



**CAMERA DI COMMERCIO
BRINDISI-TARANTO**

**MANUALE DI GESTIONE DOCUMENTALE
DELLA CAMERA DI COMMERCIO DI
BRINDISI - TARANTO**

Versione 1.1.2026

SOMMARIO

1	Premesse	4
1.1	<i>Principali riferimenti normativi</i>	4
1.2	<i>Glossario</i>	5
1.3	<i>Il manuale: approvazione ed aggiornamento.</i>	11
2	Il Sistema di Gestione documentale	12
2.1	<i>Aree Organizzative Omogenee</i>	12
2.2	<i>Il servizio per la tenuta del protocollo informatico</i>	13
2.3	<i>Ruoli e responsabilità</i>	13
2.4	<i>Il sistema di gestione documentale e protocollo informatico</i>	16
3	Tutela dei dati personali e sicurezza del sistema di gestione documentale	17
3.1	<i>Accountability</i>	17
3.2	<i>Registro delle attività di trattamento di dati personali</i>	18
3.3	<i>Ruoli</i>	19
3.4	<i>Piano della sicurezza</i>	19
3.5	<i>Accessibilità al sistema di gestione e livelli di riservatezza</i>	20
3.6	<i>Gestione documentale delle segnalazioni whistleblowing</i>	21
4	La formazione dei documenti	22
4.1	<i>Modalità di formazione dei documenti e contenuti minimi</i>	22
4.2	<i>Firme elettroniche</i>	23
4.3	<i>Posta elettronica ordinaria</i>	23
4.4	<i>Posta elettronica certificata</i>	24
4.5	<i>I formati dei documenti informatici</i>	24
4.6	<i>I metadati dei documenti informatici</i>	25
4.7	<i>Firma dei documenti informatici</i>	25
4.8	<i>La gestione dei documenti cartacei</i>	25
4.9	<i>Copie e duplicati</i>	25
4.10	<i>Copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico</i>	26
4.11	<i>Copie analogiche di originali informatici</i>	26
5	La trasmissione dei documenti	27

5.1	<i>Ricezione dei documenti informatici</i>	27
5.2	<i>Ricezione dei documenti su supporto cartaceo</i>	28
5.3	<i>Ricezione della posta elettronica ordinaria</i>	28
5.4	<i>Ricezione e gestione dei messaggi di posta elettronica certificata</i>	29
5.5	<i>Spedizione dei documenti cartacei</i>	29
5.6	<i>Spedizione dei documenti informatici</i>	29
5.7	<i>Domicilio digitale</i>	30
5.8	<i>Documenti interni</i>	31
6	La registrazione dei documenti	31
6.1	<i>Documenti soggetti a registrazione di protocollo</i>	31
6.2	<i>Documenti non soggetti a registrazione obbligatoria di protocollo</i>	32
6.3	<i>Registrazione di protocollo dei documenti</i>	32
6.4	<i>Segnatura di protocollo</i>	34
6.5	<i>Annullamento e modifica delle registrazioni di protocollo</i>	34
6.6	<i>Differimento dei termini di registrazione</i>	35
6.7	<i>Registro giornaliero di protocollo</i>	35
6.8	<i>Registro annuale di protocollo</i>	36
6.9	<i>Registro di emergenza</i>	36
7	Casi particolari	37
7.1	<i>Documentazione soggetta a registrazione particolare</i>	37
7.2	<i>Documentazione relativa a gare d'appalto</i>	39
7.3	<i>Documenti a carattere riservato, personale e/o confidenziale</i>	39
7.4	<i>Lettere anonime</i>	39
7.5	<i>Documenti non firmati o con firma illeggibile</i>	40
7.6	<i>Documentazione di competenza di altri uffici</i>	40
7.7	<i>Documento inviato a più UO e/o pervenuto attraverso canali diversi</i>	40
7.8	<i>Oggetti plurimi</i>	40
8	Assegnazione e classificazione dei documenti	40
8.1	<i>Assegnazione</i>	40
8.2	<i>Modifica delle assegnazioni</i>	42
8.3	<i>Consegna dei documenti cartacei</i>	42
8.4	<i>Consegna dei documenti informatici</i>	42
8.5	<i>Classificazione dei documenti</i>	43

9	Fascicolazione dei documenti	43
9.1	<i>Formazione dei fascicoli</i>	43
9.2	<i>Tipologie di fascicolo</i>	45
9.3	<i>Struttura gerarchica del fascicolo</i>	46
9.4	<i>Processo di identificazione e formazione dei fascicoli</i>	48
9.5	<i>Alimentazione dei fascicoli</i>	49
9.6	<i>Conservazione dei fascicoli</i>	49
9.7	<i>Gestione dello scarto</i>	49
10	Scansione dei documenti cartacei	51
10.1	<i>Processo di scansione e certificazione di conformità</i>	51
10.2	<i>Certificazione di processo</i>	52
11	Gestione documenti cartacei degli archivi di deposito	53
11.1	<i>La movimentazione dei fascicoli</i>	53
11.2	<i>Gestione dell'archivio storico</i>	53
12	Accesso ai documenti e tutela della riservatezza	53
12.1	<i>Amministrazione trasparente</i>	54
13	Disposizioni finali	54
	<i>ELENCO ALLEGATI</i>	54

1 Premesse

In ottemperanza a quanto previsto dalle «Linee Guida sulla formazione, gestione e conservazione dei documenti informatici» (AGID, Determinazione n. 407/2020, aggiornate al 18 maggio 2021) la Camera di commercio di Brindisi – Taranto ha redatto il presente Manuale di Gestione (MdG) con l'obiettivo di descrivere il sistema di gestione dei documenti, anche ai fini della conservazione, e di fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il Manuale di gestione è stato predisposto con una duplice finalità: da un lato disciplinare il sistema di gestione documentale dell'Ente e, dall'altro, rappresentare le funzionalità disponibili per tutti gli utenti, interni ed esterni, che interagiscono con la Camera di commercio di Brindisi - Taranto.

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le indicazioni per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti; pertanto si rivolge non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti e ai soggetti esterni che si relazionano con l'ente.

In particolare, il Manuale disciplina:

- le modalità informatiche di formazione e scambio dei documenti dell'amministrazione e la loro gestione;
- la gestione dei flussi documentali;
- l'utilizzo del sistema di gestione documentale;
- l'uso del Piano di classificazione e del Piano di fascicolazione;
- la conservazione dei documenti;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo o interesse;
- le politiche di protezione dati e il Piano della sicurezza;
- la gestione documentale delle segnalazioni whistleblowing.

Il presente manuale è pubblicato sul sito internet istituzionale della Camera di commercio, all'interno della Sezione "Amministrazione trasparente" nella sottosezione "Altri Contenuti > Manuale di Gestione documentale".

1.1 Principali riferimenti normativi

La principale normativa di riferimento per la gestione dei documenti informatici all'interno della pubblica amministrazione è rappresentata dalle seguenti fonti:

Normativa nazionale e comunitaria:

- Legge 7 agosto 1990, n. 241 – Norme sul procedimento amministrativo;
- D.P.R. 28 dicembre 2000, n. 445 – Testo unico sulla documentazione amministrativa (TUDA);
- D. Lgs. 30 giugno 2003, n. 196 – Codice della Privacy;
- Legge 9 gennaio 2004, n. 4 – Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;
- D. Lgs. 22 gennaio 2004, n. 42 – Codice dei Beni Culturali e del Paesaggio;

- D. Lgs. 7 marzo 2005, n. 82 – Codice dell’Amministrazione Digitale (CAD) e successive modifiche;
- D. Lgs. 14 marzo 2013, n. 33 – Trasparenza nella pubblica amministrazione;
- D. Lgs. 10 marzo 2023, n.24 – Protezione degli informatori (whistleblowing), con impatti su gestione e conservazione documentale;
- D. Lgs. 31 marzo 2023, n.36 – Codice dei contratti pubblici;
- Regolamento (UE) 2016/679 – Regolamento Generale sulla Protezione dei Dati (GDPR);
- Regolamento (UE) 2022/2554 – Digital Operational Resilience Act (DORA); Digital Operational Resilience Act: obblighi di sicurezza per sistemi digitali critici (come quelli di gestione e conservazione documentale)
- Regolamento (UE) 2022/868 – Data Governance Act - riutilizzo e condivisione dei dati pubblici

Normativa tecnica e regolamentare AgID:

- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (Determinazione n. 407/2020, aggiornate al 18 maggio 2021), che hanno assorbito e superato le previgenti regole tecniche di cui ai DPCM 3 dicembre 2013, 13 novembre 2014 e 22 febbraio 2013;
- Determinazione AgID n. 628/2021 – Requisiti per la conservazione e modelli organizzativi dei soggetti conservatori;
- Determinazione AgID n. 371/2022 – Firme elettroniche, sigilli, validazioni temporali e certificati qualificati;
- Circolare AgID n. 3/2023 – Aggiornamento delle misure minime di sicurezza ICT per le pubbliche amministrazioni (che sostituisce la previgente Circolare AgID n. 2/2017 del 18 aprile 2017);
- Determinazione AgID n. 121/2019.

Normativa fiscale e documenti digitali:

- Decreto MEF 17 giugno 2014 – Obblighi fiscali per i documenti informatici;
- Decreto MEF 3 aprile 2013, n. 55 (come modificato dal DM 18 aprile 2014 e successive modifiche) – Fattura elettronica verso la PA;
- Art. 2215-bis del Codice Civile – Documentazione informatica.

Standard e riferimenti internazionali:

- UNI 11386:2020 – Standard SInCRO;
- UNI EN ISO/IEC 27001:2022 – Sicurezza delle informazioni;
- UNI EN ISO 22301:2019 – Business Continuity Management;
- ISO/IEC 27018:2019 – Protezione dei dati nei servizi cloud;
- ISO 14721:2012 (OAIS) – Modello di riferimento per l'archiviazione;
- ETSI EN 319 401 / 411 / 421 – Standard europei su servizi fiduciari e firme digitali.

1.2 Glossario

Ai fini del presente documento si intendono:

- **Accesso:** operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti amministrativi informatici;

- **Accreditamento:** riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione;
- **Affare:** complesso di documenti prodotti (spediti, ricevuti, allegati, ecc.) da un ente, relativi alla trattazione di un oggetto specifico di sua competenza; si chiama affare o anche pratica;
- **Allegato:** documento unito a un documento o a una pratica per prova, per chiarimento o integrazione di notizie, per memoria;
- **Archivio:** il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività. Con questo termine si intende anche il luogo fisico di conservazione della documentazione;
- **Archivio informatico:** archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico;
- **Area Organizzativa Omogenea (AOO):** insieme di funzioni e di strutture che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del Testo Unico;
- **Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico:** dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico;
- **Autenticità:** caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;
- **Classificazione:** strumento per la formazione dell'archivio, cioè per l'ordinamento di tutti i documenti prodotti e acquisiti nello svolgimento dell'attività amministrativa;
- **Conservatore accreditato:** soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale;
- **Conservazione:** insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione;
- **Copia analogica del documento informatico:** documento analogico avente contenuto identico a quello del documento informatico da cui è tratto;
- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1 del GDPR);
- **Delegati:** personale dell'ente incaricato formalmente dal RGD per l'espletamento di funzioni previste dal presente Manuale;
- **Destinatario:** identifica il soggetto/sistema al quale il documento informatico è indirizzato;
- **Documento informatico:** rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti (art. 1 comma 1 lett. p) del CAD);
- **Documento analogico:** rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1 comma 1 lett. p bis) del CAD);

- **Domicilio digitale:** un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito «Regolamento eIDAS», valido ai fini delle comunicazioni elettroniche aventi valore legale;
- **Duplicazione dei documenti informatici:** produzione di duplicati informatici;
- **Esibizione:** operazione che consente di visualizzare un documento conservato e di ottenerne copia;
- **Evidenza informatica:** una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
- **Fascicolo informatico:** Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD;
- **Firma elettronica:** insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **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 consentire di rilevare se i dati stessi siano stati successivamente modificati;
- **Firma digitale:** è un particolare di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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;
- **Formato contenitore:** formato di file progettato per consentire l'inclusione («imbustamento» o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati;
- **Formato del documento informatico:** modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file;
- **Flusso documentale:** movimento dei documenti all'interno dell'archivio (dalla fase di formazione dell'archivio corrente a quella di conservazione dell'archivio storico);
- **Funzione di hash:** una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali;
- **GEDOC – Nuovo sistema di gestione documentale (GEDOC):** sistema informatico utilizzato per la protocollazione dei documenti in ingresso e uscita, la classificazione secondo un Piano di classificazione, la fascicolazione e l'archiviazione dei documenti di rilevanza amministrativa;
- **Gestione dei documenti:** l'insieme di attività finalizzate alla registrazione di protocollo e alla classificazione, fascicolazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato (Piano di classificazione);

- **Identificazione informatica:** la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco a un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;
- **Identificativo univoco:** sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione;
- **Interoperabilità:** caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi;
- **Immodificabilità:** caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso;
- **Impronta:** la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash. Un'evidenza informatica di lunghezza predefinita ottenuta da un'altra evidenza informatica mediante un'opportuna funzione matematica tale che risulti di fatto impossibile, a partire dall'impronta, ricostruire l'evidenza informatica che l'ha generata, ed altresì risulti di fatto impossibile determinare una coppia di evidenze informatiche per le quali la funzione generi impronte uguali;
- **Leggibilità:** insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;
- **Log di sistema:** registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati;
- **Manuale di Gestione del protocollo informatico, dei documenti e degli archivi (MdG):** strumento che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;
- **Massimario di selezione:** il massimario di selezione è lo strumento che consente di coordinare razionalmente lo scarto archivistico dei documenti prodotti dagli enti pubblici e dagli organi centrali e periferici dello Stato. Il massimario riproduce l'elenco delle partizioni (categorie) e sottopartizioni del Titolario con una descrizione più o meno dettagliata delle competenze cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascuna partizione quali documenti debbano essere conservati permanentemente (e quindi versati dopo trent'anni dall'esaurimento degli affari nei competenti Archivi di Stato) e quali invece possono essere destinati al macero dopo cinque, dieci anni, venti anni, ecc.;
- **Metadati:** insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione;
- **Oggetto:** in sede di formazione del documento l'oggetto è l'enunciazione sommaria, sintetizzata in poche parole, al massimo un paio di righe, dell'argomento di cui tratta il documento. L'oggetto viene scritto sul documento nello spazio apposito e deve essere riportato (talora con parole diverse) sia sul registro di protocollo dell'ente che scrive sia su quello dell'ente che riceve il documento;
- **Pacchetto di versamento (PdV):** pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione;

- **Piano di Classificazione:** struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata;
- **Piano di fascicolazione e conservazione:** documento allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di fascicolazione, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445;
- **Piano della sicurezza del sistema di gestione informatica dei documenti:** documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza;
- **Piano generale della sicurezza:** documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza;
- **Posta elettronica certificata (PEC):** sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
- **Posta elettronica ordinaria (PEO):** sistema di comunicazione che non attesta l'invio e l'avvenuta consegna di un messaggio di posta elettronica e non fornisce ricevute opponibili ai terzi;
- **Pubblico ufficiale:** il notaio, e le altre figure previste dall'art. 18, comma 2 del DPR 445/2000;
- **Registrazione di protocollo:** attività che permette di identificare in modo certo i documenti ricevuti o spediti su qualunque supporto di trasmissione da un soggetto produttore; ha una finalità giuridico-probatoria ed è strumento di certificazione e di verifica dell'autenticità dei documenti;
- **Registro:** unità archivistica costituita da un insieme di fogli rilegati. Nel registro vengono trascritti o registrati per esteso o per sunto documenti e minute di documenti, ovvero vengono effettuate trascrizioni, registrazioni e annotazioni costitutive dell'atto giuridico. Spesso si usa impropriamente l'espressione volume come sinonimo di registro;
- **Registro particolare:** registro informatico, regolato da norme specifiche, usato per particolari tipologie documentali e che può contenere trascrizioni, registrazioni e annotazioni costitutive di un atto giuridico, previsto ai sensi dell'articolo 53, comma 5 del DPR 445/2000;
- **Registro di protocollo:** registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti;
- **Repertorio informatico:** registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;
- **Repertorio della Serie:** registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del Piano di classificazione: il repertorio deve essere organizzato in maniera da riprodurre le suddivisioni del Piano di classificazione;
- **Responsabile del Procedimento (RdP):** il dipendente che assume su di sé la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un singolo procedimento amministrativo;
- **Responsabile della gestione documentale (RGD):** ovvero Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali, nonché degli archivi;
- **Responsabile della Conservazione:** dirigente o funzionario formalmente designato che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;
- **Responsabile della protezione dei dati (RPD):** il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle

prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Reg. UE 2016/679. Trattasi di un dipendente del titolare del trattamento o del responsabile del trattamento oppure di un incaricato all'assolvimento dei suoi compiti sulla base di un contratto di servizi (art. 37 del Reg. UE 2016/679);

- **Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi:** dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione;
- **Responsabile del trattamento dei dati:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **Responsabile della Transizione al Digitale (RTD):** figura dirigenziale all'interno della PA che ha tra le sue principali funzioni quella di garantire operativamente la trasformazione digitale dell'amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell'adozione di nuovi modelli di relazione trasparenti e aperti con i cittadini;
- **Responsabile della sicurezza:** soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza;
- **Riferimento temporale:** informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
- **Scarto:** operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale;
- **Segnatura di protocollo:** apposizione o associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni che consentono di identificare/individuare in modo inequivocabile il documento stesso;
- **Serie archivistica:** ciascun raggruppamento di documenti con caratteristiche omogenee, all'interno di un fondo archivistico. Può essere articolata in sottoserie;
- **Servizio archivistico:** il servizio per la gestione dei documenti, del protocollo, dei flussi documentali e degli archivi analogici e informatici;
- **Sistema informativo:** insieme degli strumenti e procedure che consente l'accesso sul web alle risorse archivistiche e ne permette la gestione e fruibilità;
- **Sistema di gestione informatica dei documenti:** nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445;
- **Sistema di conservazione:** sistema di conservazione dei documenti informatici di cui all'art. 44 del CAD;
- **Sottofascicolo:** articolazione interna al fascicolo;
- **Titolare del trattamento dei dati:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **Titolario di classificazione:** sistema precostituito di schemi di voci gerarchicamente ordinate, individuato in base alle funzioni e alle materie di competenza dell'amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la conservazione secondo un ordine

logico. Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello, etc. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato;

- **Trasmissione telematica:** trasmissione di documenti attraverso servizi di telecomunicazione;
- **Trattamento dei dati:** 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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Utente:** persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse;
- **Unità archivistica:** termine generico con cui si individua l'unità minima indivisibile di un fondo archivistico, che può aggregare più documenti, fisicamente contigui, o essere costituita da una singola unità documentaria. Può essere costituita da un fascicolo, un registro, una filza, un volume ecc.;
- **Unità Organizzativa responsabile (UOR):** ufficio che, per tipologia di funzioni e di competenza, presenta esigenze di gestione della documentazione unitarie e coordinate;
- **Validazione temporale:** il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;
- **Vicario:** il dipendente che assume le funzioni e i compiti del Responsabile della gestione documentale nei casi di assenza, vacanza o impedimento di quest'ultimo;
- **Vigilanza:** Indica l'insieme delle funzioni attribuite alle Soprintendenze archivistiche relative alla tutela degli archivi degli enti pubblici, territoriali e non territoriali, e degli archivi privati, conservati di massima presso l'ente produttore o presso istituzioni culturali diverse dagli Archivi di Stato;
- **Vincolo archivistico:** nesso che collega in maniera logica e necessaria i documenti che compongono l'archivio di un ente;
- **Violazione dei dati personali:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

1.3 Il manuale: approvazione ed aggiornamento.

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi viene adottato con determina dirigenziale del Segretario generale ed è pubblicato sul sito istituzionale nell'area «Amministrazione trasparente» prevista dall'art. 9 del D.Lgs. 33/2013.

Il Manuale descrive il sistema di gestione dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e dell'archivio corrente.

Esso è redatto a cura del Responsabile della gestione documentale (RGD), che ne propone lo schema al Segretario generale.

Il Manuale, in un contesto di continua trasformazione, deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e strumenti utilizzati. Allo stesso modo anche i processi e le attività inerenti le attività di formazione dei documenti devono essere sottoposti a costante valutazione e monitoraggio. Il RGD provvederà alle eventuali integrazioni o revisioni nei casi in cui lo ritenga opportuno, ad esempio a seguito di:

- modifiche normative o regolamentari sopravvenute;
- introduzione di nuove pratiche tendenti a migliorare l'operatività dell'ente in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- sostanziali modifiche apportate nell'ambito dell'architettura del sistema e delle singole componenti informatiche utilizzate.

In caso risultasse necessario apportare aggiornamenti, il RGD li propone al Segretario generale fornendo ogni informazione utile all'assunzione del relativo provvedimento.

Nel caso di avvicendamento del RGD, il nuovo Responsabile deve prendere visione del Manuale di gestione, verificare le regole in esso contenute ed eventualmente modificarle, proponendo aggiornamenti del manuale stesso.

2 Il Sistema di Gestione documentale

2.1 Aree Organizzative Omogenee

L'ente ha scelto di configurarsi, ai fini della gestione documentale, come unica Area Organizzativa Omogenea denominata C.C.I.A.A. di Taranto - Brindisi (di seguito AOO), composta dall'insieme di unità organizzative articolate come riportato nell'allegato denominato «Organigramma» e di definire, quindi, un unico sistema di gestione documentale e protocollo informatico.

I vantaggi derivanti da tale scelta organizzativa sono i seguenti:

- omogeneità di organizzazione del servizio;
- riduzione dei costi di gestione del servizio;
- eliminazione della frammentazione dei sistemi di protocollo;
- maggiore flessibilità del servizio;
- indipendenza dalle dinamiche di riorganizzazione dell'ente;
- semplificazione delle operazioni di archiviazione e reperimento dei documenti;
- riduzione della ridondanza della documentazione da gestire;
- semplificazione dell'iter documentale.

Per la protocollazione dei documenti in entrata si è adottato un modello operativo di tipo centralizzato bipartito tra la sede di Taranto e la sede di Brindisi.

Per la protocollazione dei documenti in uscita si è adottato un modello decentralizzato presso ciascuna UO.

2.2 Il servizio per la tenuta del protocollo informatico

Ai sensi dell'art. 61, comma 1, del D.P.R. 28 dicembre 2000 n. 445 – T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa – la Camera di commercio di Brindisi - Taranto ha provveduto ad istituire uno specifico ed unitario Servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi.

Il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi è istituito nella AOO.

La struttura organizzativa che ne ha la responsabilità è quella «Archivio e protocollo».

2.3 Ruoli e responsabilità

Nel sistema di gestione documentale sono stati individuati i seguenti ruoli previsti dalla normativa vigente:

Ruolo	Riferimento normativo
Responsabile della gestione documentale	Art. 61 del D.P.R. 28 dicembre 2000, n. 445
Responsabile della conservazione	Art. 44 del D.Lgs. 7 marzo 2005, n. 82 – CAD e art. 4.6 delle Linee Guida AGID
Responsabile della transizione al digitale	Art. 17 del D.Lgs. 7 marzo 2005, n. 82 – CAD e Circolare n. 3 del 1° ottobre 2018 del Ministro per la pubblica amministrazione
Responsabile della protezione dei dati	Art. 37 del Regolamento (UE) 2016/679 (GDPR)

Il Responsabile della gestione documentale

La Camera di Commercio, nel rispetto della normativa vigente, ha conferito, con deliberazione Presidenziale d'urgenza n.9 del 29/2/2024 ratificata dalla Giunta camerale con delibera n.11 del 3/4/2024, il ruolo di responsabile del «servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi».

Al Responsabile, sulla base di quanto previsto dalla normativa, spetta il compito di:

- predisporre lo schema del Manuale di gestione;
- verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA;
- predisporre il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:
- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID;
- curare la formazione del personale in materia di gestione documentale e rende disponibile tutta la documentazione relativa all'uso dell'hardware e software in uso all'ente (es. manuali d'uso);
- provvedere a generare, per uno o più documenti informatici, un pacchetto di versamento nelle modalità e con i formati concordati con il responsabile della conservazione e previsti dal manuale di

conservazione e, in quanto produttore del Pacchetto di Versamento (PdV), verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

Al Responsabile della gestione documentale spetta, altresì, l'invio periodico all'archivio di deposito e/o al sistema di conservazione dei fascicoli e delle serie documentarie relative a procedimenti anche non conclusi, e l'elaborazione e aggiornamento del Piano di conservazione dei documenti, siano essi digitali o cartacei.

Il Responsabile, per l'esercizio delle proprie funzioni, ha facoltà di nominare i seguenti delegati:

- delegato per la tenuta del protocollo informatico;
- delegato per la gestione dei flussi documentali.

Rientra nella discrezionalità del RDG nominare delegati, purché questi siano in possesso di requisiti professionali e tecnici necessari allo svolgimento della mansione affidatagli.

Responsabile della conservazione

Il Responsabile della conservazione è stato nominato con deliberazione Presidenziale d'urgenza n.9 del 29/2/2024 ratificata dalla Giunta camerale con delibera n.11 del 3/4/2024.

Il Responsabile della conservazione è la persona incaricata di curare l'insieme delle attività finalizzate alla conservazione dei documenti. In virtù della trasversalità delle sue funzioni, il responsabile si avvale della collaborazione del Responsabile del trattamento dei dati personali, del Responsabile della sicurezza, del Responsabile dei sistemi informativi e del Responsabile della gestione documentale.

Al Responsabile della conservazione compete l'insieme delle seguenti attività descritte nelle Linee Guida AgID:

- 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;

l) 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 al medesimo attribuite;

m) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

n) 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;

o) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Ai sensi dell'art. 44, comma 1-quater del CAD, il responsabile della conservazione può affidare, in tutto o in parte, lo svolgimento del processo di conservazione a un conservatore che possiede i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea e nazionale nonché delle Linee guida emanate da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Responsabile della transizione al digitale

Con deliberazione Presidenziale d'urgenza n.9 del 29/2/2024 ratificata dalla Giunta camerale con delibera n.11 del 3/4/2024 è stato conferito il ruolo di responsabile della transizione digitale secondo quanto previsto dall'art. 17 del CAD.

Le funzioni del Responsabile della transizione al digitale sono elencate dal comma 1 dall'articolo 17 del CAD, che attribuisce all'Ufficio per la transizione digitale i compiti relativi a:

- coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
- indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

- indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;
- accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità;
- analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- cooperazione alla revisione della riorganizzazione dell'amministrazione;
- indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione;
- pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione, al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale.

L'elenco di cui sopra è da considerarsi esemplificativo e non esaustivo, in ragione della trasversalità della figura. In aggiunta ad essi, il Responsabile può, inoltre:

- costituire tavoli di coordinamento con gli altri dirigenti dell'amministrazione e/o referenti nominati da questi ultimi;
- costituire gruppi tematici per singole attività e/o adempimenti (ad esempio: pagamenti informatici, implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, ecc.);
- proporre l'adozione di circolari e atti di indirizzo sulle materie di propria competenza (ad esempio, in materia di approvvigionamento di beni e servizi ICT) secondo quanto previsto nella Circolare n. 3 del 1° ottobre 2018 del Ministro per la pubblica amministrazione.

2.4 Il sistema di gestione documentale e protocollo informatico

L'art. 1 comma 1 lettera r) del DPR 445 del 2000 definisce il Sistema di gestione informatica dei documenti come: «l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti».

La Camera utilizza il sistema di protocollo informatico «GEDOC – Nuovo sistema di gestione documentale» (in breve GEDOC) realizzato e fornito da Infocamere Scpa nell'ambito dei rapporti in essere con l'amministrazione. Le principali componenti di GEDOC sono riportate in allegato al presente documento [ALLEGATO 01].

Il Sistema è integrato con gli strumenti di gestione documentale quali: il Piano di classificazione, il Piano di fascicolazione e di conservazione, anch'essi allegati al presente documento [ALLEGATI 02,03].

GEDOC si interfaccia con gli applicativi usati dall'amministrazione per la gestione di determinati processi e/o procedimenti e garantisce che le operazioni di registrazione, archiviazione e invio in conservazione della documentazione prodotta si svolgano nel rispetto della normativa vigente e delle regole riportate negli strumenti di gestione documentale adottati. L'elenco di tali applicativi è riportato in allegato [ALLEGATO 04].

Il sistema GEDOC, le risorse strumentali e le procedure utilizzate dalla Camera di Commercio per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento nell'ambito dell'AOO;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo.

In GEDOC non viene gestita la documentazione soggetta a registrazione particolare.

3 Tutela dei dati personali e sicurezza del sistema di gestione documentale

Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, noto come GDPR (General Data Protection Regulation), e che abroga la direttiva 95/46/CE, impone ai Titolari del trattamento di mettere in atto misure di sicurezza tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia svolto nel rispetto delle previsioni legislative europee e nazionali, nonché per tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

La Camera ha avviato un percorso di adeguamento alla nuova normativa in materia di protezione dei dati personali. Tale adeguamento rappresenta un processo *on going* che richiede un continuo monitoraggio, revisione/integrazione dei documenti adottati, delle procedure, delle policy, dei regolamenti interni e in generale della compliance dell'Ente.

3.1 Accountability

I Titolari e i Responsabili del trattamento sono tenuti a mettere in atto misure adeguate ed efficaci per la tutela dei dati personali e devono essere in grado di dimostrare la conformità alla disciplina in materia di dati personali delle attività svolte e l'efficacia e l'adeguatezza delle misure concretamente adottate.

In particolare, il Titolare del Trattamento, deve essere in grado di dimostrare che le attività di trattamento svolte rispondano ai principi di liceità dettati dall'art. 5 GDPR, ossia che i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Affinché i dati siano trattati in modo lecito, il trattamento deve essere fondato su almeno uno dei legittimi presupposti (basi giuridiche) elencati dall'art. 6 GDPR per quanto concerne i dati personali c.d. «comuni», all'art. 9 per le categorie particolari di dati e all'art. 10 per i dati relativi a condanne penali e reati. Con riferimento alle categorie particolari di dati personali, nonché ai dati relativi a condanne penali e reati, al fine di individuare compiutamente la corretta base giuridica, deve tenersi conto, altresì, della disciplina nazionale in materia di protezione dei dati personali, contenuta negli artt. 2-sexies, 2-septies e 2-octies D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018.

Per quanto concerne poi i trattamenti ulteriori svolti per finalità di archiviazione nel pubblico interesse, condizione essenziale per la liceità e correttezza degli stessi è il rispetto delle regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica, di cui al Provvedimento n. 513 del 19 dicembre 2018 Garante Privacy, pubblicate in G.U. n. 12 del 15 gennaio 2019.

Per la definizione dei tempi massimi di conservazione (c.d. data retention), sia che il trattamento avvenga con modalità analogiche sia che avvenga con modalità digitali, la Camera ha fatto riferimento alle tempistiche riportate nel Piano di conservazione predisposto da Unioncamere e adottato dalle singole Camere di commercio.

I dati possono essere trattati per periodi ulteriori unicamente per finalità di archiviazione nel pubblico interesse conformemente a quanto previsto dall'art. 89, par. 1, GDPR e delle norme del Codice dei Beni Culturali (artt. 122 – 127 T.U. 42/2004).

I documenti sono conservati nell'archivio nel rispetto delle misure tecniche e organizzative previste dalla normativa a tutela dei diritti e delle libertà dell'interessato.

3.2 Registro delle attività di trattamento di dati personali

Strettamente correlato al principio di accountability, e indispensabile a tal fine, è l'obbligo imposto dall'art. 30 GDPR in ordine alla tenuta e all'aggiornamento del Registro delle attività di trattamento, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

I contenuti minimi del Registro previsti dall'art. 30 GDPR sono i seguenti:

- 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;
- le finalità del trattamento (e la base giuridica per ciascuna finalità);

- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del GDPR.

Il Registro contiene, oltre agli elementi fondamentali indicati all'art. 30 GDPR, ulteriori elementi di dettaglio e descrittivi indispensabili, in ottica di accountability, all'Ente per documentare ed argomentare coerentemente le proprie scelte ed essere così in grado di dimostrare di aver operato correttamente.

Il Registro dei Trattamenti dell'Ente è rinvenibile nella sezione Amministrazione Trasparente del sito web camerale.

3.3 Ruoli

Alla luce del principio di «responsabilizzazione», la Camera di commercio di Brindisi – Taranto è tenuta a definire, nell'ambito della propria struttura organizzativa interna, i compiti e responsabilità in capo ai soggetti comunque coinvolti nei processi di trattamento di dati personali quali: soggetti designati/autorizzati, referenti, amministratori di sistema interni. Nella definizione dei compiti e delle responsabilità interne, e dunque nel conferimento delle designazioni/autorizzazioni al trattamento di dati personali, occorre prestare la massima attenzione all'assegnazione dei poteri di accesso, inserimento, modifica, eliminazione (etc.) dei dati trattati dall'Ente, al solo personale che necessita effettivamente di effettuare tali operazioni in ragione dello svolgimento delle proprie mansioni.

A tal fine la Camera di Commercio ha:

- formalmente individuato i soggetti designati/autorizzati al trattamento ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03 così come modificato dal D.Lgs. 101/18, assegnando agli stessi precisi compiti ed istruzioni con riferimento al trattamento dei dati personali;
- adottato un proprio Modello Organizzativo Privacy.

3.4 Piano della sicurezza

Il responsabile della gestione documentale predispone, in accordo con il responsabile della sicurezza, il responsabile della conservazione, il responsabile dell'ufficio per la transizione al digitale e acquisito il parere del responsabile della protezione dei dati personali, il Piano della sicurezza del sistema di gestione informatica dei documenti, nel rispetto delle misure minime di sicurezza ICT emanate dall'AgID con Circolare n. 3/2023 (che ha aggiornato e sostituito la previgente Circolare AgID n. 2/2017 del 18 aprile 2017).

Il Piano della sicurezza del sistema di gestione informatica dei documenti, in quanto parte del più ampio Piano generale della sicurezza, viene aggiornato periodicamente dall'ente.

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, particolari e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Le misure di sicurezza garantiscono che:

- le informazioni e i dati siano disponibili, integri e protetti secondo il loro livello di riservatezza;
- per i documenti e i fascicoli informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale e l'estensione della validità temporale;
- gli atti, i documenti e i dati, in relazione alle conoscenze acquisite in base all'evoluzione tecnologica, alla loro natura e alle specifiche caratteristiche del trattamento, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta e della gestione.

Le misure generali tecniche e organizzative inerenti alla gestione documentale sono le seguenti:

- analisi del rischio;
- piani specifici di formazione degli addetti;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di una credenziale di identificazione interna (utente), di una credenziale riservata di autenticazione (password) e di un profilo di accesso;
- cambio delle password con frequenza stabilita nel Piano della sicurezza;
- gestione delle postazioni individuali e mantenimento della scrivania e schermo puliti (mediante apposita «Clear desk and clear screen policy»);
- gestione, dismissione e smaltimento degli apparati mobili e dei supporti;
- gestione del servizio con particolare riferimento sia all'esecuzione, che alla gestione delle copie di back-up dei dati e dei documenti da effettuarsi con frequenza giornaliera;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei «moduli» (patch e service pack) correttivi dei sistemi operativi;
- tracciamento delle attività nel file di log del sistema;
- monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Poiché il Sistema di Gestione Documentale è ospitato su infrastruttura IT di InfoCamere ed è gestito dal punto di vista infrastrutturale sempre da InfoCamere, le politiche di sicurezza descritte nel presente paragrafo riguardano il fornitore (Infocamere).

3.5 Accessibilità al sistema di gestione e livelli di riservatezza

Il sistema di gestione documentale è organizzato nel rispetto delle norme vigenti in materia di diritto di accesso (artt. 22 e ss. L. 241/1990 sul procedimento amministrativo e D.Lgs. n. 33/2013 sulla Trasparenza) e protezione dei dati personali (D. Lgs n. 196/2003 e GDPR).

I dipendenti della Camera di commercio di Brindisi – Taranto possono legittimamente accedere soltanto alle informazioni, ai documenti e ai fascicoli presenti nel sistema, la cui consultazione sia relativa a procedimenti e attività di propria competenza, ovvero secondo la posizione che rivestono all'interno del funzionigramma della Camera di commercio.

Ciascun dipendente dell'amministrazione è in possesso di credenziali di accesso, consegnate previa identificazione dei soggetti stessi, in modo da creare un'associazione univoca tra identità fisica e identità digitale.

Sulla base delle funzioni svolte sono assegnate le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate dal sistema.

Il sistema di gestione documentale consente il controllo differenziato dell'accesso alle risorse di sistema per ciascun utente o gruppi di utenti, permettendo altresì di tracciare tutte le operazioni svolte individuandone, all'occorrenza, l'autore.

I profili di accesso al sistema sono suddivisi secondo le seguenti categorie:

- Responsabile della gestione documentale (vicario e delegati), che ha la visibilità completa di tutti gli oggetti documentali del sistema, quali: schede, documenti, allegati, fascicoli, registri, etc.
- Utente, che ha la visibilità per competenza o per conoscenza delle schede documentali e dei fascicoli secondo il funzionigramma.

Il sistema consente il controllo differenziato dell'accesso alle risorse di sistema per ciascun utente in base al profilo attribuito (ruoli e permessi assegnati), permettendo altresì di tracciare tutte le operazioni svolte.

3.6 Gestione documentale delle segnalazioni whistleblowing

Il D.Lgs. 10 marzo 2023, n. 24, in attuazione della Direttiva (UE) 2019/1937, disciplina la protezione delle persone che segnalano violazioni del diritto dell'Unione (whistleblowing). La norma impatta sulla gestione documentale sotto i seguenti profili:

a) **Canale di segnalazione interno:** la Camera ha attivato un canale di segnalazione interno che garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità del segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;

b) **Gestione documentale separata:** la documentazione relativa alle segnalazioni whistleblowing è gestita con modalità informatiche che assicurano il massimo livello di riservatezza e di protezione dei dati personali. Il sistema GEDOC prevede un'area riservata e segregata, accessibile esclusivamente al personale autorizzato alla gestione delle segnalazioni, con profili di accesso differenziati e tracciamento di ogni operazione;

c) **Conservazione della documentazione:** le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del D.Lgs. 24/2023 e del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e) del GDPR;

d) **Tracciamento degli accessi:** ogni accesso alla documentazione relativa alle segnalazioni è tracciato mediante log di sistema, con indicazione dell'identificativo dell'utente, della data e dell'ora dell'accesso e delle operazioni compiute;

e) **Scarto:** decorso il termine di conservazione di cinque anni, la documentazione è sottoposta a scarto, previa autorizzazione della Soprintendenza archivistica, con modalità che garantiscano la distruzione sicura dei dati personali contenuti.

4 La formazione dei documenti

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

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

Ciò premesso, il documento amministrativo va distinto in:

- documento analogico;
- documento informatico.

Tutti i documenti originali, indipendentemente dal loro supporto, sono tra loro connessi da speciale vincolo originario (vincolo archivistico), necessario e determinato e costituiscono l'archivio della Camera di commercio di Brindisi - Taranto.

Ogni documento amministrativo è riferito ad un solo protocollo e può fare riferimento ad uno o più fascicoli.

4.1 Modalità di formazione dei documenti e contenuti minimi

La Camera di commercio forma gli originali dei propri atti come documenti informatici, ai sensi dell'art. 40, comma 1 del CAD, o come copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico, consistenti nella scansione di ogni singola unità documentale pervenuta in via analogica. La loro esibizione e produzione sostituisce quella dell'originale e hanno piena efficacia ai sensi degli articoli 2714 e 2715 del codice civile, se formati ai sensi dell'articolo 20, comma 1-bis del D.Lgs 82/2005.

In particolare, i documenti informatici sono formati secondo le seguenti principali modalità:

- Redazione tramite l'utilizzo di appositi software, preferibilmente open data;
- Acquisizione per via telematica o su supporto informatico di documenti informatici;
- Acquisizione della copia per immagine su supporto informatico di un documento analogico;
- Acquisizione della copia informatica di un documento analogico;
- Registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
- 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.

In particolare, riguardo alla modalità di cui al precedente punto 1 sono previsti dei modelli di riferimento per la redazione della documentazione, resi disponibili ai dipendenti, che stabiliscono il «layout» (compreso il font). L'utilizzo dei modelli di riferimento e il rispetto di apposite linee guida assicurano la formazione dei documenti prodotti dall'amministrazione in conformità alla normativa in materia di accessibilità (Legge n. 4/2004 e relative disposizioni di attuazione).

Gli originali informatici riportano, ove disponibili, le seguenti informazioni:

- logo e denominazione completa dell'amministrazione;
- indicazione dell'UO mittente;
- dati del destinatario o dei destinatari (recapito di posta elettronica certificata o ordinaria, recapito fisico);
- numero di riferimento a un procedimento/fascicolo;
- oggetto del documento;
- testo del documento;
- numero e descrizione degli eventuali allegati;
- dati dell'Ente (indirizzo completo, numeri di telefono, indirizzi PEC e PEO a cui indirizzare risposta).

Sono incaricati della verifica della presenza delle seguenti informazioni:

- il personale coinvolto nella redazione del documento;
- il personale addetto alle funzioni di protocollo (in caso di protocollazione centralizzata in uscita).

Il RGD e i suoi delegati possono avviare verifiche a campione per il riscontro della correttezza delle informazioni surriportate.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

All'atto del caricamento del documento nel sistema di gestione documentale è previsto l'inserimento almeno di un set minimo di metadati richiesti obbligatoriamente dal sistema.

4.2 Firme elettroniche

La Camera di commercio di Brindisi - Taranto fornisce la firma digitale ai soggetti da essa delegati a rappresentarla per l'espletamento delle attività istituzionali, per quelle relative ai processi, funzioni e atti amministrativi, nonché per le attività connesse all'attuazione della normativa relativa alla gestione dei documenti informatici.

La firma digitale è assegnata su richiesta dell'interessato in base ad esigenze lavorative specifiche ed il processo è regolamentato da procedura interna.

4.3 Posta elettronica ordinaria

Il servizio di posta elettronica è disponibile per tutti gli utenti dell'ente che vengono dotati di una casella di posta elettronica e che accedono utilizzando il proprio account utente di dominio (con relativa login e password). Per i dipendenti, l'indirizzo di posta elettronica è costituito dall'account utente di dominio con l'aggiunta del suffisso «@brta.camcom.it». Inoltre vengono utilizzate delle caselle di servizio funzionali all'attività lavorativa delle singole strutture.

Per le attività di registrazione di protocollo di documenti provenienti dall'esterno che erroneamente vengano indirizzate su caselle di PEO della Camera di commercio intestate ad uffici o al dipendente è prevista la trasmissione all'indirizzo dell'ufficio protocollo destinato a raccogliere e-mail con documenti ed eventuali allegati da protocollare. Le modalità di trasmissione sono descritte nel paragrafo 5.3.

4.4 Posta elettronica certificata

L'Ente utilizza la PEC quale sistema gestionale e di comunicazione, ai sensi della normativa vigente, in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili a terzi ad ogni effetto di legge.

La casella PEC istituzionale della AOO Camera di commercio industria artigianato e agricoltura di Brindisi – Taranto è «cameradicommercio@pec.brta.camcom.it» e viene utilizzata sia per la trasmissione, sia per la ricezione di documenti ed è integrata nel sistema di gestione documentale e protocollo informatico (GEDOC).

In ricezione e in trasmissione la casella è configurata sia per la comunicazione con indirizzi PEC, per i quali si riceveranno le ricevute di accettazione/consegna, sia con indirizzi di PEO, per i quali non si riceverà la ricevuta di consegna.

E' inoltre attiva una ulteriore casella di PEC creata esclusivamente per flussi documentali specifici al Registro delle Imprese: registroimprese@ta.legalmail.camcom.it

4.5 I formati dei documenti informatici

Il formato è la modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

L'obsolescenza dei formati dei file rappresenta una criticità consistente per la conservazione a lungo termine della documentazione la quale, per essere garantita, necessita di una cura continua, che inizia con la corretta scelta del formato già nella fase di gestione documentale.

Per contenere il rischio di obsolescenza occorre utilizzare formati il più possibile «aperti», liberamente utilizzabili e non coperti da brevetto, leggibili da software applicativi gratuiti e open-source che possano, a loro volta, essere facilmente reperibili, anche online.

Di conseguenza, per la creazione e formazione dei documenti nell'AOO si usano i formati DOCX, ODT, PDF, PDF/A; i documenti informatici prodotti dalla Camera di Commercio, indipendentemente dal software utilizzato, vengono convertiti in formato PDF/A all'atto del caricamento sul Sistema di gestione documentale GEDOC, salvo nei casi in cui essi siano già stati firmati con firma CADES.

Salvo diversamente previsto, agli utenti viene richiesto l'invio di documenti in PDF/A.

Nell'ambito dei formati dei file trattati non sono ammessi codici integrati quali le cd. «macro» o cifrature dei contenuti, soprattutto per le finalità di conservazione digitale.

I modelli dei documenti sono predisposti già in formato accessibile e al loro interno sono riportate le indicazioni da seguire per rendere il documento finale conforme ai requisiti di accessibilità.

Sono state individuate due macro categorie di formati:

- una categoria generale di formati, che tutte le Pubbliche Amministrazioni e le organizzazioni sul territorio nazionale devono essere in grado di gestire;
- una categoria speciale, riguardante specifiche tipologie di documenti.

Per i formati di file gestiti dalla Camera si rimanda al Manuale di conservazione pubblicato nella sezione Amministrazione Trasparente del sito web camerale.

Nell'ambito di specifici procedimenti possono essere utilizzati formati diversi da quelli adottati. Queste eccezioni riguardano essenzialmente documenti ricevuti dall'ente.

I formati contenitori: I formati compressi (generalmente distinguibili per l'estensione .zip, .7zip e .rar) possono essere utilizzati solo nel caso in cui i file in essi contenuti siano nei formati accettati dall'amministrazione.

4.6 I metadati dei documenti informatici

Al documento amministrativo informatico sono associati i metadati previsti nel paragrafo 6.3.

4.7 Firma dei documenti informatici

I documenti informatici prodotti o ricevuti dalla Camera che richiedono la firma elettronica a valore legale verranno sottoscritti con firma digitale. Le firme digitali adottate dall'ente sono nei formati CADES e PAdES.

I documenti che vanno sottoscritti con firma digitale devono essere prodotti, prima della firma, nel formato standard PDF/A, le cui caratteristiche tecniche trovano corrispondenza nei requisiti sul formato definite dalle Linee guida.

Ove presente, la data riportata sul documento deve essere coerente con quella dei metadati del documento, della firma digitale e del protocollo informatico.

Nel caso di documenti per i quali sia necessaria una data certa e opponibile a terzi, in particolare per i contratti, si renderà necessaria l'apposizione di marca temporale al momento della sottoscrizione. In caso di documento soggetto a registrazione di protocollo, data certa e provenienza certa sono assicurate dalla natura di atto pubblico di fede privilegiata del registro di protocollo.

4.8 La gestione dei documenti cartacei

In ottemperanza alle disposizioni del CAD, l'amministrazione gestisce i documenti analogici solo laddove risulti indispensabile nei rapporti con i soggetti privati che non siano in possesso di un domicilio digitale.

I documenti analogici acquisiti con le modalità tradizionali (consegna allo sportello, ricezione via posta o fax) devono essere digitalizzati ed inseriti all'interno del fascicolo cui si riferiscono ai sensi del presente Manuale, salvo i casi particolari indicati nel paragrafo 4.1.

La conservazione dei documenti cartacei è affidata all'ufficio protocollo.

4.9 Copie e duplicati

Le copie e duplicati di documenti possono essere prodotti secondo le seguenti fattispecie:

a) Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico: consistenti nella scansione di ogni singola unità documentale pervenuta in via analogica. Il documento così acquisito dovrà essere certificato conforme all'originale ai sensi dell'art. 22, comma 2, D.Lgs. n. 82/2005.

b) Copie analogiche di originali informatici: stampa dei documenti informatici da inviare ai cittadini sprovvisti di domicilio digitale. Se per la validità di tali operazioni e degli atti emessi sia prevista l'apposizione di firma autografa, la stessa è sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile (art. 3, comma 2, D.Lgs. n. 39/1993; art. 23 del D.Lgs. n. 82/2005).

c) Duplicati informatici: prodotti mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine.

4.10 Copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico

Per quanto riguarda il punto a) le tipologie di copie informatiche possono essere prodotte nei seguenti modi:

- Copia Semplice (Art. 22, comma 3, D.Lgs. n. 82/2005): viene prodotta tramite la mera scansione e registrazione nel sistema del documento analogico originale. La copia così prodotta ha la stessa efficacia probatoria dell'originale se la sua conformità non è espressamente disconosciuta. Resta fermo l'obbligo di conservazione degli originali analogici, che dovranno essere conservati negli appositi fascicoli cartacei.
- Copia Conforme (Art. 22 comma 2, D.Lgs. n. 82/2005): è accompagnata da una certificazione di conformità e ha la stessa efficacia probatoria dell'originale da cui è tratto.

La certificazione di conformità verrà effettuata dal delegato individuato dal RGD in fase di archiviazione della copia informatica del documento analogico all'interno del fascicolo di pertinenza. Il documento acquisito tramite scanner e la dichiarazione di conformità allegata saranno sottoscritti digitalmente dal delegato. Le copie così formate sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge.

4.11 Copie analogiche di originali informatici

Per quanto riguarda il punto b) le tipologie di copie analogiche possono essere prodotte nei seguenti modi:

- Copia Semplice (Art. 23, comma 2, D.Lgs. n. 82/2005): costituita da una semplice stampa del documento amministrativo informatico. Viene utilizzata in tutti quei casi in cui la natura dell'attività non richieda particolari tutele sul piano giuridico probatorio.
- Copia Conforme (Art. 23 comma 1, D.Lgs. n. 82/2005): ha lo stesso valore del documento informatico da cui è tratta perché, a differenza della prima, viene certificata da un pubblico ufficiale e non può essere disconosciuta dal destinatario (a meno di querela di falso).

La dichiarazione di conformità è prodotta dal sistema GEDOC, e contiene i riferimenti normativi, le indicazioni per identificare univocamente il documento (numero protocollo, data, impronte, numero di

pagine), data e luogo di produzione della copia. La dichiarazione deve essere stampata e firmata dal pubblico ufficiale delegato e deve riportare il timbro dell'ufficio (art. 18 DPR. 445/2000). Le copie analogiche degli atti amministrativi informatici firmati digitalmente, possono essere sottoscritte con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 febbraio 1993, n. 39. La firma autografa sostituita a mezzo stampa consiste nell'indicazione a stampa della fonte e del nominativo del soggetto responsabile, nonché dell'eventuale dicitura che specifica che il documento informatico da cui la copia analogica è tratta è stato prodotto ed è conservato dall'amministrazione secondo come previsto dal Codice.

La firma a stampa può essere utilizzata solo nei rapporti tra l'amministrazione e i privati e solo nei casi in cui il documento non sia una certificazione rilasciata dall'amministrazione.

5 La trasmissione dei documenti

I documenti si distinguono in base allo stato di trasmissione:

- Documento in ingresso (mittente esterno e destinatario interno): documento acquisito dall'AOO nell'esercizio delle proprie funzioni e proveniente da un diverso soggetto pubblico o privato;
- Documento in uscita (mittente interno e destinatario esterno): documento prodotto dalle UO interne dell'AOO nell'esercizio delle proprie funzioni, che ha rilevanza informativa e/o giuridico-probatoria e indirizzato a un diverso soggetto pubblico o privato;
- Documento interno: documento prodotto e scambiato internamente (il mittente e il destinatario sono interni). Il documento interno può non essere protocollato.

5.1 Ricezione dei documenti informatici

Un documento informatico può essere ricevuto in diversi modi:

- a mezzo posta elettronica certificata;
- a mezzo cooperazione applicativa;
- a mezzo posta elettronica ordinaria;
- su supporto rimovibile quale, ad esempio, CD ROM, DVD, tape, pen drive, ecc., consegnato direttamente o inviato per posta convenzionale o corriere;
- mediante accesso telematico.

L'amministrazione assicura l'accettazione dei documenti informatici inviati ai suoi uffici tramite i suddetti mezzi quando prodotti in uno dei formati riportati nel presente Manuale.

In tutti gli altri casi, laddove il documento inviato o consegnato all'amministrazione sia prodotto in formati tali da non consentirne una corretta gestione, ne verrà data comunicazione al mittente richiedendo contestualmente la ripetizione dell'invio in uno dei formati indicati nell'elenco o in altro formato concordato. In ogni caso i documenti elettronici inviati o consegnati dovranno essere privi di elementi attivi, tra cui macro e campi variabili.

L'aggiornamento dell'elenco dei formati dei documenti elettronici – da pubblicarsi anche sul sito istituzionale dell'amministrazione nella Sezione Modulistica – è curato dal Responsabile della Gestione Documentale.

5.2 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare attraverso:

- servizio postale (posta ordinaria, prioritaria, raccomandata, telegrammi);
- corrieri commerciali e società di recapito convenzionate;
- consegna diretta «brevi manu».

L'accettazione della corrispondenza, recapitata in una delle modalità sopra indicate, avviene negli orari di apertura degli uffici per tutti i giorni lavorativi, salvo diverse statuizioni particolari dipendenti dalla tipologia procedimentale.

Le unità che ricevono i documenti in arrivo sono:

- l'Ufficio Protocollo;
- l'Ufficio legale per la sola notifica di atti giudiziali e stragiudiziali.

In caso di necessità, il personale abilitato può procedere all'accettazione di specifici documenti anche al di fuori delle fasce orarie sopra indicate.

Il personale addetto al Protocollo tratta la corrispondenza secondo i seguenti tre raggruppamenti:

Tipologia di corrispondenza	Trattamento
Corrispondenza indirizzata direttamente a Presidente, Segretario Generale, Componenti Giunta	- la busta non è aperta - è apposto il timbro di accettazione - è trasmessa alle Segreterie competenti
Corrispondenza riportante la dicitura «Riservato» o «Personale» o corrispondenza valutata come tale	- la busta non è aperta - è apposto il timbro di accettazione - è trasmessa all'interessato
Corrispondenza che non rientra nei due casi precedenti	- la busta è aperta - è apposto il timbro di accettazione - si procede all'assegnazione

Gli addetti al protocollo provvedono alla registrazione, segnatura e scansione dei documenti, con relativo smistamento alle UO di competenza, se possibile, nello stesso giorno di ricezione ovvero nel primo giorno lavorativo successivo, salvo il caso in cui, per la mole dei documenti pervenuti, non sia necessario differire ulteriormente i termini con provvedimento motivato del Responsabile. Su richiesta dell'interessato viene rilasciata apposita ricevuta della avvenuta registrazione mediante il programma di protocollo informatico o, in alternativa, tramite apposizione di timbro sulla copia già in possesso dell'utente, specificando che trattasi di copia per l'utente.

5.3 Ricezione della posta elettronica ordinaria

Nel caso in cui – eccezionalmente – sulle caselle di posta elettronica del personale o delle strutture vengano trasmessi messaggi e documenti che devono essere protocollati, gli utenti dovranno far pervenire i messaggi all'indirizzo PEO del protocollo, verificandone preventivamente la compatibilità con i formati ammessi.

La procedura da seguire prevede che l'utente scarichi sul proprio pc il messaggio ricevuto in formato «.eml» e lo alleggi all'email da indirizzare all'ufficio protocollo: in questo modo verrà preservata l'integrità del

messaggio da protocollare e tutti i riferimenti relativi a mittente, oggetto, destinatario e orario di ricezione della email.

5.4 Ricezione e gestione dei messaggi di posta elettronica certificata

Quando i documenti informatici pervengono all'indirizzo istituzionale di posta elettronica certificata, gli addetti al protocollo procedono alla registrazione.

La casella è gestita dal personale dell'ufficio protocollo che la consulta giornalmente e valuta, in base alle regole definite nel presente manuale, se il contenuto sia da registrare o meno.

Il sistema GEDOC assicura l'automatica verifica di ricezione di eventuali nuovi messaggi di posta elettronica certificata. L'accesso alla casella PEC può essere effettuato con frequenza maggiore in caso di particolari circostanze (es. nei giorni antecedenti alla scadenza del termine per la presentazione di domande di partecipazione a bandi o avvisi, nel caso di scadenze fiscali, ecc.).

In ogni caso, il RGD e i suoi delegati faranno in modo che la casella istituzionale non raggiunga mai i limiti di capienza indicati dal fornitore della stessa.

Nel caso in cui venga recapitata per errore una comunicazione non di competenza dell'amministrazione, l'addetto al protocollo ovvero il RGD informano tempestivamente l'Ufficio affari generali che provvederà ad impartire le opportune istruzioni.

5.5 Spedizione dei documenti cartacei

La Camera provvede a inviare le comunicazioni ai soggetti che non hanno un domicilio digitale, ovvero nei casi di domicilio digitale non attivo, non funzionante o non raggiungibile, per posta ordinaria o raccomandata con avviso di ricevimento.

Queste comunicazioni sono predisposte come documenti informatici sottoscritti con firma digitale o altra firma elettronica qualificata e archiviati nel Sistema di gestione documentale, secondo le regole riportate nel Piano di fascicolazione. All'utente verrà inviata una copia analogica sottoscritta con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

Nel caso in cui si renda necessario nel corso dell'attività di sportello, gli operatori possono procedere alla consegna a mano di copia analogica dell'originale informatico ai cittadini sprovvisti di domicilio digitale. In ogni caso, all'interno del sistema GEDOC, l'operatore dovrà indicare le modalità di spedizione/consegna del documento all'utente.

5.6 Spedizione dei documenti informatici

I documenti informatici in uscita sono trasmessi a mezzo posta elettronica certificata.

Per particolari esigenze e nei casi in cui non sia possibile l'invio a mezzo PEC, la trasmissione può avvenire tramite supporto ottico rimovibile con registrazione non modificabile (es. CD ROM, DVD), consegnati direttamente o inviato per posta convenzionale o corriere.

Il documento informatico principale viene protocollato in uscita dagli uffici di competenza e spedito tramite GEDOC insieme agli allegati utilizzando le stesse caselle di PEC abilitate alla ricezione e associate al registro di protocollo generale dell'ente.

La Posta Elettronica Certificata (PEC) è il vettore privilegiato di relazioni con l'esterno; pertanto, nel caso in cui il destinatario disponga di un domicilio digitale ogni comunicazione formale con esso dovrà essere veicolata tramite questa casella.

Se il destinatario non è ancora dotato di un domicilio digitale, allora la spedizione avviene su supporto analogico secondo la procedura descritta nel Manuale.

5.7 Domicilio digitale

Il domicilio digitale permette di facilitare e velocizzare le comunicazioni tra pubbliche amministrazioni e tra queste e i privati.

Per domicilio digitale si intende un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dall'art. 44 del Regolamento (UE) n 910/2014, valido ai fini delle comunicazioni elettroniche aventi valore legale.

L'art. 3-bis del CAD prevede che le pubbliche amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese abbiano l'obbligo di dotarsi di un domicilio digitale iscritto nell'elenco di cui agli articoli 6-bis o 6-ter, in particolare:

- Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IndicePA - IPA);
- Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC);
- Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese (INAD).

L'Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi (IndicePA) contiene i domicili digitali da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi e i privati.

Per favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito presso il Ministero per lo sviluppo economico il pubblico elenco, denominato «Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti».

L'INAD è l'elenco pubblico contenente i domicili digitali, eletti ai sensi dell'articolo 3-bis, commi 1-bis e 1-ter del CAD dalle persone fisiche nonché dai professionisti e dagli enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese. Il domicilio digitale è l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale ai sensi dell'articolo 1, comma 1, lettera n-ter del CAD. Possono eleggere il proprio domicilio digitale mediante registrazione nell'INAD: a) le persone fisiche che abbiano compiuto il

diciottesimo anno di età e che abbiano la capacità di agire; b) i professionisti che svolgono una professione non organizzata in ordini, albi o collegi ai sensi della legge n. 4/2013; c) gli enti di diritto privato non tenuti all'iscrizione nell'INI-PEC.

La consultazione online degli Indici è consentita a chiunque senza necessità di autenticazione.

I domicili digitali inseriti negli Indici nazionali costituiscono mezzo esclusivo di comunicazione e notifica, secondo quanto previsto dall'art. 6, comma 1 del CAD.

Le comunicazioni tramite i domicili digitali dichiarati negli Indici nazionali producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente. Le comunicazioni si intendono spedite dal mittente se inviate al proprio gestore, e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a un fatto non imputabile al destinatario medesimo. La data e l'ora di trasmissione e ricezione del documento informatico sono opponibili ai terzi.

5.8 Documenti interni

I documenti interni, cioè i documenti prodotti e destinati all'interno sono formati con tecnologie informatiche.

I documenti interni che abbiano un valore formale scambiati tra le UO, vengono inviati attraverso il sistema GEDOC in modo che ne rimanga traccia, e non sussiste l'obbligo della sottoscrizione e della protocollazione.

I documenti che rivestono carattere informale possono essere scambiati tra UO attraverso la Posta elettronica o i sistemi informatici interni.

6 La registrazione dei documenti

Per registrazione si intende l'insieme delle procedure, elementi e strumenti attraverso i quali i documenti vengono trattati sotto il profilo strettamente giuridico-probatorio, e dunque il pubblico dipendente che opera nel sistema di protocollazione lo fa in qualità di pubblico ufficiale ed è garante della effettiva ricezione e spedizione dei documenti. La registrazione di protocollo certifica l'acquisizione o la spedizione in data certa di ciascun documento prodotto o ricevuto, indipendentemente dalla loro regolarità, verificata in un secondo tempo dai responsabili dei relativi procedimenti e si configura per la Amministrazione come un'attività obbligatoria.

La registrazione attesta l'esistenza di un determinato documento all'interno di GEDOC identificandolo univocamente e certifica in modo inoppugnabile, in quanto atto pubblico di fede privilegiata, la data archivistica, dalla quale partono gli effetti giuridici del documento ai sensi della L. 241/1990.

6.1 Documenti soggetti a registrazione di protocollo

Sono oggetto di registrazione obbligatoria ai sensi dell'articolo 53 del DPR n. 445/2000 i documenti ricevuti e inviati dall'amministrazione, che soddisfano i requisiti di competenza soggettiva e oggettiva e hanno un oggetto che riguarda le funzioni di cui l'Ente è competente.

Ai sensi dell'art. 40-bis del CAD, formano comunque oggetto di registrazione di protocollo le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi dell'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle Linee guida.

La registrazione avviene a cura degli utenti abilitati del sistema GEDOC o, quando previsto da specifiche procedure, automaticamente sulla base di valori definiti dal Responsabile della gestione documentale.

6.2 Documenti non soggetti a registrazione obbligatoria di protocollo

I documenti per i quali non è prevista la registrazione di protocollo sono:

- gazzette ufficiali;
- bollettini ufficiali;
- notiziari della pubblica amministrazione;
- materiali statistici;
- bollettini Banco Posta (incasso);
- atti preparatori interni;
- giornali;
- riviste;
- libri;
- opuscoli;
- depliant;
- materiali pubblicitari;
- inviti a manifestazioni che non danno adito ad un'eventuale attivazione di procedimenti amministrativi;
- i documenti già soggetti a registrazione particolare da parte dell'amministrazione;
- documenti di occasione aventi carattere effimero (ringraziamenti, richieste di appuntamenti con i dirigenti, congratulazioni varie, condoglianze, ...);
- tutte le e-mail che si configurano come comunicazioni informali aventi mera natura informativa e non amministrativa, eccetto casi particolari valutati dal Responsabile del procedimento (RdP).

6.3 Registrazione di protocollo dei documenti

La registrazione di protocollo è l'insieme delle informazioni fondamentali relative al contenuto, all'autore e alla modalità di trasmissione di un documento, memorizzate sul registro di protocollo.

Questa operazione ha lo scopo di descrivere il documento, individuandolo in modo univoco e di formalizzarne l'ingresso nel sistema documentale rendendone certa l'identificazione e il momento di formazione o entrata.

Il numero di protocollo individua un unico documento, compresi i suoi allegati, e dunque ogni documento reca un solo numero di protocollo.

La registrazione di protocollo - sia per i documenti pervenuti in via analogica che telematica - viene effettuata dal personale addetto alla protocollazione con l'ausilio della componente applicativa di «Protocollo» nell'ambito del Sistema di gestione documentale GEDOC, negli orari d'ufficio dal lunedì al venerdì. Contestualmente alla registrazione viene effettuata dal sistema la segnatura di protocollo.

Di norma la protocollazione avviene lo stesso giorno della ricezione del documento o, al più, il giorno lavorativo successivo se il documento è pervenuto fuori orario. In tal caso si darà priorità alla documentazione pervenuta sulla casella PEC in ordine cronologico di arrivo. Qualora ci sia una ricezione massiva di documenti a fronte di scadenze previste, la protocollazione potrà essere effettuata in differita secondo la procedura descritta al par.6.6.

Tutti gli addetti alla protocollazione sono tenuti al rispetto della riservatezza delle informazioni trattate.

Le modalità operative di protocollazione sono riportate nel «Manuale utente» di GEDOC, reso disponibile agli utenti.

La registrazione di protocollo per ogni documento ricevuto o spedito dalle Amministrazione è effettuata, secondo quanto previsto dall'articolo 53 del DPR 445/2000, mediante la memorizzazione obbligatoria delle seguenti informazioni:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto (assegnata automaticamente dal sistema e registrato in forma non modificabile).

A questi elementi giuridicamente rilevanti se ne possono aggiungere altri, non obbligatori, ma funzionali:

- codice fiscale / P.IVA del mittente;
- numero di protocollo dell'Amministrazione mittente (ove presente) per i documenti ricevuti;
- data del documento ricevuto;
- data di arrivo presso l'Ente (solo per il cartaceo);
- mezzo di ricezione o di spedizione;
- attribuzione a UO per competenza o conoscenza;
- utenti di visibilità del documento;
- livello di riservatezza;
- formato del documento (se elettronico o cartaceo);
- tipo di documento;
- classificazione;
- catalogo dei processi;
- descrizione sintetica degli allegati;
- note dell'operatore.

6.4 Segnatura di protocollo

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

Essa viene, generalmente, apposta sui documenti in uscita quando questi siano in formato .PDF e siano stati firmati digitalmente con firma PAdES. In tutti gli altri casi, la segnatura di protocollo è associata al documento come file .PDF autonomo e la si trova tra gli allegati del documento principale.

L'articolo 55, comma 1, del DPR 445/2000 individua le informazioni che caratterizzano la segnatura di protocollo, ovvero:

- codice identificativo dell'amministrazione;
- codice identificativo della Camera di commercio in quanto AOO;
- codice identificativo del registro;
- progressivo di protocollo;
- data di protocollo.

Ulteriori informazioni previste sono:

- indicazione del mittente/destinatario;
- la tipologia di Protocollo.

Per i documenti protocollati in uscita, se inviati tramite PEC ad altre amministrazioni viene generato automaticamente un messaggio e-mail conforme alle regole di interoperabilità, che ha in allegato anche il file «segnatura.xml» contenente i dati di segnatura.

6.5 Annullamento e modifica delle registrazioni di protocollo

Le operazioni di annullamento possono riguardare l'intera registrazione (annullamento di informazioni generate automaticamente dal sistema), o le singole informazioni non assegnate automaticamente dal sistema (aggiornamento della registrazione).

Il protocollo informatico assicura il tracciamento e la storicizzazione di ogni operazione, rendendole visibili e comparabili.

Modifica delle registrazioni di protocollo.

In base alla normativa vigente le uniche informazioni modificabili di una registrazione di protocollo sono l'assegnazione interna all'amministrazione e la classificazione.

Nel caso in cui le correzioni da effettuare riguardino il contenuto, dovrà essere seguita la procedura prevista per l'annullamento delle registrazioni di protocollo.

Annullamento dell'intera registrazione

Per quanto concerne le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile, l'annullamento anche di una sola di esse determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo.

L'operazione di annullamento è autorizzata ed eseguita a cura del Responsabile della gestione documentale su formale richiesta dell'UO che ha effettuato la registrazione.

La richiesta deve riportare il numero e la data di protocollo da annullare e i motivi dell'annullamento.

Di seguito, i casi che possono richiedere l'annullamento di una registrazione di protocollo:

- registrazioni di documenti che non sono di competenza dell'Ente;
- registrazioni prodotte erroneamente dal sistema o dai protocollari;
- registrazioni che recano documenti principali errati/non pertinenti/coerenti con i metadati di registrazione;
- doppie registrazioni di un documento.

Le informazioni relative ad un protocollo annullato rimangono comunque memorizzate nella base dati per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché gli estremi dell'autorizzazione all'annullamento del protocollo.

In tale ipotesi, la dicitura «annullato» è visibile nel dettaglio del documento sul sistema GEDOC, unitamente a tutte le informazioni originarie.

6.6 Differimento dei termini di registrazione

Fatto salvo il paragrafo 6.3, nel caso in cui, per eccezionali motivi, non sia possibile procedere alla registrazione di tutta la corrispondenza pervenuta nei termini e qualora ciò possa pregiudicare un diritto di terzi, il Responsabile della gestione documentale può autorizzare, con motivato provvedimento, l'uso del protocollo differito.

Il protocollo differito consente la normale registrazione dei documenti con l'evidenziazione della data effettiva di arrivo del documento, oltre che di quella, successiva, di registrazione.

Il provvedimento individua i documenti da ammettere alla protocollazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee, descritte dal Responsabile della gestione documentale nel provvedimento.

6.7 Registro giornaliero di protocollo

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

Il registro di protocollo è unico e la sua numerazione, unica, progressiva è costituita da almeno sette cifre numeriche. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Ai sensi dell'art. 44, comma 1-bis, del CAD e delle Linee Guida AgID, il RGD – attraverso procedura automatizzata del sistema GEDOC – entro ciascuna giornata lavorativa, produce il registro giornaliero di protocollo e lo trasmette al sistema di conservazione documentale al fine di assicurarne l'immodificabilità e l'integrità, immediatamente e in modo automatico oppure previa sottoscrizione con firma elettronica qualificata.

L'esito dell'invio e la notifica di effettiva conservazione è comunicato al sistema GEDOC mediante processi automatici.

6.8 Registro annuale di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della data e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

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

Dopo il 31 gennaio di ogni anno si provvede a trasmettere al sistema di conservazione le registrazioni del protocollo dell'anno precedente.

Dal momento che successivamente alla generazione del registro giornaliero potrebbero essere effettuate modifiche sui dati minimi di registrazione, nel registro annuale sarà riportato l'elenco di tutti i protocolli effettuati nell'anno e per ogni protocollo lo storico delle variazioni in termini di annullamento totale o parziale dei campi del protocollo.

Il registro annuale, una volta generato, segue lo stesso flusso di quello giornaliero, con spedizione immediata e automatica al sistema di conservazione dei documenti informatici oppure dopo l'apposizione della firma qualificata.

L'esito dell'invio e la notifica di effettiva conservazione sono archiviati in automatico nel sistema.

6.9 Registro di emergenza

Nel caso in cui il protocollo informatico risulti temporaneamente non utilizzabile per oltre 24 ore, o nel caso in cui la durata della sospensione del servizio sia tale da pregiudicare la registrazione a protocollo in giornata di documentazione soggetta a scadenze inderogabili e prescrittive, i documenti in entrata e in uscita devono essere registrati su un registro alternativo denominato «Registro di emergenza».

Il protocollo di emergenza è avviato, previa autorizzazione del RGD o suoi delegati.

Per la registrazione di emergenza può essere utilizzato:

- Nel caso di disponibilità dei PC un modulo predisposto in formato excel, disponibile nella intranet e compilato mediante l'immissione dei dati direttamente sulla tabella;
- Nel caso di impossibilità ad utilizzare i PC ci si avvarrà del modulo allegato al Manuale di gestione che verrà compilato manualmente.

Una volta ripristinate le normali funzionalità del sistema, il servizio di Protocollo provvede a registrare sul registro generale di protocollo i relativi protocolli di «emergenza».

Sul registro di emergenza deve essere riportata la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino delle funzionalità del sistema, ed eventuali annotazioni ritenute rilevanti dal Responsabile della gestione documentale.

Prima di autorizzare l'avvio della procedura, il Responsabile del Servizio archivistico deve impostare e verificare la correttezza di data e ora sui rispettivi registri di emergenza. Ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Il Responsabile del Servizio archivistico dovrà annotare nel protocollo informatico unico i periodi di attivazione del Registro di emergenza e, nel caso in cui nel corso dell'anno non si sia fatto ricorso al Registro di emergenza, anche il mancato uso.

Ogni documento è individuato dal numero assegnato nel Registro di emergenza, UOR, anno di registrazione, numero di protocollo nel formato stabilito.

La segnatura del protocollo di emergenza deve essere apposta mediante timbro o altro dispositivo e riportare le informazioni desunte dal relativo registro.

Una volta ripristinata la piena funzionalità del sistema, il Responsabile della gestione documentale effettua la chiusura dei registri di emergenza, e annota su ciascuno il numero di registrazioni effettuate e la data e ora di chiusura.

Il periodo massimo di autorizzazione all'utilizzo del registro di emergenza è pari ad una settimana ed in ogni caso devono essere riportati gli estremi del provvedimento di autorizzazione nel registro stesso.

La numerazione del protocollo riprende, al ripristino delle funzionalità del sistema informatico e ad ogni registrazione recuperata dal registro di emergenza sarà attribuito un nuovo numero di protocollo a partire dal numero successivo all'ultimo registrato prima dell'interruzione.

A tale registrazione sarà associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza. Di conseguenza, i documenti annotati nel registro di emergenza e trasferiti nel protocollo informatico unico saranno contraddistinti da due numeri: uno del protocollo di emergenza e uno del protocollo informatico unico. Al numero attribuito dal registro di emergenza si fa riferimento per l'avvio dei termini del procedimento amministrativo.

7 Casi particolari

7.1 Documentazione soggetta a registrazione particolare

In quanto soggetti a normativa separata, oltre al protocollo generale della Camera di commercio di Brindisi - Taranto sono in vigore:

- il protocollo del Registro Imprese;
- il protocollo dell'Albo Imprese Artigiane;
- Il protocollo dello Sportello Unico per le Attività Produttive (SUAP);
- il protocollo dell'Ufficio Protesti.

Rimane in vigore, altresì, il registro delle delibere e delle determinazioni dell'Amministrazione: a ciascuna delibera o determinazione è associato un numero di repertorio di efficacia giuridico-probatoria tramite il software che gestisce l'intero iter dei provvedimenti adottati dall'Ente.

REGISTRO DELLE DENUNCE AL REGISTRO DELLE IMPRESE E ALL'ALBO IMPRESE ARTIGIANE

Sono soggette a registrazione particolare:

- le domande di iscrizione, modifica o cancellazione dal R.I.

Tutte le altre tipologie di documento non sono soggette a registrazione particolare da parte dell'Ufficio R.I. e sono registrate nel protocollo generale dell'Ente:

- le richieste di accertamento inviate a coloro che hanno presentato le domande;
- l'invio dei suddetti accertamenti da parte dei diretti interessati;
- le richieste di visure /certificati/elenchi inviate per posta;
- l'invio di visure /certificati/elenchi;
- dichiarazioni di fallimento e tutto ciò che attiene alle procedure concorsuali (concordati preventivi e fallimentari, stato di insolvenza, liquidazioni coatte).

PRATICHE SUAP

- Segnalazione Certificata di Inizio Attività;
- Comunicazioni agli enti terzi;
- Comunicazione REA;
- Comunicazione esito REA.

DELIBERE E DETERMINAZIONI

Le delibere e le determinazioni in quanto documenti già soggetti a registrazione particolare da parte dell'Amministrazione non vanno registrati nel protocollo generale.

A ciascuna delibera o determinazione è associato un numero di repertorio di efficacia giuridico-probatoria.

Ciascun complesso delle delibere e delle determinazioni costituisce una serie.

Ciascuna serie delle delibere e delle determinazioni deve essere corredata da un proprio repertorio generale.

Nel repertorio generale va riportato un numero progressivo, denominato «numero di repertorio», che identifica il documento all'interno della serie.

Il repertorio generale ha cadenza annuale, cioè inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

REGISTRO DEI VERBALI DI SEDUTA

Le seguenti tipologie di documento sono soggette a registrazione particolare annuale progressiva da parte della Segreteria Organi Collegiali:

- verbali della Giunta Camerale;
- verbali del Consiglio Camerale.

Ciascun verbale di seduta contiene le deliberazioni adottate in quella data ed è corredata da un proprio repertorio generale.

REGISTRO DEI PROTESTI CAMBIARI

Sono soggette a registrazione particolare da parte dell'Ufficio:

- l'elenco Protesti consegnato dall'Ufficiale Levatore.

Sono soggette sia a registrazione particolare da parte dell'Ufficio sia a registrazione nel protocollo generale dell'Ente le seguenti tipologie di documenti:

- le istanze di cancellazione/riabilitazione/rettifica presentate dall'interessato;
- le istanze di annotazione consegnate dall'Ufficiale Levatore;
- le istanze di rettifica consegnate dai pubblici ufficiali incaricati alla levata dei protesti.

Non sono soggette a registrazione particolare da parte dell'Ufficio e sono registrate solo nel protocollo generale dell'Ente, tutte le altre tipologie di documento, quali, ad es.:

- le comunicazioni di avvenuta cancellazione;
- le comunicazioni di avvenuta annotazione;
- la notifica di rigetto dell'istanza;
- le comunicazioni di avvenuta rettifica;
- le comunicazioni di mancato accoglimento delle istanze;
- le richieste di regolarizzazione;
- le richieste di visure protesti da parte di enti pubblici;
- l'invio delle visure protesti ad enti pubblici;
- le istanze presentate per i rimborsi di diritti di segreteria.

7.2 Documentazione relativa a gare d'appalto

I documenti relativi alle gare svolte su portale telematico e quelli pervenuti in modalità elettronica devono essere inseriti nel sistema di gestione documentale. Qualora il portale non abbia possibilità di riversare i file della documentazione di gara o procedura negoziata direttamente nel sistema di gestione documentale, la UO dovrà provvedere a scaricarli e inserirli manualmente nei rispettivi fascicoli.

7.3 Documenti a carattere riservato, personale e/o confidenziale

La corrispondenza che rechi nell'oggetto la dicitura «personale», «riservato» e destinata al personale dipendente deve essere direttamente assegnata al destinatario il quale, dopo averne preso visione, deciderà se farla protocollare o meno.

L'addetto al protocollo che effettua la registrazione di protocollo in ingresso o in uscita attribuisce al documento il livello di riservatezza/visibilità necessario in base a criteri definiti da procedure interne o su indicazione del responsabile del documento.

L'addetto alla gestione dei fascicoli, contenenti documenti protocollati o non protocollati, attribuirà al fascicolo il livello di riservatezza/visibilità necessario in base ai criteri e alle regole di fascicolazione definite nel piano di fascicolazione. Il livello di riservatezza applicato ad un fascicolo, è acquisito automaticamente da tutti i documenti che vi confluiscono.

7.4 Lettere anonime

Tutte le lettere anonime con contenuto non pertinente ai procedimenti dell'ente devono essere sottoposte all'attenzione del Segretario generale o di persona da lui stesso delegata e, a seconda delle indicazioni ricevute, saranno protocollate specificando «Mittente anonimo», nel campo «Mittente» dell'applicazione di protocollo, oppure eliminate. È comunque garantita la protocollazione delle comunicazioni anonime inviate al Responsabile per la prevenzione della corruzione, nominato ai sensi dell'art. 1 Legge n. 190/2012.

7.5 Documenti non firmati o con firma illeggibile

I documenti non firmati per i quali è possibile individuare il mittente vengono protocollati indicando, nel sistema GEDOC, la circostanza che si tratta di «Documento privo di sottoscrizione». Nel caso in cui il documento in questione sia parte della documentazione relativa ad un determinato procedimento, l'eventuale regolarizzazione sarà disposta a discrezione del responsabile del procedimento (RdP).

Per i documenti con sottoscrizione indecifrabile e privi di ogni altro elemento utile ad identificarne il mittente, si procede alla protocollazione indicando la dicitura «Firma illeggibile» nel campo «Mittente».

7.6 Documentazione di competenza di altri uffici

Nel caso in cui pervenga erroneamente ad un Ufficio documentazione sulla quale lo stesso non abbia competenza, il responsabile dell'ufficio non competente, ove non provveda lui stesso, ne dà notizia all'ufficio protocollo che provvederà a riassegnare i documenti all'ufficio competente.

7.7 Documento inviato a più UO e/o pervenuto attraverso canali diversi

Uno stesso documento potrebbe pervenire tramite canali diversi (consegna a mano, invio postale, invio telematico) o, ancora, potrebbe essere indirizzato a più destinatari. In questi casi, l'addetto prima di protocollarlo deve verificare attraverso il sistema informatico che esso non sia già stato registrato per evitare doppie registrazioni.

Anche se pervenuto in più esemplari, un documento deve essere individuato da un solo ed unico numero di protocollo, ma qualora questo documento sia già stato registrato più volte, ai fini del calcolo dei tempi del procedimento amministrativo si dovrà tener conto della data archivistica di quello protocollato per primo.

7.8 Oggetti plurimi

Ogni documento protocollato in entrata o in uscita dovrebbe obbligatoriamente trattare un solo oggetto e riferirsi ad un unico procedimento. Nel caso in cui un documento tratti una pluralità di argomenti (pluralità di oggetti), afferenti a procedimenti diversi e a fascicoli diversi, l'addetto alla registrazione deve smistare il documento acquisito a sistema alle UO competenti che provvederanno a:

- multifascicolarlo, in modo che esso risulti agli atti in ogni fascicolo di pertinenza;
- multiclassificarlo, ove necessario, in base alla natura dei singoli procedimenti interessati.

8 Assegnazione e classificazione dei documenti

8.1 Assegnazione

L'assegnazione è l'operazione che consente di tracciare ogni passaggio del documento e dei fascicoli per competenza o per conoscenza, al fine di garantire la massima trasparenza nell'ambito di qualsiasi procedimento amministrativo.

Il dirigente/responsabile di ciascuna UO provvede ad assegnare a sé, o altro dipendente addetto all'unità, la responsabilità dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento nonché, eventualmente, dell'adozione del provvedimento finale. Fino a quando non sia effettuata l'assegnazione è considerato responsabile del singolo procedimento il funzionario preposto alla UO competente.

Tutte le assegnazioni sono tracciate dal sistema: GEDOC memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

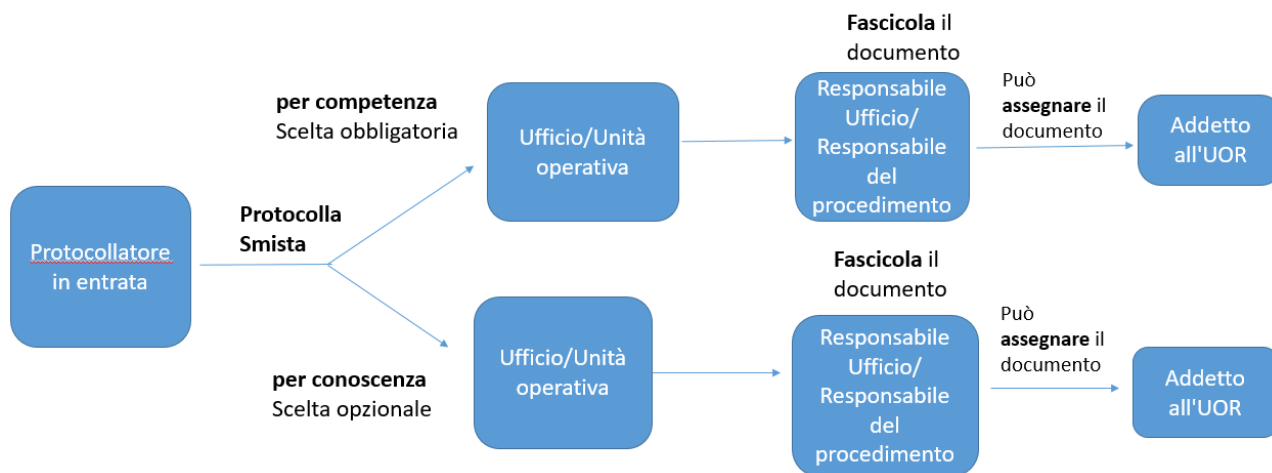


Figura 1 Flusso di smistamento e assegnazione dei documenti

I passaggi del flusso di smistamento e assegnazione sono descritti di seguito:

- a seguito della protocollazione, un documento viene smistato all'ufficio/unità operativa (UO) competente;
- con l'assegnazione del documento a un ufficio si provvede al conferimento della responsabilità del procedimento amministrativo al responsabile Ufficio, che potrà prendere in carico il documento o, a sua volta, assegnarlo ad un collaboratore (RdP) attraverso l'apposita funzione prevista da GEDOC.

Il sistema GEDOC prevede le seguenti assegnazioni:

- Assegnatario competenza (obbligatorio): identificazione dell'UO a cui è attribuita la responsabilità dei procedimenti attivati dal documento o ai quali il documento è correlato. Attraverso questa funzione, il documento verrà visualizzato nella scrivania del responsabile del procedimento (RdP)/responsabile Ufficio tra i documenti da assegnare.
- Assegnatari per conoscenza: indica le UO che, a vario titolo, possono essere interessate a conoscere un documento. Il responsabile del procedimento (RdP)/responsabile d'ufficio potrà visualizzarlo tra i documenti assegnati per conoscenza ed, eventualmente, prenderlo in carico per lavorarlo a sua volta.
- Utenti a cui è assegnata la visibilità: sono soggetti appartenenti a uno o più uffici che devono poter avere accesso a un documento. In questo caso non si tratta di una vera e propria assegnazione, pertanto il sistema non ne darà immediata evidenza, ma il documento potrà essere consultato attraverso le apposite funzioni di ricerca.

È possibile selezionare l'assegnatario dallo schema dell'organigramma reso navigabile da GEDOC. In fase di smistamento i documenti, salvo casi particolari, devono essere assegnati ad un'unica UOR di competenza

per non appesantire le successive operazioni di archiviazione e di eliminazione dei documenti dalle scrivanie degli uffici. Gli uffici scelti per conoscenza possono, invece, essere molteplici.

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

8.2 Modifica delle assegnazioni

In caso di errato smistamento l'UO assegnataria può:

- rimandare il documento al Protocollo informandolo dell'errore attraverso il campo note disponibile in GEDOC;
- smistare in autonomia la notifica ad altra UO.

Gli operatori di protocollo possono riassegnare il documento ad altra struttura di competenza.

È possibile aggiungere altri uffici in conoscenza ad un documento assegnato: possono farlo gli utenti dell'ufficio che hanno inserito il documento, ovvero ogni altro ufficio per cui il documento è in competenza. L'aggiunta di uffici assegnatari «in conoscenza» è ammessa per soli documenti «non riservati». Dalle funzioni di assegnazione del documento si possono selezionare gli uffici tra l'elenco dei possibili assegnatari per conoscenza, selezionandoli dall'organigramma dell'Ente.

8.3 Consegna dei documenti cartacei

Nel caso di ricezione di documenti cartacei (consegnati a mano o per mezzo di vettore postale), gli addetti al protocollo verificano innanzitutto la completezza della documentazione (es. corretto destinatario, presenza sottoscrizione autografa) e procedono alla scansione e alla verifica della rispondenza del documento digitalizzato (copia informatica del documento analogico) all'originale cartaceo.

Successivamente gli addetti procedono alla protocollazione, alla segnatura e all'assegnazione dei documenti, indicando nel campo Annotazioni della scheda documentale eventuali rilievi/osservazioni sulle verifiche effettuate.

La procedura di scansione e le successive verifiche di rispondenza precedono l'attestazione di conformità della copia dei documenti informatici all'originale che deve essere effettuata per il tramite dell'apposita procedura presente in GEDOC e sottoscritta mediante la firma digitale dell'operatore.

8.4 Consegna dei documenti informatici

La ricezione dei documenti informatici indirizzati all'Amministrazione è assicurata tramite caselle di posta elettronica istituzionale riservate alla protocollazione (PEC).

Nel caso in cui un documento venga ricevuto sulla PEO dell'Ufficio o personale, il destinatario deve invitare il mittente a inviare il documento alla casella di posta elettronica istituzionale agganciata in GEDOC.

Nel caso in cui l'Ufficio decidesse di accettare la PEO occorre seguire la procedura descritta nel paragrafo 5.3.

8.5 Classificazione dei documenti

La classificazione è un'attività obbligatoria che permette la corretta organizzazione dei documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'amministrazione e consente di ordinare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

Tutti i documenti, in entrata e in uscita, indipendentemente dal supporto sul quale vengono formati e dalla loro protocollazione o meno, devono essere classificati in base al Piano di classificazione adottato dall'ente [ALLEGATO 02].

Il Piano di classificazione è strutturato tenendo conto delle funzioni svolte dall'Amministrazione e non si basa sulla struttura organizzativa. Si configura come uno schema generale di «voci» articolate in modo gerarchico, partendo da quelle a carattere generale (Titoli) fino ad arrivare a quelle di carattere particolare (Classi e sottoclassi), al fine di identificare secondo uno schema logico i documenti e i fascicoli.

Classificare vuol dire attribuire, in fase di inserimento di un documento informatico in GEDOC, o in seguito alla sua assegnazione nel caso si tratti di un documento in entrata, un indice di classificazione desunto dal Piano di classificazione. La classificazione è propedeutica all'attività di fascicolazione e uno stesso documento può essere classificato più volte, in base alla molteplicità di funzioni individuate, e associato a più fascicoli.

Eventuali modifiche alla classificazione di un documento sono possibili da parte degli utenti abilitati alla funzione e sono tracciate nel sistema.

La revisione, anche parziale, del Piano di classificazione viene proposta dal RSP quando necessario ed opportuno. Dopo ogni modifica il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Le eventuali modifiche e integrazioni entrano in vigore, salvo casi eccezionali, il 1° gennaio dell'anno seguente.

Il Piano di classificazione non è retroattivo: non si applica, cioè, ai documenti archiviati prima della sua introduzione.

9 Fascicolazione dei documenti

9.1 Formazione dei fascicoli

L'archivio è il complesso dei documenti prodotti o comunque acquisiti da un ente durante lo svolgimento della propria attività.

Ai sensi dell'art. 52 del D.P.R. 28 dicembre 2000, n. 445 il sistema di gestione informatica dei documenti deve:

- garantire la sicurezza e l'integrità del sistema;
- garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;

- fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- consentire il reperimento delle informazioni riguardanti i documenti registrati;
- consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

All'interno dell'archivio il documento non è considerato come unità, ma connesso ad un contesto. L'unità minima più comunemente diffusa in un archivio è il fascicolo.

Tutti i documenti registrati nel sistema informatico e classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli, ad eccezione di tutto quanto attiene i materiali preparatori e di lavoro per arrivare alla formazione del documento (bozze, proposte, primi elaborati, report di controllo, appunti ecc.). Nel sistema di gestione documentale si collocano solo i documenti nella loro versione definitiva, salvo casi in cui ci siano particolari esigenze di tenere traccia di alcuni passaggi nella formazione del documento o di dividerne il contenuto già in questa forma con altri.

La fascicolazione è l'attività attraverso cui un documento viene ricondotto logicamente all'interno dell'unità archivistica assieme ai documenti precedenti, e che mantiene vivo il vincolo archivistico che lega ogni singolo documento alla pratica di cui fa parte (ordine cronologico di sedimentazione). Questa attività permette di costruire un sistema basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore dell'archivio. La fascicolazione è obbligatoria per tutti i documenti, anche quelli non protocollati.

Il fascicolo è lo strumento operativo per organizzare i documenti all'interno di un archivio ed è l'unità primaria e fondamentale di conservazione dei documenti. Esso costituisce la raccolta ordinata della documentazione prodotta e accumulata nel corso della trattazione di un affare/procedimento o riguardante un determinato oggetto.

I fascicoli si aprono al livello più basso del Piano di classificazione (classe o sottoclasse) e non costituiscono un ulteriore livello.

Ai sensi dell'art. 41 del CAD, il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dalle Linee Guida AgID, assicurando la possibilità di essere direttamente consultato e alimentato dalle amministrazioni che partecipano al procedimento. Il fascicolo informatico è costituito in modo da garantire l'accessibilità in corso di procedimento alle amministrazioni coinvolte e l'accesso in via telematica agli interessati.

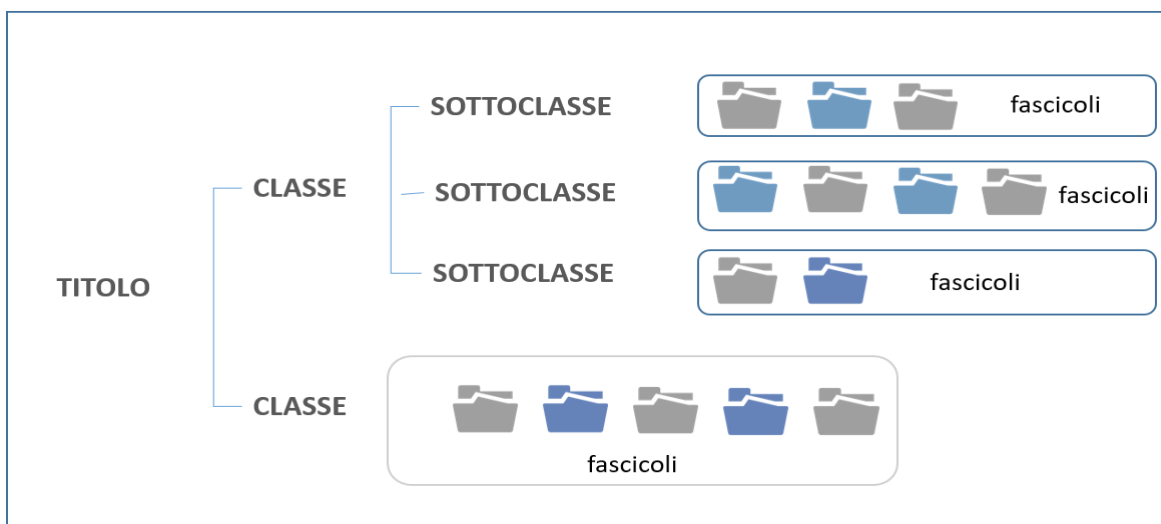


Figura 2 Piano di fascicolazione – schema

Il Repertorio dei fascicoli

Ogni fascicolo formato viene registrato nel repertorio dei fascicoli, che è il registro cronologico nel quale vengono progressivamente annotati, secondo l'ordine di formazione, tutti i fascicoli presenti nell'archivio.

Il numero di repertorio è composto da: .

Presso ciascuna AOO è istituito un unico repertorio dei fascicoli.

Il repertorio contiene le seguenti informazioni:

- l'anno di creazione del fascicolo;
- il numero di repertorio del fascicolo;
- il codice di classificazione;
- l'eventuale presenza di sottofascicoli, ed il numero dei documenti contenuti nel fascicolo;
- la descrizione del fascicolo;
- l'ufficio di competenza e il Responsabile del Fascicolo;
- la data di apertura (data di creazione) e chiusura del fascicolo;
- lo stato del fascicolo (aperto/chiuso/Eliminato o Spostato).

Annualmente il sistema di gestione documentale GEDOC genera il Repertorio Fascicoli in formato PDF e lo invia automaticamente in conservazione.

9.2 Tipologie di fascicolo

I fascicoli possono essere suddivisi in tipologie che variano a seconda della natura dei documenti da inserire e della loro organizzazione interna. Le tipologie di fascicoli sono cinque:

Fascicolo procedimentale

Il fascicolo procedimentale è un fascicolo che raccoglie tutta la documentazione relativa a un procedimento amministrativo e, in base alla complessità e alla numerosità della documentazione prodotta, può essere articolato in sottofascicoli che rispecchiano le fasi del procedimento. Nella generalità dei casi esse sono:

- fase dell'iniziativa;
- fase istruttoria;
- fase costitutiva;
- fase integrativa dell'efficacia.

La durata di un fascicolo per procedimento equivale alla durata del procedimento stesso.

Fascicolo per affare

Il fascicolo per affare raggruppa in un unico fascicolo i documenti relativi ad una competenza che non prevede l'adozione di un provvedimento finale. Può essere articolato in sottofascicoli in base alla complessità e alla numerosità della documentazione prodotta e la sua durata può essere pluriennale.

Fascicolo per attività

Il fascicolo per attività è costituito dai documenti prodotti nel corso dello svolgimento di attività semplici, che non afferiscono a un procedimento amministrativo e non richiedono l'istruzione di un fascicolo per affare, esaurendosi in risposte obbligate o in meri adempimenti di legge.

Il fascicolo per attività si apre e si chiude nell'ambito dell'anno di gestione.

Fascicolo di persona fisica

È anche conosciuto come fascicolo per oggetto o nominativo o persona e si utilizza per raggruppare tutti i documenti relativi ad una persona fisica, anche relativi a procedimenti diversi.

Tipico è il caso dei fascicoli del personale, dove tutta la documentazione di un dipendente è racchiusa in un fascicolo, suddiviso a sua volta in sottofascicoli.

La durata del fascicolo per persona fisica è in genere pluriennale, in quanto legata alla durata della relativa materia/oggetto.

Fascicolo di persona giuridica

Il fascicolo di persona giuridica, come il precedente, conserva documenti relativi a diversi procedimenti amministrativi, distinti affari o diverse attività, ma legati da un vincolo archivistico interno, relativo ad una persona giuridica.

Anche i fascicoli intestati alle persone giuridiche possono avere durata pluriennale.

9.3 Struttura gerarchica del fascicolo

Un fascicolo può essere articolato in sottofascicoli, e questi in inserti, con l'obiettivo di facilitare la gestione, l'accessibilità, il reperimento e la selezione della documentazione in esso contenuta.

Le buone prassi archivistiche sconsigliano di andare oltre nella suddivisione del fascicolo, cosa che avrebbe l'effetto di appesantire il governo della documentazione.

Alcune tipologie di fascicoli rendono necessaria la suddivisione dei documenti in modo articolato a causa della quantità, dell'articolazione del loro contenuto, delle varie fasi del procedimento cui afferiscono, del livello di riservatezza attribuito alla documentazione e delle differenze nei tempi di conservazione: un fascicolo può contenere, infatti, documentazione con una valenza temporale limitata e documenti soggetti a conservazione illimitata.

Sono riportati, di seguito, alcuni esempi che non devono, tuttavia, essere interpretati in modo rigido.

Fascicoli relativi ad eventi, iniziative, progetti

Si tratta di fascicoli per affare che possono avere durata pluriennale e possono essere articolati in sottofascicoli relativi a ciascuna fase dell'iniziativa, anche se si tratta di fasi non standardizzate come quelle di un procedimento.

Fascicoli relativi a organismi

Si tratta di un fascicolo che gestisce l'organizzazione/gestione di un organismo (ad esempio Gruppi di lavoro, commissioni ecc.).

Per gli organismi complessi si può considerare un'articolazione in sottofascicoli, ad esempio:

- Parte istituzionale: costituzione, funzionamento, normativa e organi (deleghe)
- Attività e funzionamento: riunioni degli organi, atti e verbali
- Gestione iter elaborazione, progettazione e organizzazione: corrispondenza, documenti istruttori, bozze preparatorie
- Progetti e azioni specifiche: progetti, proposte, interventi

Un caso particolare riguarda la documentazione prodotta dai cosiddetti «tavoli o gruppi di studio», che consta solitamente di report relativi all'analisi di determinati fenomeni.

Nel caso in cui queste attività abbiano una cadenza periodica, è possibile creare un fascicolo per ciascun gruppo. Nel caso in cui la cadenza fosse episodica, la documentazione potrebbe essere organizzata in fascicoli per iniziativa.

Bandi per contributi

Si tratta di fascicoli procedurali che possono articolarsi in sottofascicoli relativi a:

- Gestione generale del bando
- Richieste di contributo, istruttoria e valutazione ammissibilità
- Comunicazione esito richiesta
- Comunicazione liquidazione contributo
- Rendicontazione contributo e esiti attività
- Visite ispettive e controlli

Fascicoli personali

I fascicoli del personale sono destinati alla conservazione permanente e si riferiscono al personale in servizio e in quiescenza, di ruolo e non di ruolo. Essi sono relativi a ciascun dipendente e hanno una strutturazione interna articolata e complessa.

I sottofascicoli possono essere creati in base alle varie fasi del rapporto di lavoro, a quelle della gestione dell'aspetto economico o dell'aspetto normativo.

9.4 Processo di identificazione e formazione dei fascicoli

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, di un'attività istruttoria, di un'attività continuativa, anche relativa a un soggetto giuridico o a una persona fisica (es. personale), il funzionario preposto provvede all'apertura di un nuovo fascicolo.

I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, di un sottofascicolo/inserto, secondo l'ordine cronologico di registrazione.

Con la formazione di un nuovo fascicolo si provvederà a registrare nel sistema informatico le seguenti informazioni:

- indice di classificazione;
- numero del fascicolo (assegnato automaticamente dal sistema);
- oggetto del fascicolo;
- data di apertura (assegnata automaticamente dal sistema);
- responsabile del procedimento.

Quando i documenti vengono associati al fascicolo ne assumono la voce di classificazione, se non già attribuita a livello di documento.

L'oggetto (o descrizione) del fascicolo deve essere strutturato secondo criteri uniformi e condivisi per evitare:

- inefficienza nella ricerca;
- difformità nella redazione dell'oggetto di fascicoli omologhi;
- difficoltà a identificare il contenuto di un fascicolo.

Il Piano di fascicolazione adottato dalla Camera di Commercio propone un'organizzazione delle informazioni costruita intorno alle seguenti regole:

- le informazioni devono seguire una gerarchia dal generale al particolare;
- è bene evitare singole parole generiche (indagini, ricerche, attestazioni, certificazioni, comunicazioni ecc.);
- si devono utilizzare brevi frasi di senso compiuto che forniscano indicazioni chiare sul contenuto del fascicolo (ovvero l'affare / attività / procedimento amministrativo ecc.);
- si devono inserire nella descrizione le «parole chiave», laddove possibile;
- nel caso di fascicoli che si ripetono nel tempo, indicare l'anno di riferimento (o altre informazioni distintive) per differenziarli;
- la descrizione di un fascicolo deve essere sempre diversa da quella di un altro.

Per evitare duplicazioni è fortemente consigliato procedere posizionandosi sulla corrispondente voce di titolare nella sezione «gestione fascicoli», così da verificare la presenza di fascicoli già creati per il medesimo affare/procedimento, anche predisposti da altro ufficio che concorre al medesimo procedimento, che è possibile condividere.

In fase di creazione di nuovi fascicoli è fatto obbligo di inserire il tempo di conservazione corrispondente alla classifica, previa consultazione del massimario di selezione.

9.5 Alimentazione dei fascicoli

I fascicoli correnti sono conservati nel sistema di gestione documentale e possono essere alimentati dal responsabile del fascicolo, da eventuali suoi incaricati, oppure da una o più UO nell'ambito dello stesso procedimento amministrativo.

Il fascicolo deve essere chiuso al termine del procedimento amministrativo, dell'istruttoria o dell'attività cui si riferisce, oppure su base temporale (per esempio alla fine dell'anno solare se si tratta di un fascicolo di attività).

In caso di chiusura di un numero significativo di fascicoli è possibile chiedere al Responsabile del protocollo (RdP) la chiusura massiva.

Ai fini della corretta tenuta dell'archivio il Responsabile del protocollo avrà il compito di verificare periodicamente la corretta tenuta dei fascicoli da parte delle UO e di sollecitare la chiusura dei fascicoli ingiustificatamente non chiusi o l'eliminazione di fascicoli duplicati. In caso di inerzia da parte dell'utente creatore, sarà obbligo del RdP informare il Segretario generale per l'adozione di atti formali.

È fatto obbligo altresì di fascicolare tempestivamente i documenti per consentire la completezza delle operazioni di fascicolazione e consultazione dell'archivio.

9.6 Conservazione dei fascicoli

I documenti e i fascicoli sono archiviati sul sistema informatico GEDOC ed inviati automaticamente al sistema di conservazione, sulla base delle regole stabilite nel Manuale di conservazione.

I fascicoli vengono inviati in conservazione dopo 30 giorni dalla chiusura.

Il sistema di gestione documentale mantiene in forma di duplicato i fascicoli e i documenti già inviati in conservazione finché essi sono necessari allo svolgimento delle attività, pertanto è possibile continuare a consultare il contenuto di un fascicolo anche dopo il suo invio in conservazione.

9.7 Gestione dello scarto

Lo scarto di documenti degli archivi della pubblica amministrazione è soggetto alla preventiva autorizzazione della Soprintendenza archivistica, secondo quanto disposto dall'art. 21, comma 1, lettera d) del Codice dei Beni Culturali.

Il Piano di conservazione stabilisce le tempistiche di conservazione e di scarto tenendo conto sia della normativa di riferimento sia dell'analisi interna effettuata dal RGD, congiuntamente con le UOR responsabili del trattamento dei documenti.

I termini minimi di conservazione vanno intesi dalla data di chiusura del fascicolo in via generale, salvo contenzioso in essere, e sono periodicamente verificati alla luce di nuove possibili normative di settore che obbligano ad un periodo di conservazione maggiore rispetto a quello indicato alla data di emanazione del Piano di conservazione dei documenti.

Le modalità di scarto dei documenti e dei fascicoli elettronici contenuti nei pacchetti di archiviazione sono concordate tra la Camera di commercio e il Conservatore (InfoCamere) e descritte nel Manuale di conservazione del Conservatore.

Periodicamente, il Responsabile della gestione documentale predispone, con propria determinazione, l'elenco del materiale documentario da scartare, al fine di ottenere la necessaria autorizzazione della Soprintendenza archivistica competente.

Il Responsabile della gestione documentale invia alla Soprintendenza archivistica una lettera formale con la richiesta di autorizzazione allo scarto di atti d'archivio, accompagnata da un elenco dettagliato della documentazione che intende eliminare, in duplice copia.

L'elenco deve contenere almeno i seguenti dati:

- tipologia dei documenti da scartare e relativo indice di classificazione;
- estremi cronologici della documentazione;
- numero dei pezzi, da quantificare in buste, registri, scatole, metri lineari etc.;
- peso (in Kg per la documentazione analogica, KB, MB ecc. per quella digitale);
- motivazione della proposta di scarto.

Dopo un attento esame, che comprende il raffronto con le indicazioni del Piano di conservazione, la Soprintendenza può autorizzare la distruzione integrale o parziale dei documenti indicati nell'elenco, ovvero respingere la richiesta sulla base di motivazioni che verrebbero di volta in volta esposte.

La Soprintendenza ha l'obbligo di concludere il procedimento entro il termine di 60 giorni dalla ricezione della proposta, fatte salve eventuali richieste di ulteriori informazioni circa i materiali che si intendono scartare, che sospenderebbero la decorrenza del termine.

Qualora l'autorizzazione venga rilasciata, la documentazione analogica da eliminare dovrà essere consegnata a una ditta specializzata o ad altre organizzazioni che ne garantiscano in modo certo la distruzione. Particolare attenzione dovrà essere posta ai documenti contenenti dati sensibili, che dovranno essere salvaguardati ai sensi della vigente normativa sulla privacy e dei quali si dovrà evitare ogni possibile uso improprio.

Nel caso di documentazione digitale, la richiesta di scarto e il conseguente provvedimento autorizzatorio dovranno essere trasmessi al Conservatore affinché provveda alla distruzione della documentazione contenuta nei pacchetti di archiviazione.

L'operazione di scarto viene tracciata sul sistema di conservazione mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e la sua autorizzazione.

Il verbale di avvenuta distruzione dei documenti, rilasciato dal soggetto incaricato della distruzione della documentazione (sia essa analogica o digitale), dovrà essere trasmesso alla Soprintendenza archivistica entro 60 giorni, per la conclusione del procedimento.

I documenti e i fascicoli sottoposti a scarto nel sistema di conservazione saranno eliminati anche dal sistema di gestione documentale e dagli altri applicativi integrati.

Il Piano di conservazione è riportato nell'allegato 03.

10 Scansione dei documenti cartacei

Tutti i documenti di rilievo per l'Ente devono essere inseriti e gestiti nel sistema di gestione documentale che rappresenta l'archivio unico informatico. Pertanto, la documentazione cartacea pervenuta in Camera di Commercio deve essere convertita in digitale mediante processi e strumenti che assicurino che i documenti informatici abbiano contenuto e forma identici a quelli dei documenti analogici da cui sono tratti, come previsto dall'art. 22 del CAD.

Per assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto sono previste dalla normativa due modalità:

- Raffronto dei documenti e relativa certificazione di conformità;
- Certificazione di processo mediante tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

10.1 Processo di scansione e certificazione di conformità

Il procedimento di scansione dei documenti analogici e di apposizione della certificazione di conformità si articola nelle seguenti fasi:

- scansione del documento analogico ed ottenimento di un file PDF. Ad un documento, anche composto da più pagine, deve corrispondere un unico file;
- verifica della correttezza dell'acquisizione delle immagini mediante raffronto con l'originale;
- redazione dell'attestazione di conformità del documento informatico al documento analogico da cui è tratto, generata nell'ambito del sistema GEDOC;
- apposizione della firma digitale al documento così ottenuto da parte del personale a ciò autorizzato.

Gli utenti abilitati provvedono alla scansione dei documenti secondo le opzioni previste dalla procedura, ovvero all'acquisizione diretta tramite scanner del file in formato PDF salvandolo in una directory interna e riservata alla Camera, accessibile dall'operatore che procederà all'acquisizione in GEDOC del documento. È a carico dell'operatore la verifica visiva della corrispondenza in termini di contenuti tra il documento originale analogico e il documento scansionato.

Il documento informatico così prodotto viene inserito come documento in ingresso nel sistema di gestione documentale, che chiederà all'utente di specificare il formato del documento originale. In questo caso, l'utente dovrà selezionare «cartaceo».

Il sistema attribuirà al documento i metadati minimi obbligatori, tra cui l'impronta che viene generata in automatico dal sistema e l'operatore provvederà a inserire i metadati previsti.

Effettuata l'acquisizione del documento, il sistema di gestione documentale verifica il formato del file acquisito (PDF/A), conta il numero di pagine e produce un documento in formato PDF/A di contenuto identico, ma con l'aggiunta in ultima pagina dell'attestazione di conformità, con l'evidenza del pubblico ufficiale/funzionario che la firmerà digitalmente.

Il documento da firmare digitalmente è, quindi, comprensivo sia dei contenuti del documento analogico originale, che dell'attestazione di conformità.

La firma digitale dell'attestazione di conformità è permessa a utenti ai quali è stato attribuito uno specifico ruolo funzionale del sistema di gestione documentale.

Il documento informatico così prodotto viene inserito come documento in ingresso nel sistema di gestione documentale con l'attribuzione dei metadati minimi obbligatori, tra cui l'impronta del documento che viene generata in automatico dal sistema.

Nel caso in cui il pubblico ufficiale/funziionario che firmerà il documento digitalizzato munito di attestazione di conformità sia diverso dall'operatore che ha provveduto alla scansione/acquisizione, dovranno essere inviati al firmatario sia il documento informatico, che l'originale analogico. Dopo la firma dell'attestazione di conformità, il documento analogico dovrà essere archiviato nell'archivio cartaceo, mentre il documento informatico seguirà il proprio flusso di protocollazione (se richiesto) e il sistema apporrà la segnatura di protocollo nella parte alta del documento.

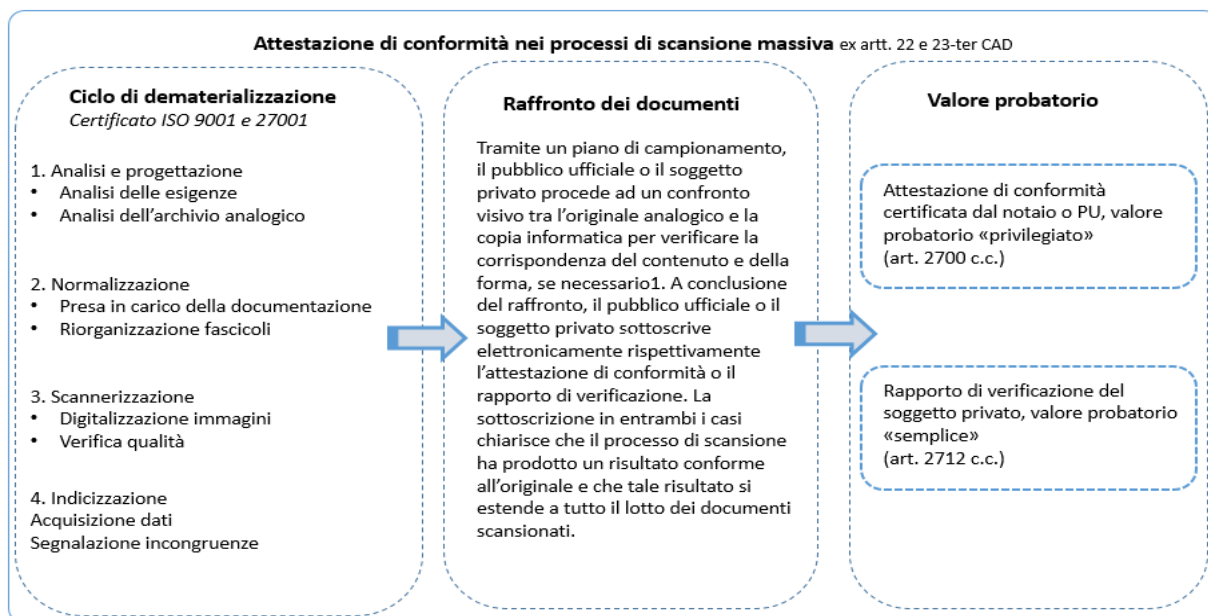
10.2 Certificazione di processo

La certificazione di processo è stata introdotta dal legislatore con la finalità di favorire la dematerializzazione di grosse quantità di documenti analogici.

La procedura deve essere conforme agli standard ISO 9001 e 27001 e a quanto riportato nell'allegato 5 delle Linee Guida AgID.

L'attestazione di conformità delle copie-campione passa necessariamente attraverso il metodo del raffronto tra originale e copia, attività che deve essere svolta dal personale autorizzato perché finalizzata all'attestazione:

- dei requisiti tecnici essenziali di leggibilità del documento immagine risultato della scansione;
- di garanzia dell'integrità del contenuto;
- di completezza del processo di scansione.



11 Gestione documenti cartacei degli archivi di deposito

L'archivio di deposito è costituito dai documenti relativi ad affari e a procedimenti amministrativi di cui è terminata la trattazione e che richiedono un accesso poco frequente. Nell'archivio di deposito vengono effettuate le operazioni di selezione e scarto della documentazione in base ai criteri indicati nel Piano di conservazione:

- i documenti digitali relativi ad affari conclusi sono archiviati in GEDOC e nel Sistema di conservazione;
- i documenti originali cartacei, acquisiti o meno nel sistema di gestione documentale come copie digitali, devono essere archiviati e conservati secondo le modalità descritte di seguito e per i tempi previsti dal Piano di conservazione.

11.1 La movimentazione dei fascicoli

Per la consultazione dei fascicoli custoditi nell'archivio di deposito è necessario inviare una richiesta scritta (a mezzo PEO) sulla quale devono essere indicati gli estremi di riferimento del materiale da consultare; il ritiro della documentazione richiesta viene annotato su un apposito registro, sul quale verrà poi annotata anche la definitiva restituzione del materiale consultato.

11.2 Gestione dell'archivio storico

Nell'archivio storico vengono conservati tutti quei fascicoli, non più utilizzati, risalenti ad un periodo pari o superiore ai 40 anni dalla loro definizione.

Per la consultazione dei fascicoli custoditi nell'archivio storico è necessario inviare una richiesta scritta e motivata (a mezzo PEO) sulla quale devono essere indicati gli estremi di riferimento del materiale da consultare.

Non sono consentiti prelievi documentali.

12 Accesso ai documenti e tutela della riservatezza

La Camera di commercio di Brindisi - Taranto orienta la propria azione al perseguimento di obiettivi di imparzialità e trasparenza, promuove e garantisce l'esercizio del diritto di accesso alla documentazione amministrativa detenuta dai propri uffici, in conformità ai principi vigenti in materia di accesso e di protezione dei dati personali.

Il diritto di accesso ai documenti, alle informazioni e ai dati detenuti dall'amministrazione è disciplinato dalla Legge n. 241/90; dal D.Lgs. n. 33/2013 e dal Regolamento per l'esercizio del diritto di accesso documentale della Camera di commercio pubblicato sul sito web istituzionale dell'Ente, nella sezione Amministrazione Trasparente, nel quale sono individuate le categorie di documenti sottratti all'accesso.

Per ciascuna richiesta di accesso l'amministrazione riporta l'oggetto, la data dell'istanza e il relativo esito con la data della decisione in un registro, pubblicato e aggiornato semestralmente nella sezione Amministrazione trasparente, avendo cura di omettere la pubblicazione di dati personali eventualmente presenti.

12.1 Amministrazione trasparente

Come prescritto dalla normativa in tema di trasparenza e accesso civico la Camera di commercio di Brindisi - Taranto ha costituito la sezione di «Amministrazione trasparente» nel sito istituzionale, nella quale sono pubblicate le informazioni soggette a obbligo di pubblicità, indicate nel Decreto legislativo n. 33 del 14 marzo 2013 e successive modifiche recante «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni», e le altre informazioni soggette a obbligo di pubblicità.

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

13 Disposizioni finali

Le disposizioni contenute nel Manuale devono essere adottate a partire dal giorno successivo a quello della pubblicazione della determina di approvazione all'Albo camerale informatico.

Per quanto non espressamente previsto dal manuale, si fa riferimento alla normativa vigente in materia, adottando comportamenti ispirati al principio del buon andamento dell'attività amministrativa.

Il RGD, in attuazione del presente documento, ha il compito di:

- a) proporre o redigere progetti speciali tendenti alla valorizzazione dei documenti della Camera di commercio, alla conservazione, alla sicurezza dei locali di deposito e a quant'altro possa migliorare l'attività istituzionale inerente agli archivi;
- b) proporre iniziative di formazione e aggiornamento professionale.

ELENCO ALLEGATI

- 1) Manuale utente applicativo GEDOC;
- 2) Piano di classificazione;
- 3) Piano di fascicolazione e conservazione;
- 4) Elenco applicative integrati;
- 5) Modello Registro di emergenza
- 6) Provvedimento annullamento registrazione;
- 7) Provvedimento differimento termini di registrazione;
- 8) Modello attestazione di conformità