



**Manuale di gestione
documentale
del
Comune di Reggio Calabria**

Indice generale

Sommario

Premessa	5
1. Aspetti organizzativi	7
1.1. Indice dei domicili digitali e codice IPA.....	7
1.2. L’Ufficio Protocollo: ruolo e compiti	8
1.3. Ruolo e compiti dei Responsabili	9
2. Richiami normativi.....	13
3. Il documento	14
3.1. Il documento: definizioni.....	14
3.2. Firme elettroniche, certificati di firma e validazione temporale	15
3.3. Sottoscrizione e verifica della firma	17
3.4. Copie e attestazioni di conformità	19
3.5. Redazione e formazione del documento informatico	20
3.6. I formati dei documenti	21
4. La protocollazione.....	23
4.1 Premessa	23
4.2. Il sistema di protocollo informatico: Auriga.....	23
5. La classificazione	24
6. L’organigramma	24
7. Casi d’uso e comportamenti	25
7.1. Gestione della PEC (protocollo@pec.reggiocal.it) e indicazioni per la compilazione dell’oggetto e del corrispondente	25
7.2. Gestione delle altre caselle PEC istituzionali.....	25
7.3. Gestione della PEO istituzionale.....	26
7.4. Le fatture passive dal Sistema di interscambio – SdI	26
7.5. Registro accesso civico	27
7.6. Determine, delibere di Giunta e di Consiglio, ordinanze.....	27
7.7. Altri atti soggetti alla pubblicazione in Albo Pretorio.....	28
8. La gestione dell’archivio del Comune di Reggio Calabria	29
8.1. Archivio corrente: definizione e prassi	29
8.2. Archivio di deposito: definizione e prassi	30

8.3.	Archivio storico: definizione e prassi di consultazione	31
9.	Misure di sicurezza e di protezione dei dati personali.....	32
9.1.	La tutela dei dati personali	32
9.2.	Sicurezza dei sistemi informatici del Comune di Reggio Calabria: misure e istruzioni	34
10.	Elenco degli allegati.....	36

Premessa

Il Comune di Reggio Calabria, in quanto pubblica amministrazione¹, è tenuto a redigere, nonché ad adottare con provvedimento formale e pubblicare sul proprio sito istituzionale (nell'area Amministrazione trasparente²), il manuale di gestione documentale. Il manuale è compilato conformemente alle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*³ a cura del Responsabile della gestione documentale, e assolve l'obbligo normativo. Esso «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 archivi»⁴, riportando, in particolare, gli aspetti organizzativi, i formati dei documenti, le informazioni relative al protocollo informatico, alle registrazioni particolari, alla classificazione, alla formazione delle aggregazioni documentali, ai flussi di lavoro, all'organizzazione dei documenti stessi, alle misure di sicurezza informatica e protezione dati personali (in conformità con le disposizioni vigenti) e alla conservazione. Nel rispetto delle Linee Guida, quindi, il manuale rimanda anche al piano per la sicurezza informatica per la parte di competenza, fornisce il piano di classificazione e le indicazioni in materia di continuità operativa.

1 Cfr. D. lgs. 7 marzo 2005, n. 82 o *Codice dell'amministrazione digitale*, d'ora in poi CAD.

2 Cfr. D. lgs. 14 marzo 2013, n. 33 o *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*, art. 9.

3 Le *Linee Guida* sono state adottate da AgID con la determinazione n. 407/2020, ma entrate effettivamente in vigore dal 1° gennaio 2022, d'ora in poi LLGG o Linee Guida.

4 Cfr. LLGG, 3.5.

Il manuale si rivolge ai dipendenti del Comune di Reggio Calabria, poiché descrive l'organizzazione dell'ente, fornendo delle istruzioni operative e definendo le corrette procedure di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti. Esso, tuttavia, inserito nella sezione Amministrazione trasparente del sito istituzionale, è anche un documento pubblico ed esterno rivolto al cittadino, redatto affinché possa comprendere la gestione documentale dell'ente. Il documento è oggetto di aggiornamento e formazione continua.

Il manuale, su proposta del Responsabile della gestione documentale, è approvato con provvedimento della Giunta comunale, che vaglia e approva pure gli eventuali aggiornamenti sostanziali (come una modifica al piano di classificazione o al piano di conservazione). Al contrario, gli aggiornamenti sugli allegati possono essere approvati con determina del dirigente del Settore competente per materia.

1. Aspetti organizzativi

Il Comune di Reggio Calabria è costituito da un'unica Area Organizzativa Omogenea (d'ora in poi AOO)⁵, identificata come "Protocollo Generale". All'AOO citata è associato un unico servizio per la tenuta del protocollo informatico, e un solo registro di protocollo. La AOO è costituita dai Settori (U.O.R. Unità Organizzativa Responsabile) soggetti a modifiche e integrazioni sulla base delle riorganizzazioni amministrative, e sono individuate in riferimento all'organigramma e al funzionigramma del Comune di Reggio Calabria. Ad ognuna sono attribuite funzioni e competenze specifiche: vi si trattano attività e procedimenti amministrativi peculiari. Per la struttura dell'ente, si rimanda all'Allegato 1.

1.1. Indice dei domicili digitali e codice IPA

AOO e Settori sono definite e accreditate nell'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi (d'ora in poi IPA). L'indice raccoglie gli indirizzi telematici e il domicilio digitale del Comune di Reggio Calabria, oltre che i codici univoci per Settore, ed è necessario comunicare tempestivamente i nuovi dati, in caso di modifiche. Il codice IPA del Comune è "c_h224".

5 Cfr. DPR 28 dicembre 2000, n. 445 o *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*, d'ora in poi TUDA, art. 50, c. 4.

Cfr. Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi – IPA, Comune di Reggio Calabria, <https://indicepa.gov.it/ipa-portale/consultazione/indirizzo-sede/ricerca-ente/scheda-ente/9011/elenco-aree-organizzative-omogenee>

1.2. L'Ufficio Protocollo: ruolo e compiti

Nell'AOO è istituito l'Ufficio Protocollo, incaricato della tenuta del protocollo informatico e della gestione dei flussi documentali e dell'archivio corrente, affidato alla guida del Responsabile della gestione documentale. L'Ufficio svolge i compiti previsti dalla norma⁶:

- in collaborazione con i tecnici informatici, attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura (abilitazioni per consultare o modificare le informazioni);
- garantisce che le operazioni di registrazione e segnatura del protocollo siano effettuate nel rispetto delle disposizioni vigenti;
- garantisce la produzione e la corretta conservazione del registro giornaliero di protocollo;
- in collaborazione con i tecnici informatici, cura le funzionalità del sistema, ripristinandole nel più breve tempo possibile in caso di guasti e anomalie;
- garantisce il buon funzionamento degli strumenti e delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
- autorizza le operazioni di annullamento delle registrazioni di protocollo;
- attiva, se necessario, il registro di emergenza;
- collabora per adeguare il sistema di gestione documentale all'organigramma dell'ente, in base alle riorganizzazioni amministrative;

⁶ Cfr. TUDA, art. 61, *Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi*.

- aggiorna regolarmente il manuale di gestione documentale;
- vigila sull'osservanza delle disposizioni del TUDA, del CAD e delle Linee Guida del personale incaricato.

1.3. Ruolo e compiti dei Responsabili

Il **Responsabile della gestione documentale** è individuato dall'art. 61 del TUDA: è un funzionario in possesso di adeguati requisiti professionali e conoscenze tecnico-archivistiche, informatiche e giuridiche. Questi collabora con il Responsabile per la transizione digitale e il Responsabile della protezione dei dati personali, ed è incaricato con formale atto di nomina. Il Responsabile della gestione documentale:

- redige e aggiorna regolarmente il manuale di gestione documentale, provvedendo alla massima diffusione dello stesso;
- vigila sulla corretta tenuta del protocollo informatico;
- garantisce il rispetto delle disposizioni normative vigenti in materia di gestione documentale;
- definisce criteri uniformi di trattamento dei documenti, di classificazione e archiviazione, validi per tutte le UOR, monitorando le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
- produce il pacchetto di versamento, contenente i documenti destinati alla conservazione;
- verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli o diversi dal protocollo informatico previsto dal TUDA⁷.

⁷ Cfr. Linee Guida, cap. 3.4, *Compiti del responsabile della gestione documentale*.

Il **Responsabile della conservazione**⁸ effettua la conservazione dei documenti conformemente alle disposizioni vigenti, garantendone l'integrità. Nella Pubblica Amministrazione, è un ruolo previsto nell'organigramma, funzionario con idonee competenze giuridiche, informatiche e archivistiche, incarico che può essere svolto anche dal Responsabile della gestione documentale (o dal coordinatore della gestione documentale, ove nominato). Questi:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e agli standard internazionali, analizzando gli oggetti digitali da conservare, l'attività dell'ente e le caratteristiche del sistema di gestione documentale;
- gestisce il processo di conservazione;
- redige e sottoscrive il rapporto di versamento, come previsto dal manuale di conservazione;
- genera e sottoscrive con firma digitale il pacchetto di distribuzione;
- effettua la verifica periodica della leggibilità e dell'integrità dei documenti informatici e delle aggregazioni documentarie;
- rileva con tempestività il degrado dei sistemi di memorizzazione e delle registrazioni, nonché l'obsolescenza dei formati;
- in relazione all'evolversi della tecnologia, provvede alla duplicazione dei documenti informatici;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura la presenza di un pubblico ufficiale, ove richiesto;
- assicura assistenza e risorse agli organismi competenti che

⁸ Cfr. CAD, art. 44, *Requisiti per la gestione e conservazione dei documenti informatici* comma 1-quater e LLGG, cap. 4.6, *Manuale della conservazione*.

espletino attività di verifica e vigilanza;

- versa i documenti informatici, le aggregazioni informatiche e gli archivi informatici all'Archivio di Stato competente;
- redige e aggiorna periodicamente il manuale di conservazione.

Il Responsabile della transizione al digitale dirige l'ufficio che si occupa di transizione alla modalità operativa digitale e riorganizzazione dei processi, tali da creare un'amministrazione digitale e aperta, con servizi facili da utilizzare e di qualità⁹. Egli:

- coordina strategicamente lo sviluppo dei sistemi informativi, di telecomunicazione e telefonia, conformemente agli standard tecnici e organizzativi comuni;
- coordina lo sviluppo dei servizi;
- indirizza, pianifica, coordina e monitora la sicurezza informatica dei dati, dei sistemi e della infrastrutture, in relazione al sistema pubblico di connettività;
- promuove l'accessibilità dello strumento informatico;
- analizza periodicamente il rapporto dell'organizzazione con le tecnologie, per migliorare i servizi;
- coopera per la revisione delle riorganizzazione amministrativa, sempre in ottica di transazione al digitale;
- progetta iniziative per un'erogazione efficace di servizi in rete a cittadini e imprese;
- pianifica e coordina all'interno dell'amministrazione, in

⁹ Cfr. CAD, art. 17, *Responsabile per la transizione digitale e difensore civico digitale*.

collaborazione con il Responsabile della gestione documentale, la diffusione dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale.

- coordina l'acquisto di sistema informatici e soluzioni che garantiscano la compatibilità con gli obiettivi dell'Agenda Digitale.

Il **Responsabile per la protezione dei dati personali**¹⁰ è a sua volta contraddistinto da specifiche qualità professionali (quali una conoscenza profonda della normativa in materia di protezione dei dati); può essere un dipendente dell'Ente, oppure assolvere i suoi compiti in base a un contratto di servizi, come nel caso del Comune di Reggio Calabria. Egli:

- è consulente per il titolare del trattamento (o il responsabile del trattamento, o i dipendenti) in merito al regolamento GDPR, o altre disposizioni in materia di protezione dei dati;
- sorveglia l'osservanza del GDPR, o di altre disposizioni UE, e delle politiche del titolare del trattamento (o del responsabile del trattamento) in materia di protezione dei dati personali;
- avanza un parere in merito alla valutazione di impatto sulla protezione dei dati;
- coopera con l'autorità di controllo, fungendo da punto di contatto per ciò che è connesso al trattamento.

¹⁰ Cfr. GDPR, art. 37 e art. 39.

2. Richiami normativi

Il manuale di gestione si compone di richiami a fonti normative. Nello specifico, si rimanda a:

1. Codice dell'Amministrazione Digitale (CAD) – Decreto legislativo del 7 marzo 2005, n. 82.
2. Linee Guida sulla formazione, gestione e conservazione dei documenti informatici e rispettivi n. 6 allegati tecnici (allegato 1: Glossario di termini e degli acronimi; allegato 2: Formati di file e riversamenti; allegato 3: Certificazione di processo; allegato 4: Standard e specifiche tecniche; allegato 5: Metadati; allegato 6: Comunicazione tra AOO di documenti amministrativi), in vigore dal 1° gennaio 2022.
3. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA) – Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445.
4. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi – Legge del 7 agosto 1990, n. 241.
5. Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni – Decreto legislativo del 14 marzo 2013, n. 33.
6. Regolamento eIDAS (*electronic Identification Authentication and Signature*) – Regolamento UE n. 910/2014.
7. Regolamento generale sulla protezione dei dati (GDPR) – Regolamento UE n. 679/2016.

3. Il documento

Durante l'attività istituzionale, gli uffici del Comune di Reggio Calabria producono e acquisiscono documenti. Come pubblica amministrazione, il Comune forma gli originali dei documenti (anche quelli inerenti albi, elenchi e pubblici registri) con mezzi informatici, secondo le disposizioni del CAD e delle Linee Guida¹¹.

3.1. Il documento: definizioni

Il **documento informatico** è una «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»; esso si contrappone al **documento analogico**, ch'è una «rappresentazione *non* informatica di atti, fatti o dati giuridicamente rilevanti»¹². Quest'ultimo, in via di semplificazione, è un documento cartaceo, scritto manualmente, o redatto con un *text editor*, stampato ed eventualmente sottoscritto. Per completezza di terminologia, il documento analogico può essere distinto in documento originale unico, o in **documento originale non unico**, ovvero un documento per il quale sia possibile risalire al suo contenuto attraverso altre scritture, o documenti per cui è obbligatoria la conservazione (anche se in possesso di terzi)¹³.

Il **documento amministrativo** è «ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni, o comunque utilizzati ai fini dell'attività amministrativa»¹⁴; ne deriva che un **documento amministrativo**

11 Cfr. CAD, art. 40, *Formazione di documenti informatici*.

12 Cfr. CAD, art. 1, *Definizioni*.

13 *Ibidem*.

14 Cfr. TUDA, Capo 1, art. 1, *Definizioni*.

informatico è un atto formato da una PA (o dati e documenti detenuti da essa) con strumenti informatici¹⁵.

3.2. Firme elettroniche, certificati di firma e validazione temporale

La validità e l'efficacia probatoria del documento informatico sono strettamente connesse alla firma elettronica.

Esso, infatti, «soddisfa il requisito della forma scritta (e ha l'efficacia prevista dall'articolo n. 2702 del Codice Civile) quando vi è apposta una firma digitale, o altri tipo di firma elettronica qualificata o firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore»¹⁶.

Per quanto concerne le firme elettroniche, si fa riferimento al Regolamento UE n. 910/2014, o Regolamento eIDAS. In particolare, si definisce:

- **firma elettronica:** dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare¹⁷; al documento informatico firmato è associato un valore probatorio liberamente valutabile in giudizio, sulla base delle caratteristiche di sicurezza, integrità e immodificabilità; una firma elettronica può essere effettuata anche con l'uso di credenziali di accesso (uno *user ID* e una

¹⁵ Cfr. CAD, art. 23-ter, *Documenti amministrativi informatici*.

¹⁶ Cfr. CAD, art. 20, comma 1-bis, *Validità ed efficacia probatoria dei documenti informatici*.

¹⁷ Cfr. Regolamento eIDAS, art. 3, punto 10.

password), ma il suo livello di affidabilità sarà alquanto basso (si parla, in questo specifico caso, di firma elettronica “debole”);

- **firma elettronica avanzata** (FeA): la FeA è connessa unicamente al firmatario e lo identifica; è creata mediante dati per la creazione di una firma elettronica che il firmatario può utilizzare sotto il proprio controllo esclusivo; è inoltre collegata ai dati sottoscritti, in modo da consentire l’identificazione di ogni successiva modifica;
- **firma elettronica qualificata** (FeQ): è una FeA basata su un certificato qualificato per firme elettroniche e creata con un dispositivo di firma.
- **firma digitale**: è un particolare tipo di FeQ¹⁸, generata con un algoritmo crittografico asimmetrico.
- **firma digitale remota**: è un tipo di FeQ, generata su un *Hardware Security Module* (gestito da un prestatore di servizi fiduciari qualificato), che garantisce il controllo esclusivo delle chiavi private da parte dei titolari delle stesse. I firmatari non dispongono di un dispositivo di firma portatile: la generazione di una firma avviene in seguito a un processo di identificazione informatica e autenticazione basato su un elevato livello di sicurezza.

Nel Comune di Reggio Calabria si utilizza la firma digitale.

Il certificato elettronico che sia revocato, scaduto o sospeso rende il documento mancante di sottoscrizione. Le firme elettroniche avanzate, qualificate o digitali rimangono valide, al contrario, se al documento

¹⁸ Cfr. CAD, art. 24, *Firma digitale*.

informatico è associato un riferimento temporale opponibile a terzi, che sia costituito dalla data e dall'ora determinata con un riferimento al Tempo Universale Coordinato – UTC. Tale indicazione è indispensabile per la verifica della validità degli strumenti di firma alla data dell'apposizione e per stabilire, di conseguenza, il valore probatorio del documento stesso. Un riferimento temporale che sia opponibile a terzi si ottiene:

- con una marca temporale (certificatori accreditati);
- con la data e l'ora di generazione della segnatura di protocollo;
- con la data e l'ora del rapporto di versamento generato con la procedura di conservazione digitale, in conformità alle norme vigenti;
- con la data e l'ora della ricevuta rilasciata dal servizio di Posta Elettronica Certificata – PEC.

3.3. Sottoscrizione e verifica della firma

Quando prescritta, la sottoscrizione è ottenuta con un processo di firma digitale conforme alle disposizioni vigenti, tale da garantire l'integrità e l'immodificabilità del documento.

Nel Comune di Reggio Calabria, l'apposizione della firma può avvenire in modalità CAdES, con l'ottenimento di un file (una busta contenente sia il documento firmato, sia il file con la firma digitale) con estensione “.p7m”, o in modalità PAdES, operazione che permette di sottoscrivere unicamente un documento in formato “.pdf”; il file ottenuto avrà estensione, appunto, “.pdf”, e permetterà di gestire diverse versioni dello stesso documento, senza invalidare le firme apposte precedentemente.

- È buona norma non sovrapporre le modalità di firma, poiché possono riscontrarsi anomalie durante la verifica dei certificati, o in sede di conservazione dei documenti.
- È altrettanto buona norma sottoscrivere unicamente documenti che siano in formato “.pdf” (convertiti prima del processo).

La firma in formato XAdES è lo standard per la sottoscrizione dei documenti in formato XML (le fatture elettroniche trasmesse al Sistema di Interscambio, ad esempio).

La verifica della firma digitale dei documenti prodotti o ricevuti avviene con l'utilizzo di applicazioni online o software rilasciati gratuitamente da enti certificatori, elencati dall'Agenzia per l'Italia digitale, o attraverso il software attualmente in uso presso il Comune.

Il sistema di protocollo, infatti, prevede delle funzioni automatiche di verifica della firma digitale:

- la busta virtuale contenente il documento firmato è aperta;
- la validità del certificato è verificata;
- nel momento della sottoscrizione digitale, è verificata la presenza della *Certification Authority* (che emette il certificato di firma) nell'elenco pubblico dei certificatori accreditati;
- è segnalato al protocollista l'esito della verifica.

3.4. Copie e attestazioni di conformità

La **copia**¹⁹ **per immagine su supporto informatico di documento analogico** è un documento informatico avente contenuto e forma identico a quelli del documento analogico da cui è tratto, previo raffronto (o certificazione di processo). Ha la stessa efficacia probatoria dell'originale se la conformità è attestata da notaio o da un pubblico ufficiale autorizzato (o da funzionario incaricato), o non è espressamente disconosciuta.

La **copia informatica di documento analogico** è un documento informatico avente contenuto identico a quello del documento analogico da cui è tratto, previo raffronto (o certificazione di processo). Ha la stessa efficacia probatoria dell'originale se la conformità è attestata da notaio o da un pubblico ufficiale autorizzato (o da funzionario incaricato), o non è espressamente disconosciuta. L'attestazione di conformità sottoscritta con firma digitale è inserita nel documento informatico contenente la copia, o, eventualmente, è prodotta con un documento separato, che contenga un riferimento temporale e l'impronta digitale d'ogni copia.

La **copia informatica di documento informatico** è un documento informatico avente contenuto identico al documento da cui è tratto, con diversa sequenza di valori binari o evidenza informatica (s'intenda un differente formato); la copia ha la stessa efficacia probatoria se la conformità all'originale è attestata da pubblico ufficiale autorizzato (o da

¹⁹ Cfr. CAD, dall'art. 23.

funzionario incaricato), o non è espressamente disconosciuta. Il **duplicato informatico di documento informatico** è un documento informatico avente contenuto identico al documento da cui è tratto, medesima sequenza di valori binari, nonché stesso valore giuridico. Non necessita, pertanto, di attestazione di conformità all'originale.

La **copia analogica di documenti informatici** ha la stessa efficacia probatoria dell'originale da cui è tratto, a patto che la conformità all'originale sia attestata da pubblico ufficiale o funzionario autorizzato, o non sia espressamente disconosciuta.

L'**estratto** del documento informatico è una copia con una riproduzione parziale del contenuto del documento stesso. Anche l'estratto necessita di sottoscrizione mediante firma digitale o FeQ: in questo modo, infatti, ha la stessa efficacia probatoria dell'originale, a patto che tale conformità non sia espressamente disconosciuta.

3.5. Redazione e formazione del documento informatico

Tutti i documenti prodotti dal Comune di Reggio Calabria sono documenti informatici, formati secondo le seguenti quattro modalità²⁰:

- sono creati utilizzando software di *office automation* o editor di testo o servizi cloud qualificati, tali da assicurare la produzione dei documenti nei formati e nel rispetto delle regole di interoperabilità;

²⁰ Cfr. LLGG, 2.1.1, *Formazione del documento informatico*.

- sono acquisiti per via telematica (tramite casella PEC o PEO) o su supporto informatico (si pensi a una *pendrive*), o sono acquisite delle copie per immagine su supporto informatico (con una scansione) o delle copie informatiche di un documento analogico;
- le informazioni che derivino da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli resi disponibili all'utente sono memorizzate su supporto informatico in formato digitale;
- un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica, sono generati e raggruppati (anche in via automatica).

Oltre ad essere identificato univocamente, il documento informatico ha caratteristiche di immodificabilità e integrità, garantite dall'apposizione di una FeA, una FeQ, una firma digitale o un sigillo elettronico qualificato, dalla memorizzazione su un sistema di gestione documentale (che adotti idonee misure di sicurezza) e dalla registrazione nel registro di protocollo, dal versamento a un sistema di conservazione, o dal trasferimento a soggetti terzi attraverso un servizio di PEC o di recapito certificato qualificato.

3.6. I formati dei documenti

Per la formazione e la gestione dei documenti informatici, il Comune di Reggio Calabria opta per dei formati²¹ standard, coerenti con quanto

²¹ Il formato elettronico è un insieme di regole che organizza e dà un significato alla sequenza binaria che costituisce il documento informatico. Mediante un apparato hardware e software, le regole sopracitate permettono la visualizzazione a stampa o video della sequenza binaria, e dunque del contenuto del documento.

specificato nell'Allegato 2 delle *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*.

In genere, è buona prassi prediligere formati non vincolati a piattaforme tecnologiche, aperti e standard *de iure* (le cui specifiche siano liberamente accessibili), non proprietari e caratterizzati da robustezza (affinché i file corrotti siano recuperabili), accuratezza, usabilità, stabilità e sicurezza. È bene, inoltre, che non ammettano macroistruzioni all'interno del file. Si guarda costantemente all'interoperabilità tra sistemi differenti, ma anche all'evoluzione tecnologica, che porta con sé l'inevitabile obsolescenza degli strumenti e degli standard internazionali.

Formati differenti da quelli indicati sono utilizzabili, previa periodica (se non annuale) valutazione di interoperabilità, effettuata sulla base delle indicazioni dell'Allegato 2 delle *Linee Guida*.

Talvolta, è opportuno effettuare un riversamento dei file da un formato all'altro.

4. La protocollazione

Il capitolo intende illustrare le modalità di produzione e conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate.

4.1 Premessa

La registrazione segue all'acquisizione del documento nel sistema di gestione documentale (è il caso del documento in entrata) o precede la spedizione dello stesso (è il caso del documento in partenza).

Registrare un documento equivale a introdurlo nella memoria dell'ente produttore, identificandolo e descrivendolo con dei metadati utili alla ricerca, al reperimento e alla conservazione. Una volta inserito nell'archivio digitale, il documento confluisce in un fascicolo informatico, o aggregazione documentale informatica (ADI).

4.2. Il sistema di protocollo informatico: Auriga

Il sistema di protocollo informatico attualmente in uso presso il Comune di Reggio Calabria è l'applicativo "Auriga".

Per il funzionamento dell'applicativo, si rimanda all'Allegato 2 del presente Manuale, nel quale sono illustrate le modalità operative, le funzionalità principali e le relative procedure.

5. La classificazione

L'operazione di classificazione, parallelamente alle operazioni di registrazione e segnatura di protocollo, è un'operazione necessaria e sufficiente per la tenuta del sistema di gestione informatica dei documenti dalle PA.

La classificazione organizza logicamente i documenti amministrativi informatici prodotti o acquisiti dal Comune di Reggio Calabria durante l'esercizio delle sue funzioni, e le informazioni che ne derivano sono parte integrante dei metadati previsti per la formazione dei documenti stessi.

L'Allegato 3 del presente manuale riporta il Titolario di Classificazione.

6. L'organigramma

L'applicativo Auriga è strutturato secondo un organigramma funzionale che ne garantisce efficienza, scalabilità e una chiara suddivisione dei compiti. La sua architettura modulare consente una gestione ordinata delle funzionalità, facilitando sia l'uso da parte degli utenti finali sia la manutenzione da parte del team tecnico.

Alla base dell'organigramma si trova il modulo di accesso, che gestisce l'autenticazione degli utenti tramite credenziali sicure (login/password). Questo componente garantisce che solo gli utenti autorizzati possano accedere ai dati e alle funzioni dell'applicativo.

L'Allegato 4 del presente manuale riporta l'Organigramma.

7. Casi d'uso e comportamenti

7.1. Gestione della PEC (protocollo@pec.reggiocal.it) e indicazioni per la compilazione dell'oggetto e del corrispondente

La Posta Elettronica Certificata – PEC è un servizio che assicura alle comunicazioni elettroniche le stesse garanzie del servizio di posta raccomandata con ricevuta di ritorno. La PEC istituzionale del Comune di Reggio Calabria è integrata nel sistema di gestione documentale.

In merito ai messaggi in entrata, come già indicato, la registrazione è effettuata entro 24 ore lavorative dal ricevimento o, nel caso di giorni festivi e chiusure dell'ente, nel primo giorno lavorativo utile.

L'Ufficio Protocollo procede alla registrazione conferendo priorità alle comunicazioni dei Ministeri, della Prefettura, della Questura, del MEF, della Corte dei Conti e della Regione Calabria, nonché agli atti giudiziari notificati. Gli addetti proseguono poi cronologicamente, registrando i messaggi dal meno al più recente. I documenti pervenuti tramite PEC hanno priorità sui documenti pervenuti tramite PEO.

7.2. Gestione delle altre caselle PEC istituzionali

Il Comune di Reggio Calabria ha attivato delle caselle PEC per specifiche UOR e per determinati servizi. Le caselle PEC sono integrate nel sistema di gestione documentale e perlopiù di tipo “aperto”: ciò vuol dire che possono pervenire documenti informatici sia da mittenti PEC, che da mittenti PEO.

Valgono le medesime raccomandazioni valide per la gestione della PEC istituzionale, con un'accortezza ulteriore: è consigliabile verificare che i messaggi non siano già stati protocollati, se inviati a più indirizzi del Comune di Reggio Calabria.

Le PEC istituzionali attualmente attive e integrate nel sistema di gestione documentale sono elencate nell'Allegato 5 del presente manuale.

7.3. Gestione della PEO istituzionale

Al dipendente è assegnata una casella di posta elettronica nominativa, in modo che il titolare sia identificato in modo univoco. La posta elettronica è uno strumento di lavoro agile e sostituisce la comunicazione scritta.

Non è opportuno, tuttavia, che lo scambio di documenti all'esterno del Comune di Reggio Calabria avvenga mediante caselle di posta elettronica nominative. Se ciò avvenisse, i documenti concernenti affari o procedimenti amministrativi devono essere tempestivamente protocollati (inoltrati all'Ufficio Protocollo, o, preferibilmente, in autonomia).

7.4. Le fatture passive dal Sistema di interscambio – SdI

La fattura elettronica è trasmessa e ricevuta attraverso il Sistema di interscambio, e rispetta i requisiti, in termini di formato e contenuto. La fattura perviene attraverso lo SdI in cooperazione applicativa, in formato *.xml*, tramite i canali dichiarati e registrati sull'indice IPA. La registrazione a protocollo è automatica: la fattura è classificata e assegnata, trasmessa poi al sistema di contabilità.

7.5. Registro accesso civico

L'ente ha attivato un portale per la gestione informatizzata di tutte le richieste di accesso civico ed accesso civico generalizzato. Il portale "Accesso Civico" è raggiungibile dall'utenza al seguente indirizzo web:

<https://reggiocal.accessocivico.eu>.

La piattaforma è stata istituita anche con lo scopo di migliorare la compilazione e la pubblicazione periodica del registro degli accessi agli atti del Comune di Reggio Calabria.

Le richieste di accesso agli atti pervenute e le relative risposte (di accoglimento, diniego, differimento) sono registrate in piattaforma, in modo che sia possibile il tracciamento.

7.6. Determine, delibere di Giunta e di Consiglio, ordinanze

La creazione di determinazioni dirigenziali, delibere di Giunta e di Consiglio Comunale e ordinanze è subordinata all'utilizzo dell'applicativo *Auriga*. Gli atti, una volta redatti, sono inseriti in un iter approvativo organizzato in fasi. La conclusione dell'iter è la pubblicazione automatica in Albo Pretorio online.

Poiché l'utilizzo degli specifici applicativi è imprescindibile per una corretta gestione documentale – determine, delibere e ordinanze sono oggetto di registrazione particolare – è esclusa un'ordinaria registrazione di protocollo.

7.7. Altri atti soggetti alla pubblicazione in Albo Pretorio

Qualora il documento debba essere pubblicato in Albo Pretorio, ma non rientri in un iter automatico⁵⁴, è necessario assegnarlo manualmente, tramite registrazione di protocollo, all'Ufficio Albo pretorio. Se richiesto il referto di avvenuta pubblicazione, l'UOR compila il campo "note" della registrazione, esplicitando l'esigenza.

Per la redazione e la pubblicazione dell'atto si rimanda alle *Linee guida sulla pubblicità legale dei documenti e sulla conservazione dei siti web delle PA*⁵⁵, elaborate da un gruppo di lavoro AgID.

L'attenzione è rivolta, in particolare, alla pubblicazione all'albo pretorio di dati personali, necessaria solo se espressamente prevista da norma di legge, o regolamento. È pertanto fondamentale verificare quando sia necessario pubblicare tali dati, e quando, invece, è sufficiente diffondere un documento che descriva la circostanza dell'azione amministrativa del Comune di Reggio Calabria.

Il criterio a cui attenersi è quello di pertinenza e non eccedenza.

8. La gestione dell'archivio del Comune di Reggio Calabria

Convenzionalmente, si distinguono nella vita d'un archivio tre età: l'archivio corrente, l'archivio di deposito e l'archivio storico.

8.1. Archivio corrente: definizione e prassi

L'archivio corrente è il complesso di documenti che riguardano procedimenti, attività o affari in corso, non ancora esauriti. In questa fase, il Responsabile del procedimento dell'UOR apre, popola e cura i fascicoli, monitorando la corretta e ordinata sedimentazione dell'archivio. Un archivio corrente organizzato, infatti, è efficace ed efficiente sia per preservare la memoria dell'ente, sia per garantire il regolare svolgimento dell'attività giuridico-amministrativa.

Indipendentemente dal supporto, i fascicoli devono essere creati e gestiti correttamente.

Nel caso di fascicoli analogici, questi sono raccolti in faldoni, unità di conservazione che riporta riferimenti e indicazioni chiare. In particolare, i faldoni:

1. Sono numerati progressivamente, se afferiscono a uno stesso procedimento, attività, affare.
2. Riportano sul dorso l'UOR del Comune di Reggio Calabria e il Responsabile del procedimento interessati.
3. Riportano sul dorso un oggetto completo, non muto o parziale.
4. Riportano sul dorso riferimenti temporali corretti.
5. Riportano sul dorso la classificazione archivistica, come da titolare.
6. Riportano sul dorso gli estremi dei fascicoli contenuti.

Gli strumenti dell'archivio corrente sono il registro di protocollo, il piano di fascicolazione e il repertorio dei fascicoli, il titolario di classificazione e il piano di conservazione.

8.2. Archivio di deposito: definizione e prassi

L'archivio di deposito, età intermedia, si colloca tra l'archivio corrente e l'archivio storico. È una fase caratterizzata da transitorietà, ove i documenti, non più attivi, sono consultati sporadicamente ed esauriscono a poco a poco la loro funzione.

Il trasferimento dei documenti all'archivio di deposito. Almeno una volta all'anno fascicoli e serie archivistiche relativi a procedimenti conclusi sono trasferiti all'archivio di deposito⁵⁷, nel rispetto dell'organizzazione data nell'archivio corrente, senza manipolazioni o alterazioni. Allo stesso modo, almeno una volta l'anno il Responsabile della gestione documentale produce e trasmette al sistema di conservazione (nel caso del Comune di Reggio Calabria un soggetto esterno) i pacchetti di versamento.

Premessa a una corretta gestione e conservazione documentale è l'operazione di **sfoltimento dei fascicoli**, a cura dell'UOR che li ha creati, curati e popolati. L'operazione consiste nell'estrazione, una volta chiuso il fascicolo, della documentazione strumentale (quale la normativa, i documenti generali o privi di valore a seguito del provvedimento finale, le copie, le bozze e gli appunti), prima del versamento all'archivio di deposito.

Con il riversamento dei fascicoli all'archivio di deposito, la gestione degli stessi passa all'Ufficio Archivio, ma la responsabilità delle unità archivistiche rimane comunque in capo all'UOR: la consultazione, ad ogni modo, passa per una richiesta interna, formulata tramite casella di posta elettronica. È bene ricordare che:

- Consultazione e prelievo avvengono esclusivamente su richiesta scritta.
- L'accesso all'archivio di deposito (e storico) è consentito al solo personale dell'Ufficio Archivio, a chi detiene un'autorizzazione esplicita e scritta o agli addetti delle pulizie.

Selezione e scarto archivistico. In archivio di deposito si effettuano le operazioni di selezione e scarto archivistico. La selezione è un momento valutativo che mira ad individuare i documenti essenziali, con conservazione a lungo termine o permanente. I documenti transitori sono scartati, e dunque destinati alla distruzione.

8.3. Archivio storico: definizione e prassi di consultazione

L'archivio storico tutela, conserva e valorizza i documenti che abbiano valore storico, culturale e giuridico-amministrativo. È costituito da documenti relativi a procedimenti, affari o attività esauriti da oltre quarant'anni²², e su di esso è esercitata la vigilanza della Soprintendenza archivistica.

²² Cfr. Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42), art. 21, *Interventi soggetti ad autorizzazione*.

Consultazione dei documenti di interesse storico. Il cittadino che, per motivi di studio, ricerca e pubblicazione, abbia interesse a consultare i documenti dell'archivio storico del Comune di Reggio Calabria, è invitato a presentare richiesta al Responsabile dell'Ufficio Archivio Storico per tramite del protocollo.

Al momento della consultazione, il cittadino è invitato a compilare un modulo, poi registrato a protocollo per tracciare l'accesso, allegato alla richiesta espressa tramite mail.

Le riproduzioni fotografiche e digitali, utilizzando degli apparecchi propri, sono permesse per uso personale o motivi di studio e valorizzazione (senza scopo di lucro), a patto che non interessino documenti sottoposti a restrizioni di consultabilità²³.

9. Misure di sicurezza e di protezione dei dati personali

9.1. La tutela dei dati personali

I dipendenti del Comune di Reggio Calabria in conformità a quanto previsto dal decreto del Sindaco, sono autorizzati a trattare i dati necessari allo svolgimento delle proprie mansioni lavorative, sulla base delle esigenze del servizio e le finalità dell'ente, nel rispetto del **principio di liceità, correttezza e trasparenza**.

L'accesso è circoscritto alle informazioni necessarie per adempiere ai compiti istituzionali assegnati, nel rispetto del **principio di necessità, pertinenza e non eccedenza**, nonché del **principio di minimizzazione**.

²³ Cfr. *Nomina designati ed autorizzati al trattamento dei dati personali ai sensi dell'art. 29 del Regolamento UE 679/2016 e dell'art. 2-quaterdecies del D. lgs. n. 196/2003* del 1° febbraio 2024.

Gli autorizzati assicurano l'esattezza dei dati, e che questi sono conservati in una forma che identifica gli interessati per un arco di tempo coerente con le finalità per cui sono trattati. Nessuna informazione è trattata, comunicata o diffusa all'esterno del Comune, fatta eccezione per i casi esplicitamente previsti.

Gli autorizzati ricevono indicazioni precise sul tipo di trattamento dati²⁴ consentito: la lista dei trattamenti, fondata sull'organigramma dell'ente, è periodicamente aggiornata. Il registro delle attività di trattamento è curato dal DPO.

Il Comune, al fine di garantire la sicurezza e riservatezza dei dati personali, anche nel rispetto del principio di *accountability* di cui al Regolamento UE 679/16, ha adottato il "Protocollo per la rilevazione, valutazione e gestione delle violazioni di dati personali ai sensi degli articoli 33 e seguenti Regolamento UE 679/2016" contenente le procedure da seguire in caso di avvenuta violazione di sicurezza, nonché le indicazioni per valutarne i rischi, contenerne gli effetti negativi e porvi rimedio.

Si rimanda alla sezione in Amministrazione trasparente per la nomina del Responsabile della Protezione dei Dati personali (detto DPO).

24 Ove per "trattamento" si intende una qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, anche se non registrati in una banca dati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'elaborazione, la selezione, il blocco, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali.

9.2. Sicurezza dei sistemi informatici del Comune di Reggio Calabria: misure e istruzioni

Per la presente sezione si rimanda al redigendo documento sulla sicurezza delle informazioni.

Il sistema informatico comunale è costituito dall'insieme degli strumenti tecnologici per il trattamento delle informazioni (hardware e software) e dalle reti telematiche.

I dipendenti del Comune di Reggio Calabria sono tenuti al rispetto delle *Istruzioni e misure di sicurezza nell'utilizzo di strumenti informatici e analogici* (nonché agli aggiornamenti della circolare e alle istruzioni impartite dal Titolare, alle disposizioni in materia di dati personali e ai provvedimenti del Garante per la protezione dei dati personali e delle altre Autorità europee competenti).

Il sistema gestisce i dati conformemente a quanto previsto dalla legge. La memorizzazione dei documenti è effettuata sui sistemi del Comune. La prima fase consiste nel salvataggio immediato nelle cartelle di rete presenti nel server del Comune.

Si assicura per i documenti informatici l'autenticità, la non ripudiabilità, la validità temporale (e la sua estensione).

La postazione di lavoro e l'accesso ai dati.

I dipendenti osservano le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita di dati (anche accidentale), accessi non autorizzati e trattamenti non consentiti, o conformi alle finalità²⁵.

²⁵ Si agisce nel rispetto del principio *privacy by default*.

Accedono alle cartelle di rete e alle banche dati solo se qualificati e abilitati, poiché le risorse del sistema sono sottoposte a un controllo differenziato, a seconda dell'utente o del gruppo di utenti.

I dipendenti hanno cura di non lasciar accessibile o incustodito uno strumento elettronico durante una sessione di trattamento di dati.

L'accesso ai dispositivi in uso è possibile con credenziali di autenticazione di tipo *username* e *password*, parola chiave da aggiornare ogni tre mesi, di adeguata complessità.

L'accesso al sistema di gestione documentale.

Le abilitazioni di accesso al sistema di gestione documentale sono domandate per iscritto (*e-mail*) dai Dirigenti dei Settori.

I dipendenti, infatti, operano solo se in possesso di *username* e *password* (un identificativo utente e una parola chiave), dati segreti che consentono l'accesso alle sole risorse informatiche per cui si è autorizzati. L'uso del profilo è strettamente personale, e le attività sono tracciate ai fini della sicurezza.

Le registrazioni di protocollo sono riservate perché è prevista l'identificazione dell'utente.

Sono assegnati profili di autorizzazione differenti (*access control list - ACL*), tali da disciplinare accesso e operazioni svolte, in rapporto alle funzioni e al ruolo svolto dal dipendente. I profili agiscono anche sui diritti di visibilità.

Il Comune è dotato di sistemi automatici di filtraggio degli indirizzi Internet, nonché d'un software antivirus regolarmente aggiornato, per contrastare l'intrusione ad opera di programmi.

10. Elenco degli allegati

Allegato 1: Struttura del Comune di Reggio Calabria

Allegato 2: Manuale dell'applicativo *Auriga*

Allegato 3: Titolario di classificazione *Auriga*

Allegato 4: Organigramma *Auriga*

Allegato 5: Elenco PEC istituzionali attive

Allegato 6: Elenco estensioni ammesse su *Auriga*