoco per collegare il contenuto descritto negli elenchi di consistenza all'unità di condizionamento.

8.2.2 Il versamento

Periodicamente, o comunque a cadenza annuale, dev'essere effettuato il versamento dei fascicoli relativi ad affari e procedimenti amministrativi conclusi in Archivio comunale. Tale attività può essere svolta da personale appositamente delegato dal Responsabile della gestione documentale o da una ditta esterna che offre questa tipologia di servizi.

Al momento del versamento deve essere predisposto un apposito elenco di versamento, così come proposto all'*Allegato 12*.

Il versamento all'Archivio comunale comporta il passaggio di responsabilità dalla UO competente al Responsabile dell'Archivio, sotto la supervisione del Responsabile della gestione documentale.

8.2.3 Movimentazione e prelievo dei fascicoli

Una volta che i fascicoli sono stati versati in Archivio comunale, possono essere prelevati dal personale espressamente incaricato dal Responsabile della gestione documentale. La consultazione e il prelievo avvengono solo a seguito di richiesta scritta e sono annotati dal personale all'interno di un registro informatico compilato sul modello predisposto (*Allegato 13*). Inoltre, il prelievo dei singoli pezzi è segnalato con la collocazione di un cedolino di prelievo al posto del pezzo prelevato. Il personale deputato a compiere tale attività su espressa disposizione del Responsabile della gestione documentale verifica periodicamente lo stato dell'archivio di deposito e può richiedere alle UO la restituzione dei pezzi in consultazione.

8.2.4 Selezione e scarto

In fase d'archivio di deposito avvengono, con cadenza periodica, le attività di selezione e scarto della documentazione. Tale attività è organizzata dal Responsabile della gestione documentale, che

la pianifica e la svolge in accordo con le rispettive UO, anche affidando il servizio ad una ditta esterna.

La selezione degli atti da proporre allo scarto avviene per il materiale che il Comune ritiene che non sia più opportuno conservare, perché privo di rilevanza amministrativa e di rilevanza storica e l'attività si svolge assicurando i requisiti legali dei tempi di prescrizione della documentazione e senza pregiudicare le esigenze presenti e future degli utenti per perseguire il fine del pubblico interesse.

Per svolgere queste operazioni, l'Ente si serve del Piano di conservazione adottato, il quale integra il Piano di classificazione individuando per ogni titolo e classe le aggregazioni documentali previste e i termini decorsi i quali si può prevedere lo scarto.

Il Piano di conservazione è quello prodotto dal Gruppo di lavoro e costituisce l'*Allegato 10*.

La selezione si svolge elaborando un elenco secondo il modello proposto dalla Soprintendenza archivistica e bibliografica per il Veneto e il Trentino Alto Adige (*Allegato 14*). L'elenco deve essere approvato con un provvedimento dell'Ente, secondo diversi casi:

- deliberazione di Giunta per lo scarto che riguarda diversi settori del Comune;
- determinazione del Responsabile della gestione documentale, sentito il parere dell'UO competente per lo scarto che riguarda il settore di riferimento;
- determinazione del dirigente dell'UO competente per lo scarto di documenti che non sono ancora stati versati in archivio.

Il provvedimento adottato dal Comune di Abano Terme con relativo elenco deve essere inviato alla Soprintendenza archivistica competente per la necessaria autorizzazione.

I fascicoli e i documenti per i quali è autorizzata la procedura di scarto sono destinati all'eliminazione fisica, individuando modalità di distruzione che garantiscano dalla diffusione illecita della documentazione, attraverso incenerimento, triturazione o macerazione della carta con particolare riferimento agli atti riservati e a quelli che contengono dati sensibili, in accordo alla vigente normativa e secondo raccomandazioni della competente Soprintendenza archivistica.

Infine, il verbale di consegna del materiale cartaceo e la certificazione delle operazioni sopra descritte devono essere conservati e inoltre comunicati alla Soprintendenza archivistica competente per territorio.

9. CONSERVAZIONE DEI DOCUMENTI

9.1. Conservazione dei documenti analogici

Il Comune di Abano Terme conserva i propri documenti analogici negli archivi di deposito presenti presso le UO e presso i depositi dell'Archivio comunale di via dei Colli, via Stella e via Levante Ferrovia e i documenti sono conservati in modo permanente o per il periodo determinato dal Piano di conservazione in uso.

Compete al Responsabile della gestione documentale, dunque, il monitoraggio sul versamento della documentazione analogica selezionata per la conservazione permanente nella sezione separata d'archivio (archivio storico) quando gli affari sono conclusi da oltre un quarantennio. Parimenti, il Responsabile della gestione documentale si occupa di garantire la sicurezza e la conservazione nel tempo degli archivi nella loro organicità e nel loro ordine e provvede a definire gli strumenti per la consultazione dell'archivio e per promuoverne la valorizzazione anche affidando il servizio a ditte esterne.

Tutte le attività descritte si svolgono in ottemperanza al presente Manuale e secondo quanto stabilito dal *Codice dei beni culturali e del paesaggio*.

9.2. Conservazione dei documenti digitali

Secondo quanto disposto dal par. 4.6 delle *Linee guida*, il Comune di Abano Terme predispone questa sezione come Manuale di conservazione in quanto volta a descrivere i ruoli e le responsabilità della conservazione digitale, gli oggetti conservati e le modalità operative della conservazione rimettendo al Manuale di conservazione del Conservatore per le specifiche tecniche. Il Comune di Abano Terme ha incaricato quale fornitore del servizio di conservazione, Unimatica, individuato tra i conservatori accreditati come previsto dalla normativa vigente. In tale contesto di transizione il Responsabile della Conservazione del Comune di Abano Terme fa riferimento al *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* e verifica il possesso ed eventualmente l'adeguamento da parte del conservatore ai requisiti per l'erogazione del servizio alle PA (allegato A del *Regolamento*) ed elabora un Piano di cessazione del servizio di conservazione in conformità a quanto previsto dall'allegato B del *Regolamento*.

9.2.1. Ruoli e responsabilità

Sulla base di quanto disposto dalla normativa vigente, il Responsabile della conservazione è un dirigente o un funzionario formalmente incaricato e può coincidere con il Responsabile della gestione documentale.

Nel contesto organizzativo dell'Ente è stato previsto che il soggetto produttore (Comune di Abano Terme) abbia affidato la conservazione a norma e il processo di conservazione a soggetti conservatori esterni. Al Responsabile della conservazione, o comunque al Responsabile della gestione documentale, restano affidati i seguenti compiti:

- 1) monitoraggio delle attività svolte dai conservatori esterni;
- 2) delineazione delle politiche generali di conservazione dei documenti;

- 3) determinazione dei requisiti generali e di carattere archivistico del sistema di conservazione;
- 4) configurazione delle politiche di accesso ai documenti, anche attraverso canali web.

9.2.2. Oggetti conservati

Avendo il Comune di Abano Terme affidato esternamente il servizio di conservazione a norma dei propri documenti, per l'approfondimento del tema in oggetto si rimanda alla lettura della scheda cliente prodotta dal conservatore esterno allegata al presente Manuale (*Allegato 18*).

9.2.3. Procedure di conservazione e di monitoraggio effettuate dal Comune

Le procedure di conservazione effettuate dal Comune si estrinsecano in mere operazioni di copia giornaliera del server: una prima copia incrementale viene eseguita tutte le notti dal lunedì al giovedì, mentre il venerdì notte viene eseguita una copia completa; la seconda copia completa del *disaster recovery*, invece, viene eseguita il sabato notte. Tale copia popola un ulteriore server virtualee contiene sia i database sia gli applicativi.

Infine, è prodotto un report giornaliero delle attività sopra descritte e vengono effettuati costanti monitoraggi da parte del CED.

Il server attualmente presente presso la sede municipale di Piazza dei Caduti sarà spostato in altra struttura, presente sul suolo comunale, per delocalizzare la copia dei software, dei database e degli applicativi in uso e di archivio. Questo garantirà maggiore sicurezza fisica dell'infrastruttura informatica.

Inoltre, essendo i nuovi software gestionali in versione Cloud e ospitati in hostig qualificato e approvato da AGID e ANC, si elencano di seguito le caratteristiche di sicurezza offerte:

- a) CSP (cloud service provider) dal 12/12/2018
- b) SaaS (software as a service) dal 25/01/2019
- c) Certificazione Iso27001 sulla sicurezza informatica, Iso27017, Iso27018
- d) Certificazione sul sistema CLOUD : iso 20000
- e) Certificazione sul sistema di qualità : iso 9001
- f) Certificazione sulla gestione ambientale : iso 14001

10. PROCEDIMENTI AMMINISTRATIVI, ACCESSO AI DOCUMENTI E TUTELA DELLA RISERVATEZZA

Il presente capitolo riprende i regolamenti approvati dal Comune in materia di procedimento amministrativo e si rifà alla normativa vigente per descrivere i criteri e le modalità di gestione dei procedimenti amministrativi, le diverse modalità di accesso ai documenti e la tutela della riservatezza dei dati personali.

10.1 Regolamenti

Al momento della redazione ed approvazione del presente Manuale, sono in vigore nel Comune di Abano Terme i seguenti regolamenti:

- *Regolamento comunale in materia di procedimento amministrativo* (Approvato con deliberazione consiliare n. 2 del 01.02.2024);
- *Regolamento comunale per l'accesso ai documenti amministrativi* (Approvato con deliberazione del Consiglio comunale n. 63 del 18.09.2007 e modificato con deliberazione del Commissario straordinario n. 70 del 16.06.2010);
- *Regolamento comunale in materia di accesso civico ed accesso civico generalizzato* (Approvato con deliberazione del Consiglio comunale n. 2 del 25.02.2019);
- *Regolamento per il trattamento di dati sensibili e giudiziari* (Approvato con deliberazione del Commissario straordinario n. 112 del 21.12.2005 e modificato con deliberazione del Commissario Straordinario n. 89 del 03.05.2006).

10.2 Amministrazione trasparente e Albo online

Sulla base di quanto disposto dal D.Lgs del 14 marzo 2013 n. 33 - *Riordino della disciplina riguardante gli obblighi di pubblicazione, trasparenza e diffusione delle informazioni da parte della pubblica amministrazione*, il Comune di Abano Terme ha allestito, nell'ambito del proprio sito istituzionale, una sezione denominata *Amministrazione trasparente* tramite la quale sono comunicati e diffusi dati, informazioni e documenti la cui conoscibilità non è limitata da alcun vincolo di riservatezza e riguardano l'organizzazione dell'Ente e le sue attività.

Nelle sottosezioni della pagina sono disponibili disposizioni di carattere generale, informazioni sull'organizzazione e su enti controllati dal Comune, disposizioni riguardanti gli incarichi al personale, così come a consulenti e incarichi esterni; documentazione sulla contabilità e sul patrimonio, informazioni sulla gestione del territorio; controllo e valutazione della performance e infine informazioni sulle diverse tipologie di procedimento e la relativa modulistica.

In applicazione della normativa che prevede gli obblighi di pubblicità relativi all'azione amministrativa e secondo i regolamenti citati che prevedono l'affissione all'albo comunale e in altri mezzi idonei di comunicazione, il Comune ha attivato un portale denominato *Albo pretorio online*, strumento con il quale la Pubblica amministrazione può rendere pubblici provvedimenti e bandi e comunicare con i cittadini e le imprese.

10.3 Tutela della trasparenza e accesso ai documenti

Secondo la normativa vigente e tenendo in considerazione i regolamenti adottati, i documenti e i provvedimenti acquisiti o formati dal Comune di Abano Terme sono accessibili attraverso diverse modalità. Lo Statuto del Comune promuove il diritto-dovere dei cittadini alla partecipazione, individuale o in forma associata, e alla partecipazione dei cittadini ai procedimenti amministrativi³³. Inoltre, il diritto all'accesso civico e all'accesso civico generalizzato sono riconosciuti e organizzati secondo il *Regolamento comunale in materia di accesso civico ed accesso civico generalizzato* «allo scopo di favorire forme diffuse di controllo del perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche nonché di promuovere la partecipazione al dibattito pubblico»³⁴.

10.3.1 Accesso ai documenti amministrativi

È garantito il diritto di accesso alla documentazione del Comune di Abano Terme, secondo le modalità descritte nel *Regolamento comunale per l'accesso ai documenti amministrativi*, a tutti i soggetti che abbiano interesse per la tutela di situazioni giuridicamente rilevanti. L'istanza di accesso deve essere indirizzata al settore competente e il responsabile individuato è colui che è preposto all'unità operativa. Il modulo per la compilazione dell'istanza è liberamente scaricabile dal sito istituzionale. Il diritto d'accesso non è consentito per i documenti riservati e spetta al RPA differire o limitare l'accesso oltre ad adottare le opportune misure per la tutela della riservatezza dei dati.

10.3.2 Accesso civico e accesso civico generalizzato

I criteri e le modalità organizzative per l'esercizio del diritto di accesso civico e accesso civico generalizzato sono definiti dal sopra citato regolamento. Nel dettaglio, l'accesso civico è da intendersi come il «diritto di chiunque di richiedere documenti, informazioni e dati oggetto di obblighi di pubblicazione»³⁵, mentre l'accesso civico generalizzato consiste nel diritto di «accedere a dati e documenti detenuti dall'Autorità, ulteriori rispetto a quelli sottoposti ad obbligo di pubblicazione»³⁶. A tal fine, il Comune di Abano Terme ha istituito il registro delle richieste di accesso, organizzato in due sezioni per le differenti tipologie di accesso, gestito come banca dati digitale e aggiornato dall'ufficio Affari generali. Il registro è reso pubblico nell'apposita sezione del sito istituzionale. Il regolamento descrive eventuali limiti, eccezioni e limitazioni nell'esercizio dei diritti.

³³ Statuto, art. 11.

³⁴ Art. 1, comma 2.

³⁵ Art. 2.

³⁶ Ivi

10.3.3 Accesso ai documenti per fini di ricerca storico-scientifica

Tutta la documentazione del Comune di Abano Terme è liberamente consultabile, come stabilito dal *Codice dei beni culturali e del paesaggio*, nei termini individuati dalle *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica* che recepiscono le modifiche alla normativa precedente introdotte dal Regolamento (UE) 2016/679 del Parlamento europeo.

Dunque, fanno eccezione:

- i documenti a carattere riservato che contengono dati relativi alla politica interna ed estera dello Stato, consultabili dopo 50 anni dalla chiusura del fascicolo che li contiene;
- i documenti contenenti dati particolari, consultabili dopo 40 anni dalla chiusura del fascicolo che li contiene;
- i documenti contenenti una specifica categoria di dati particolari che rivelano informazioni sulla salute, la o la vita sessuale o i rapporti riservati di tipo familiare, consultabili dopo 70 anni dalla chiusura del fascicolo che li contiene.

I documenti per i quali sono individuate le eccezioni di cui sopra possono comunque essere consultati prima della scadenza dei termini previa autorizzazione del Ministro dell'Interno secondo le modalità definite dalla normativa vigente.

11. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione aggiornamento del Manuale

Il presente Manuale è approvato dalla Giunta comunale con propria deliberazione ed è aggiornato, su proposta del Responsabile della gestione documentale o della ditta incaricata, 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;
- introduzioni di nuovi software o innovazioni tecnologiche o informatiche;
- inadeguatezza delle procedure individuate 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 della gestione documentale, una volta acquisiti i pareri del capo del settore Servizi amministrativi e del CED.

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 approvato con deliberazione di Giunta Comunale n°172 del 24.11.2020.

11.2. Pubblicità del presente Manuale

In ottemperanza a quanto disposto dal paragrafo 3.5 delle *Linee guida* per quanto concerne il Manuale di gestione e al paragrafo 4.6 per quanto concerne il Manuale di conservazione, il presente documento è reso pubblico dal Comune di Abano Terme mediante la pubblicazione sul proprio sito istituzionale.

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