CONSORZIO DI AREA VASTA CB16

MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE

SOMMARIO

Sommario

PARTE PRIMA – DISPOSIZIONI PRELIMINARI 2
PARTE SECONDA – ORGANIZZAZIONE 3
PARTE TERZA – FORMAZIONE DEI DOCUMENTI 6
Sezione prima – Modalità di formazione 6
Sezione seconda – Disposizioni comuni a tutte le modalità di formazione 10
Sezione terza - Disposizioni sulla formazione di documenti analogici 12
PARTE QUARTA - GESTIONE DOCUMENTALE 14
Sezione prima - Flussi documentali esterni 14
Sezione seconda - Protocollo informatico 17
Sezione terza – Classificazione e fascicolazione 25
PARTE QUARTA – CONSERVAZIONE DEI DOCUMENTI 26
PARTE QUINTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI 27

ALLEGATI

Allegato 1. Organigramma con indicazione delle UO
Allegato 2. Manuali operativi degli strumenti software
Allegato 3. Piano di classificazione (Titolario)
Allegato 4. Guida alla formazione del documento accessibile
Allegato 5. Indicazioni sulla formazione dei documenti
Allegato 6. Piano di conservazione (Massimario di selezione e scarto)
Allegato 7. Piano di fascicolazione
Allegato 8. Gestione dei protocolli riservati

Approvato con deliberazione del Cda n. 22 del 31/10/2023

PARTE PRIMA – DISPOSIZIONI PRELIMINARI

1. Riferimenti normativi

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

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

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

Ulteriori norme rilevanti ai fini della gestione documentale sono:

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

- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 *"Regolamento generale sulla protezione dei dati"* ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

2. Finalità, contenuti e metodologia del documento

Il presente Manuale, ai sensi del paragrafo 3.5. delle Linee guida, descrive il sistema di gestione informatica dei documenti del Consorzio e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi, ivi compresa la conservazione dei documenti informatici.

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell'ente. Sono da considerarsi modifiche sostanziali quelle aventi a oggetto il Piano di classificazione (Titolario) e il Piano di conservazione dei documenti.

Il Manuale, di cui è prevista la pubblicazione, costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

3. Approvazione e modalità di aggiornamento del Manuale

Il presente Manuale e i suoi allegati sono approvati con delibera del CdA del Consorzio, su proposta del Responsabile della gestione documentale dell'ente.

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

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

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea e Unità Organizzative

Il Consorzio si configura come un'unica Area Organizzativa Omogenea ("AOO") denominata "CONSORZIO DI AREA VASTA CB 16" . L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

Le Unità Operative (UO) che afferiscono alla AOO sono riportate nell'**Allegato 1**, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa del Consorzio. Le UO sono individuate in modo da rispecchiare l'organigramma dell'ente.

5. Responsabile della gestione documentale

Il Consorzio, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura direttiva, il "Responsabile della Gestione Documentale" (d'ora in avanti anche solo "**Responsabile**" o "**RGD**"), nella figura del Direttore o, in sua assenza, nel Responsabile dell'Area di competenza.

I compiti del Responsabile sono definiti nell'atto di nomina. In particolare, il Responsabile:

a) è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica del Consorzio;
b) provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
c) monitora i processi e le attività che governano le fasi di formazione e gestione dei documenti informatici e definisce, d'intesa con il Responsabile della conservazione, i formati da adottare per la formazione e i metadati, ulteriori a quelli obbligatoriamente previsti dall'allegato 5 alle Linee Guida AgID, da associare al fine di assicurare la corretta conservazione nel tempo dei documenti informatici;
d) assicura la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione;
e) valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
f) vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo e produzione del registro giornaliero di protocollo;
g) assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati;
h) effettua un periodico censimento degli strumenti software di gestione documentale in uso presso il Consorzio e, di concerto con il RTD, ne verifica la conformità alla normativa vigente.

Ulteriori e specifici compiti del Responsabile sono indicati nei provvedimenti che istituiscono il servizio per la tenuta del protocollo informatico, nel provvedimento di nomina e nelle sezioni pertinenti del presente Manuale, ovvero nel manuale di conservazione dell'Ente.

Il RGD, ferma restando la propria responsabilità, può delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

6. Sistema informatico di gestione documentale del Consorzio

Il Consorzio, per la gestione documentale, si avvale di un apposito sistema software gestionale (d'ora in avanti "**Sistema**"), che garantisce le seguenti funzionalità, tra loro integrate:

- acquisizione dei documenti informatici provenienti da caselle PEC e strumenti web di acquisizione delle istanze online;
- protocollazione dei documenti e tenuta del protocollo informatico;
- sistema di workflow per l'assegnazione, lo scambio e la lavorazione dei documenti da parte degli uffici;
- creazione e gestione dei fascicoli informatici;
- gestione dell'iter di approvazione di approvazione degli atti amministrativi;
- pubblicazione degli atti in albo pretorio e nella sezione amministrazione trasparente deli sito istituzionale.

La puntuale descrizione delle componenti e delle modalità di funzionamento del Sistema è riportata nei relativi manuali operativi del software, di cui all'**Allegato 2** al presente Manuale.

7. Abilitazioni di accesso

Le abilitazioni di accesso degli utenti alle componenti del Sistema informatico di gestione documentale del Consorzio sono assegnate personalmente a ciascun dipendente dall'Amministratore, su indicazione di ciascun Responsabile di Area entro cui è inquadrato il dipendente e vengono rilasciate dall'Amministratore di Sistema.

A ciascun utente del Sistema, pertanto, sono attribuite specifiche funzioni, diversificate in ragione dell'appartenenza a un determinato settore dell'organizzazione o dell'assunzione di specifici ruoli e compiti.

Tutti gli utenti potranno consultare i documenti presenti in protocollo, ad eccezione dei documenti riservati, che potranno essere consultati solo dagli utenti identificati dall'UP nella fase di protocollazione.

Eventuali richieste di consultazione di documenti riservati da parte degli utenti potranno essere presentate al proprio Responsabile di Area che, a sua volta, farà formale richiesta al RGD.

Tutti i documenti relativi ai processi elencati nell'**Allegato 8** saranno oggetto di protocollazione riservata.

8. Soggetti delegati alle attività di protocollazione

Tutti i dipendenti a cui è assegnata un'utenza per l'abilitazione d'accesso al Sistema informatico di gestione documentale del Consorzio, sono abilitati alla protocollazione informatica dei documenti in uscita (con esclusione degli utenti a cui sono attribuite funzioni di mera consultazione).

La protocollazione dei documenti informatici in entrata è, invece, centralizzata ed è curata dal personale dell'Ufficio Protocollo (di seguito anche "**UP**"), che, di norma, provvede alla protocollazione di tutti i documenti informatici acquisiti dal Consorzio.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Sezione prima – Modalità di formazione

9. Modalità di formazione dei documenti informatici

Tutti i documenti del Consorzio sono formati in originale come documenti informatici, secondo le modalità individuate nella presente Parte del Manuale.

I documenti informatici degli uffici del Consorzio sono formati mediante una delle seguenti modalità:

a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati (ad esempio, mediante programmi di scrittura delle suite *Microsoft Office* o *Libre Office*, o mediante l'utilizzo delle funzioni dei sistemi di gestione documentale);
b) acquisizione:
   - della copia per immagine di un documento analogico su supporto informatico (ad esempio, mediante scansione di documento cartaceo);
   - della copia informatica di un documento analogico (ad esempio, acquisizione del documento tramite lettore OCR);
   - del duplicato di un documento informatico per via telematica o da supporto informatico (ad esempio, mediante download da posta elettronica o da chiave usb);
c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici, oppure delle informazioni risultanti dall'acquisizione telematica di dati attraverso moduli o formulari resi disponibili all'utente (ad esempio, memorizzazione dei dati immessi in un *form* reso disponibile online agli utenti);
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni secondo una struttura logica predeterminata e memorizzata in forma statica (ad esempio, generazione del registro di protocollo giornaliero).

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopra descritte

9.1. Creazione e redazione tramite software di documenti informatici

Gli uffici del Consorzio dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Microsoft Office*: *Word, Excel, PowerPoint, Outlook, ecc.*

Il testo del documento informatico creato dagli uffici del Consorzio deve essere redatto utilizzando esclusivamente uno dei seguenti font Arial*

9.2. Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dal Consorzio deve recare obbligatoriamente i seguenti elementi:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. oggetto del documento;
4. sottoscrizione;
5. data e luogo;
6. numeri di pagina;
7. indicazione degli allegati (se presenti);
8. identificazione e dati dei destinatari (se si tratta di documento in uscita);
9. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
10. mezzo di spedizione (se documento in uscita);
11. indicazione del livello di riservatezza del documento.

9.3. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dal Consorzio deve essere scelto tra i seguenti **formati standard**: **.pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods**. Inoltre:

- per le **immagini vettoriali** devono essere adottati i seguenti formati: **.dwg, .dwfx, .dwf, .svg, .svgz**;
- per le **immagini raster** devono essere adottati i seguenti formati: **.png .jpg, .jpeg, .tiff**;
- per i **dati strutturati** devono essere adottati i seguenti formati: **.sql, .accdb.**

Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico, in ogni caso, deve essere preferibilmente individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID ed adottato osservando le raccomandazioni ivi contenute.

Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio,

.docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Presidente e degli organi collegiali, i contratti, le determine a contenuto provvedimentale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). Anche al fine di facilitare la visualizzazione da parte degli utenti, i documenti in formato PDF e PDF/A sono sottoscritti con firma PADES o CADES. Si precisa che, dal punto di vista giuridico, entrambe le tipologie di firma (PADES e CADES) sono idonee a garantire l'autenticità dei documenti informatici sottoscritti.

Nel caso il documento definitivo sia di un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (.p7m).

9.4. Acquisizione di documenti informatici

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

a) acquisizione di un documento informatico per via telematica o su supporto informatico (ciò avviene, ad esempio, quando si effettua il download di un documento dalla casella di posta elettronica, oppure, quando si trasferisce un documento da un dispositivo di archiviazione esterno, come una penna usb);

b) acquisizione della copia per immagine su supporto informatico di un documento analogico (ciò avviene, ad esempio, quando si effettua la scansione di un documento cartaceo, memorizzandolo in un formato digitale);

c) acquisizione della copia informatica di un documento analogico (ciò avviene, ad esempio, quando un documento di testo analogico viene riversato in formato digitale tramite lettore OCR per il riconoscimento ottico dei caratteri).

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), al fine di assicurarne l'efficacia giuridico-probatoria, occorre attestare la conformità della copia all'originale da cui è estratta (con le modalità indicate nelle disposizioni successive).

In caso di acquisizione di un duplicato informatico, ai sensi dell'art. 23-*bis* del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto, non è richiesta l'attestazione di conformità.

9.5. Copie per immagine di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia

contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti. È questo il caso della scansione di documento cartaceo.

Nel caso in cui si debba garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il dirigente o il funzionario all'uopo delegato, che agisce in veste di pubblico ufficiale, archivia il documento analogico e appone sulla copia informatica, la propria firma digitale o altra tipologia di firma forte, previa iscrizione sul documento di dicitura del seguente tenore:

"*Io sottoscritto/a*, *ai sensi dell'art. 22, co. 2, d.lgs. n. 82/2005, attesto che la presente copia per immagine è conforme in ogni sua parte al documento originale analogico dal quale è stata estratta.* [indicare: nome e cognome, nome ente e ufficio, data e luogo]."

Nel caso sia necessario attestare la conformità all'originale di più documenti, acquisiti per copia di immagine, ferma restando la necessità di effettuare il raffronto per ogni documento originale scansionato, è possibile effettuare un'unica attestazione di conformità, su foglio separato e collegato alle copie informatiche, da sottoscrivere digitalmente, contenente l'indicazione delle impronte hash associata a ciascuna copia informatica.

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

a) quando si deve provvedere a notificazione via PEC di documento (o allegato a documento) sottoscritto in originale analogico;
b) quando si deve formare un contratto tra l'ente e un privato che sottoscrive con firma autografa (**formazione di contratti *ibridi***). In questi casi il pubblico ufficiale acquisisce la scansione del documento firmato in originale cartaceo dal privato e, previo raffronto, attesta la conformità della copia digitale (con le modalità sopra indicate). Infine, il soggetto competente alla stipula sottoscrive la copia con la propria firma digitale, così perfezionando il contratto.

   Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi (così avviene, ad esempio, quando si effettua un download, oppure, quando si duplica un documento trasferendolo dall'hard disk del proprio computer a un dispositivo di archiviazione esterno quale una chiave usb). Tale modalità di formazione della copia del documento informatico non richiede alcuna attestazione di conformità all'originale, perché vi è perfetta coincidenza tra le due evidenze informatiche. Tale identità è rilevabile tramite raffronto delle impronte hash.

La copia di un documento informatico, invece, è un documento il cui contenuto è il medesimo dell'originale, ma con una diversa evidenza informatica rispetto al documento da cui è tratto (ad esempio, quando si trasforma un .docx in .pdf, i due docu-

menti avranno hash differenti. Lo stesso avviene se si estrae una parte di documento per formarne uno nuovo). Tale operazione è anche detta riversamento da un formato digitale verso un altro.

Se il documento originale è un documento firmato, affinché la copia conservi la medesima efficacia giuridico-probatoria, è necessario attestarne la conformità della copia all'originale. Come per le copie per immagine, dunque, il dirigente o il funzionario delegato, che agisce in veste di pubblico ufficiale, dovrà apporre la propria firma digitale, previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

"*Io sottoscritto/a, ai sensi dell'art. 23-bis, comma 2, d.lgs. n. 82/2005, attesto che la presente copia informatica è conforme in ogni sua parte al documento originale informatico dal quale è stata estratta* [indicare: nome e cognome, nome ente e ufficio, data e luogo]."

La necessità di apporre l'attestazione di conformità dipende dall'uso che viene fatto della copia, da valutare caso per caso, a seconda della rilevanza giuridica che si ritiene necessario conferire.

9.6. Acquisizione di istanze tramite moduli online

Le istanze provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e *form* messi a disposizione sul sito web del Consorzio e resi accessibili previa identificazione dell'utente con gli strumenti di identificazione SPID, CIE e CNS. I dati immessi dall'istante sono acquisiti e memorizzati su supporto informatico.

9.7. Formazione di registri e repertori

I registri e repertori tenuti dal Consorzio, ivi compreso il registro giornaliero di protocollo, sono formati mediante la generazione/raggruppamento in via automatica e memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

10. Dispositivi di firma elettronica

Il Consorzio garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica.

L'utilizzo da parte del personale dei dispositivi di firma e/o delle credenziali è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati o le credenziali di utilizzo.

10.1. Scadenza dei certificati di firma

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile.

11. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica *hash*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni del Sistema di protocollo informatico del Consorzio.

Il calcolo dell'impronta crittografica deve essere basato su una funzione di hash conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida (cfr. p. 2.2, tab. 1).

12. Associazione degli allegati al documento principale

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

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

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

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

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

13. Accessibilità del documento informatico

Per garantire l'accessibilità dei documenti informatici ai soggetti portatori di disabilità, anche ai fini della pubblicazione e dell'accesso documentale, i soggetti responsabili della formazione del documento seguono le indicazioni contenute nella "Guida pratica per la creazione di un documento accessibile" di cui all'**allegato 4** al presente Manuale.

14. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID. Ulteriori metadati facoltativi possono essere associati a particolari tipologie di documenti.

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

15. Immodificabilità e integrità del documento informatico

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

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

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

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

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

Sezione terza - Disposizioni sulla formazione di documenti analogici

16. Copie analogiche di documenti informatici

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

Quando è necessario che al destinatario giunga un documento avente la medesima efficacia giuridico probatoria del documento originale (ad esempio, quando bisogna

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

La copia analogica inviata al cittadino, inoltre, deve contenere apposita dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto come documento nativo digitale ed è disponibile presso l'amministrazione (ad es.: "*La presente copia è tratta da documento informatico, predisposto come documento nativo digitale da* [nome responsabile]*, Responsabile dell'Ufficio* [indicazione UO]*. Il documento originale informatico è archiviato nel sistema informatico del Consorzio, presso cui è disponibile per l'accesso*").

In alternativa all'apposizione della firma a stampa e della dicitura, può essere apposto il contrassegno di cui all'art. 23, comma 2-*bis*, CAD, (c.d. "*QR code*"), tramite il quale deve essere possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica.

17. Casi in cui è ammessa la formazione di documenti originali analogici

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

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

La formazione di contratti e altre scritture private in originale analogico non è consentita. A tal fine, nel caso in cui la parte contraente non sia munita di strumenti di firma digitale o qualificata, si seguono le indicazioni riportate al **par. 9.5, lett. b)** del presente Manuale.

PARTE QUARTA - GESTIONE DOCUMENTALE

Sezione prima - Flussi documentali esterni

18. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella Sezione seconda della presente Parte del Manuale. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

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

a) sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;

b) sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;

c) sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE o CNS;

d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma 4-quinquies del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domicilio digitale speciale per quel singolo procedimento o affare;

e) sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;

f) è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

19. Canali di ricezione

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

- casella PEC del Consorzio: amministrazione@cert.consorziobacino16.it;
- caselle PEC Area Contabile: fatturazione@cert.consorziobacino16.it
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti.

Gli indirizzi di posta elettronica certificata sono riportati nell'Indice delle Pubbliche Amministrazioni e pubblicizzato sul sito web istituzionale.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici del Consorzio comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi.

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

20. Formati accettati

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei seguenti **formati standard**: **.pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods, .eml.** Inoltre:

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

Possono essere accettati, inoltre, i formati contemplati nell'Allegato 2 delle Linee guida dell'AgID e indicati come "standard".

Resta salva la possibilità, da parte del responsabile del procedimento, di prevedere espresse limitazioni in relazione allo specifico procedimento, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze.

20.1. Verifica sul formato dei documenti allegati

Anche per gli allegati al documento principale, formati non previsti dal presente Manuale, dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per obiettive e motivate esigenze rappresentate dal mittente, il documento non può essere riversato in altro formato tra quelli ammessi.

21. Controllo dei certificati di firma

L'Ufficio protocollo segnala al proprio Responsabile eventuali casi in cui rilevi la mancata validità dei certificati di firma. Il Responsabile valuterà le azioni da intraprendere, a seconda della tipologia di procedimento.

22. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD.

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati, fascicolati e protocollati, secondo le disposizioni della presente Parte del Manuale.

23. Individuazione del domicilio digitale presso cui effettuare la comunicazione

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

Le comunicazioni agli indirizzi estratti da INI-PEC devono essere fatte quando hanno a oggetto informazioni o documenti rilevanti nell'ambito di rapporti professionali intercorrenti tra l'Amministrazione e il destinatario.

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

I. se vi è stata elezione di domicilio digitale, all'indirizzo PEC espressamente dichiarato dal cittadino;
II. se non vi è stata elezione di domicilio digitale, nelle more dell'attivazione dell'INAD (Indice Nazionale dei Domicili digitali), deve essere trasmessa al domicilio fisico la copia cartacea del documento. Se si tratta di documento sottoscritto dall'Amministrazione, la copia deve essere prodotta in conformità a quanto previsto al par. 16 del presente Manuale.

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (indicepa.gov.it) di cui all'art. 6-*ter* del CAD.

24. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire al Consorzio attraverso:

- il servizio postale;
- la consegna diretta agli addetti alle attività di sportello.

I documenti provenienti dal servizio postale tradizionale o da corrieri autorizzati sono consegnati all'Ufficio Protocollo.

Qualora un documento sia consegnato personalmente dal mittente o da altra persona incaricata e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'addetto alla ricezione del documento è autorizzato a fotoriprodurre gratuitamente il documento da protocollare ed apporre il solo timbro ricezione presso l'Ente, comprensivo di data e di firma autografa dell'operatore che lo riceve. Qualora il documento sia composto di più pagine, è sufficiente la fotoriproduzione della prima pagina, mentre eventuali ulteriori costi di riproduzione sono a carico di chi presenta il documento da protocollare.

Qualora chi presenta il documento richieda anche l'apposizione della ricevuta prodotta dal sistema di protocollo informatico con gli estremi, l'addetto all'Ufficio Protocollo provvede al rilascio della stessa nei tempi permessi dalle esigenze dell'ufficio.

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

Sezione seconda - Protocollo informatico

25. Sistema di protocollo informatico

Il Consorzio, per la protocollazione dei documenti, utilizza un sistema di protocollo informatico integrato con il sistema di gestione documentale. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale operativo di cui all'**allegato 2.**.

Non è consentita l'acquisizione o la trasmissione di documenti soggetti a protocollazione e relativi allegati tramite canali diversi da quelli messi a disposizione dall'Ente (ad es. strumenti personali per il trasferimento dei file).

26. Registro generale di protocollo

Nell'ambito della AOO, il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

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

27. Registro giornaliero di protocollo

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

28. Documenti soggetti a registrazione di protocollo e documenti esclusi

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

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

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

Non sono soggetti a protocollazione obbligatoria, inoltre, gli atti e i documenti registrati in repertori e registri differenti dal registro di protocollo ai sensi del **par. 39** del presente Manuale.

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

28.1 Protocollazione di documenti interni

Fermo restando quanto precisato nel paragrafo precedente con riferimento agli atti preparatori interni, sono soggetti a protocollazione tutti i documenti interni aventi rilevanza giuridico-probatoria, redatti dal personale nell'esercizio delle proprie funzioni ed al fine di documentare fatti inerenti all'attività svolta ed alla regolarità dell'azione dell'Ente o qualsiasi altro documento dal quale possano nascere diritti, doveri, o le-

gittime aspettative di terzi. Deve essere protocollata altresì la corrispondenza interna di carattere formale.

29. Disposizioni per particolari tipologie di documenti

La protocollazione della documentazione di gara e delle offerte, scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, della Regione o da altre piattaforme conformi alla normativa vigente, non è necessaria quando i gestori di tali sistemi assicurano la conservazione a tempo indeterminato della documentazione relativa alle singole gare. In tali casi si ritiene comunque opportuno, anche se non necessario, la protocollazione della richiesta d'offerta o dell'ordine diretto di acquisto e dell'offerta dell'impresa aggiudicataria acquisendo, per questa, tutti i documenti relativi e specificando, negli appositi campi, data e ora di arrivo.

30. Registrazione di protocollo

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

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

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

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

31. Modalità di registrazione

La registrazione di protocollo di un documento è eseguita dopo averne verificato la provenienza e ogni ulteriore elemento essenziale al corretto inserimento dei metadati obbligatori di cui al precedente paragrafo, nonché a evitare doppie registrazioni.

La registrazione dei documenti ricevuti, spediti e interni è effettuata in un'unica operazione, utilizzando le apposite funzioni previste dal Sistema di protocollo informatico. Al documento indirizzato a più destinatari deve essere assegnato un solo e unico numero di protocollo.

Il Sistema genera automaticamente il numero progressivo e la data di protocollazione associata. Alla registrazione di protocollo, inoltre, sono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi PEC in uscita, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione. L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo.

31.1. Protocollazione delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione

Gli utenti non abilitati alla protocollazione in entrata, per la protocollazione della posta elettronica ordinaria, provvedono a inoltrare la mail a segreteria@consorziobacino16.it, esplicitando nell'oggetto la richiesta di protocollare.

32. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA.

Se le informazioni della registrazione di protocollo sono errate (anche in caso mera svista), dunque, sarà necessario procedere alla richiesta di annullamento.

Come previsto dal par. 3.1.5 delle Linee guida AgID, le uniche informazioni che possono essere modificate – e che, dunque, non richiedono l'annullamento – sono quelle relative a:

- classificazione;
- assegnazione interna.

Pertanto, è opportuno che ogni operatore, al momento della protocollazione, presti la massima attenzione. Il registro di protocollo, infatti, è un atto pubblico a cui la legge riconosce un particolare valore giuridico-probatorio..

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

33. Gestione degli allegati

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Tutti gli allegati devono pervenire con il documento principale al fine di essere inseriti nel Sistema di protocollo informatico ed essere sottoposti a registrazione.

Gli allegati dei documenti ricevuti tramite il canale PEC sono gestiti in forma automatizzata dal sistema di protocollo informatico.

34. Tempi di registrazione e casi di differimento

La registrazione della documentazione in entrata deve avvenire in giornata o comunque, non oltre due giorni lavorativi dal ricevimento. Nel caso in cui non sia stato possibile protocollare il documento entro le 24 ore, viene comunque registrata la data di effettiva ricezione. Ai fini della gestione del protocollo, non sono in ogni caso considerati lavorativi il sabato e la domenica.

In casi eccezionali ed imprevisti che non permettono di evadere la corrispondenza ricevuta e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi (ad esempio per la registrazione di un consistente numero di domande di partecipazione ad un concorso in scadenza), con motivato provvedimento del Responsabile, è autorizzato il differimento dei termini di registrazione (protocollo differito).

Ai fini del computo di termini previsti dalla legge o da altri atti (es. bandi, contratti, ecc.), resta fermo quanto previsto dall'art. 45 del CAD, ai sensi del quale il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

35. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

a. indicazione della Amministrazione mittente;
b. codice identificativo dell'AOO mittente;
c. codice identificativo del registro;

d. numero progressivo di protocollo;
e. data di registrazione;
f. oggetto del messaggio di protocollo;
g. classificazione del messaggio di protocollo;
h. indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste al p. 2 e ss. dell'Allegato 6 alle Linee guida dell'AgID e, in particolare, deve rispettare lo schema di cui all'Appendice A (v. p. 4.1. "Segnatura di protocollo XML Schema").

36. Protocollo riservato

Sono previste particolari forme di riservatezza e di accesso controllato al Sistema di protocollo per categorie particolari di dati di cui all'articolo 9 GDPR o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR":

- documenti che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (ad es. documenti che contengono certificati medici con diagnosi o patologie, certificati di invalidità, documenti attestanti l'adesione a partiti politici, documenti contenenti sfratti esecutivi e pignoramenti, ecc.), dati personali relativi a condanne penali e reati o a connesse misure di sicurezza (ad es. documenti provenienti da Case di Reclusione);
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite all'art. 24 della legge n. 241/1990).
- segnalazioni indirizzate al RPCT ai sensi della normativa in materia di whistleblowing.

I documenti registrati con tali forme appartengono al protocollo riservato del Consorzio, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

37. Registro di emergenza

L'utilizzo del registro di protocollo emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile, in situazioni nelle quali, per cause tecniche, non sia possibile utilizzare il registro generale di protocollo informatico e la sospensione del servizio si protragga per un tempo tale da poter pregiudicare la registrazione a protocollo in giornata. In tali casi, il Responsabile dà immediata comunicazione a tutti gli uffici

della temporanea sospensione dell'utilizzo della procedura informatizzata ordinaria di protocollazione e della necessità, per la protocollazione sia in entrata che in uscita, di consegnare la documentazione all'Ufficio Protocollo.

Il registro di protocollo di emergenza ha una numerazione progressiva propria, perciò ai documenti protocollati su tale registro, una volta riversati, saranno associati due numeri di protocollo, quello del registro di emergenza e quello del registro di protocollo generale. Le registrazioni sul registro di emergenza avvengono, quando possibile, secondo le medesime regole e con le stesse modalità adoperate per le registrazioni sul registro generale di protocollo.

Sul registro di emergenza, inoltre, sono riportati:

- gli estremi del provvedimento di autorizzazione all'utilizzo del registro;
- la causa, la data e l'ora di inizio dell'interruzione;
- il numero totale di registrazioni effettuate nel corso di ogni giornata di utilizzo;
- la data e l'ora del ripristino della funzionalità del sistema
- ogni altra annotazione ritenuta rilevante.

38. Documenti soggetti a registrazione particolare

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

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

- Delibere degli organi collegiali;
- Ordinanze e decreti presidenziali;

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

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

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

39. Disposizioni sulla protocollazione e gestione dei documenti analogici.

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

Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione.

39.1. Registrazione, segnatura, annullamento.

Alla registrazione di protocollo dei documenti cartacei si applicano, in quanto compatibili, le medesime regole previste per la registrazione dei documenti informatici.

Le lettere anonime sono soggette a registrazione di protocollo, eventualmente riservato, indicando nel campo del mittente la dicitura “Anonimo”.

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l’avvenuta consegna del documento, è cura del personale dell’Ufficio Protocollo rilasciare la **ricevuta di avvenuta protocollazione** prodotta direttamente dal protocollo informatico.
Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l’addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi – se richiesto – a far pervenire la ricevuta all’indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall’interessato o da persona espressamente delegata nei giorni successivi.

39.2. Corrispondenza contenente dati sensibili

I documenti contenenti categorie particolari di dati, di cui all'articolo 9 GDPR o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR”, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura “contiene dati sensibili” e successivamente consegnati al Responsabile.

39.3. Corrispondenza personale o riservata

La corrispondenza nominativamente intestata è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, ad eccezione di quella diretta ai titolari di cariche istituzionali. Se la corrispondenza riveste carattere “riservato” o “personale”, e ciò è desumibile prima dell’apertura della busta, questa viene inviata chiusa direttamente al destinatario priva di registrazione. Se il carattere “riservato” o “personale” della corrispondenza viene desunto dopo averne preso visio-

ne, il plico viene richiuso e inviato al destinatario privo di registrazione. L'eventuale registrazione di protocollo potrà essere effettuata in un momento successivo.

39.4. Corrispondenza cartacea non di competenza dell'Amministrazione

Qualora pervenga, tramite posta tradizionale, un documento cartaceo che non sia evidentemente indirizzato al Consorzio (es. altro destinatario), lo stesso è trasmesso a chi di competenza, se individuabile, altrimenti è restituito al mittente.

Nel caso in cui un documento della fattispecie sia erroneamente registrato al protocollo, questi è spedito a chi di competenza, oppure restituito al mittente, con una lettera di trasmissione protocollata.

Sezione terza – Classificazione e fascicolazione

40. Classificazione dei documenti

I documenti formati e acquisiti dall'Consorzio sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Piano di classificazione (Titolario) di cui all'**allegato 2.**.

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

La classificazione dei documenti in entrata è effettuata dal personale addetto alla protocollazione, mentre la classificazione dei documenti prodotti dal Consorzio è effettuata dal personale preposto all'invio del documento.

41. Fascicolazione informatica dei documenti

Al fine di garantire la consultazione dei documenti informatici, da parte sia di altre amministrazioni che degli utenti, questi sono raccolti in fascicoli informatici. I fascicoli, eventualmente, possono essere organizzati in sottofascicoli, come da **Allegato 7**.

Il destinatario del documento dovrà provvedere alla fascicolazione, tramite l'apposita funzione del Sistema di gestione documentale (cfr. **allegato 3**).

I fascicoli informatici possono essere organizzati:

a. per affare, quando i documenti raccolti nel fascicolo, accomunati secondo un criterio di classificazione basato sulla competenza amministrativa, non sono tutti riferibili a un singolo procedimento amministrativo. Il fascicolo per affare deve avere una data di apertura e una durata circoscritta;
b. per attività, quando i documenti raccolti nel fascicolo attengono allo svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale;

c. per persona (fisica o giuridica), quando i documenti raccolti nel fascicolo, anche con classificazioni diverse, sono riferibili a un medesimo soggetto. Sono fascicoli di tipo “aperto”, con durata pluriennale e indeterminata;
d. per procedimento amministrativo, quando i documenti raccolti nel fascicolo rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

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

PARTE QUARTA – CONSERVAZIONE DEI DOCUMENTI

42. Sistema di conservazione dei documenti informatici

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nel:

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell’archiviocorrente dell’Agenzia
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

43. Servizio archivistico

Il Protocollo informatico è custodito presso locale server in sede esternalizzata agli uffici di DIREZIONE.
L’accesso al locale server non è consentito a personale non autorizzato
Sono state altresì regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità, nel tempo, di tutti i documenti trasmessi o ricevuti, adottando i formati previsti dalle regole tecniche vigenti.

44. Conservazione del registro giornaliero di protocollo

Il registro giornaliero di protocollo è trasmesso, entro la giornata lavorativa successiva, al sistema di conservazione, garantendone l’immodificabilità del contenuto.

Nelle more di avvio del servizio di invio in conservazione sopra descritto, il file PDF del registro giornaliero è registrato nel registro di protocollo interno dell’Agenzia a tutela della immodificabilità del medesimo ai sensi dell’art.3, comma 4, lettera d), del DPCM 13 novembre 2014.

45. Misure di sicurezza e monitoraggio del sistema di conservazione

Nel Manuale di conservazione (**Allegato 6**) sono descritte le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti

del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

PARTE QUINTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

46. Sicurezza dei sistemi informatici del Consorzio

La memorizzazione dei documenti correnti è effettuata sui server del Consorzio, in attesa dell'archiviazione tramite versamento al sistema di conservazione.

47. Amministratore di sistema

Il ruolo di Amministratore del Sistema informativo del Consorzio è conferito a Sat (Servizi amministrativi Territoriali). L'Amministratore di sistema svolge i compiti operativi relativi alla gestione delle abilitazioni di accesso (quali il rilascio, la revoca, l'attribuzione di particolari privilegi, ecc.), su indicazione del Responsabile della gestione documentale e dei responsabili di servizio.

48. Uso del profilo utente per l'accesso ai sistemi informatici

La gestione degli utenti abilitati ad accedere al protocollo informatico, in base alla pianta organica dell'ente e sulla base delle indicazioni dei responsabili competenti**,** è affidata all'Ufficio Protocollo.
Per l'accesso ai sistemi informatici del Consorzio, è necessaria l'assegnazione di un profilo utente formalmente autorizzata dal Responsabile di Area.
Ogni profilo è protetto da un sistema di credenziali (username e password). L'uso di ogni profilo utente è strettamente personale e ogni dipendente, sotto la propria responsabilità, è tenuto a custodire e non diffondere le proprie credenziali.

49. Accesso alle postazioni di lavoro, ai locali e agli archivi del Consorzio

L'accesso alle postazioni di lavoro è consentito esclusivamente al personale degli uffici ed ai soggetti terzi regolarmente autorizzati (ad es., per necessità connesse a esigenze di manutenzione, interventi tecnici, consegne di forniture, ecc.).
L'archivio storico del Consorzio è collocato nella sede centrale in locali opportunamente chiusi al pubblico.