



MANUALE DI GESTIONE DOCUMENTALE

SOMMARIO

PARTE PRIMA – DISPOSIZIONI PRELIMINARI	5
1. Riferimenti normativi	5
2. Finalità, contenuti e metodologia del documento	6
3. Approvazione e modalità di aggiornamento del Manuale	6
PARTE SECONDA – ORGANIZZAZIONE	7
4. Area organizzativa omogenea e Unità Organizzative	7
5. Responsabile della gestione documentale e altri soggetti responsabili	7
6. Sistema informatico di gestione documentale dell'Unione	8
7. Abilitazioni di accesso	8
8. Soggetti delegati alle attività di protocollazione	9
PARTE TERZA – FORMAZIONE DEI DOCUMENTI	10
<i>Sezione prima – Modalità di formazione</i>	10
9. Modalità di formazione dei documenti informatici	10
9.1. Creazione e redazione tramite software di documenti informatici	10
9.2. Elementi essenziali del documento amministrativo informatico	11
9.3. Scelta del formato e modalità di sottoscrizione	11
9.4. Acquisizione di documenti informatici	12
9.5. Copie per immagine di documenti analogici	12
9.6. Duplicati, copie ed estratti informatici di documenti informatici	13
9.7. Potere di attestare la conformità delle copie	14
9.8. Acquisizione di istanze tramite moduli online	14
9.9. Formazione di registri e repertori	14
<i>Sezione seconda – Disposizioni comuni a tutte le modalità di formazione</i>	15
10. Dispositivi di firma elettronica	15
11. Identificazione univoca del documento informatico	15
12. Associazione degli allegati al documento principale	16
13. Accessibilità del documento informatico	16
14. Metadati del documento informatico	16
15. Immodificabilità e integrità del documento informatico	17
<i>Sezione terza - Disposizioni sulla formazione di documenti analogici</i>	18
16. Copie analogiche di documenti informatici	18
17. Casi in cui è ammessa la formazione di documenti originali analogici	18

PARTE QUARTA - GESTIONE DOCUMENTALE	20
<i>Sezione prima - Flussi documentali esterni</i>	20
18. Ricezione telematica di documenti informatici in entrata	20
19. Canali di ricezione	20
20. Formati accettati	21
21. Controllo dei certificati di firma	21
22. Trasmissione telematica di documenti informatici in uscita	22
23. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni	22
24. Disposizioni sui documenti analogici	22
<i>Sezione seconda - Protocollo informatico</i>	23
25. Sistema di protocollo informatico	23
26. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico	23
27. Registro generale di protocollo	24
28. Registro giornaliero di protocollo	24
29. Documenti soggetti a registrazione di protocollo e documenti esclusi	24
30. Disposizioni per particolari tipologie di documenti	25
31. Registrazione di protocollo	25
32. Modalità di registrazione	26
33. Annullamento e modifiche della registrazione di protocollo	26
34. Gestione degli allegati	27
35. Tempi di registrazione e casi di differimento	27
36. Segnatura di protocollo	28
37. Protocollo riservato	29
38. Registro di emergenza	29
39. Documenti soggetti a registrazione particolare	30
40. Disposizioni sulla protocollazione di documenti analogici	31
40.1. Registrazione, segnatura, annullamento	32
40.2. Corrispondenza contenente dati sensibili	32
40.3. Corrispondenza personale o riservata	32
40.4. Corrispondenza cartacea non di competenza dell'Amministrazione	32
<i>Sezione terza – Classificazione, fascicolazione e accesso ai documenti e ai fascicoli informatici</i>	34
41. Classificazione dei documenti	34
42. Fascicolazione informatica dei documenti	34
43. Accesso ai fascicoli e ai documenti informatici	36
<i>Sezione quarta – Flussi documentali interni</i>	36
44. Assegnazione dei documenti in entrata agli uffici	36
45. Comunicazioni interne	37

46. Pubblicazioni nell'Albo pretorio	37
PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI	38
47. Sistema di conservazione dei documenti informatici	38
48. Responsabile della conservazione	38
49. Oggetti della conservazione	39
50. Formati ammessi per la conservazione	39
51. Modalità e tempi di trasmissione dei pacchetti di versamento	40
52. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica	40
53. Accesso al Sistema di conservazione	41
54. Selezione e scarto dei documenti	41
55. Conservazione, selezione e scarto dei documenti analogici	41
56. Misure di sicurezza e monitoraggio	42
PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI	44
57. Sicurezza dei sistemi informatici dell'Unione.	44
58. Amministratore di sistema	44
59. Uso del profilo utente per l'accesso ai sistemi informatici	44
60. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Unione	45
ALLEGATI	
1. Organigramma	
2. Provvedimento di nomina del Responsabile	
3. Manuali del software di gestione documentale	
4. Abilitazioni di accesso	
5. Guida alla formazione del documento accessibile	
6. Piano di classificazione	
7. Modello di registro di emergenza	
8. Linee Guida alla fascicolazione	
9. Manuale di conservazione del Polo Archivistico Regionale (ParER)	
10. Disciplinare tecnico del servizio di conservazione	
11. Piano della Sicurezza Informatica	
12. Massimario di selezione e scarto	
13. Modulistica versamenti documentazione analogica	
14. Piano di Fascicolazione	

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 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 Aree Organizzative Omogenee 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 dell'Unione Terre di Castelli e fornisce le istruzioni per la formazione dei documenti informatici, per il corretto funzionamento del servizio di 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 sia 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.

Con la pubblicazione nella sezione “Amministrazione Trasparente” del sito internet istituzionale (sottosezione “Atti Generali”), il Manuale è reso noto anche esternamente all'ente. In quest'ottica, il Manuale 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 di Giunta dell'Unione, su proposta del Responsabile della gestione documentale dell'ente.

I successivi aggiornamenti del Manuale devono essere sottoposti all'approvazione della Giunta dell'Unione. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale.

Il Manuale e gli allegati sono pubblicati sul sito istituzionale dell'Unione, nella sezione “Amministrazione Trasparente”, sottosezione “Atti generali”.

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea e Unità Organizzative

L'Unione Terre di Castelli si configura come un'unica Area Organizzativa Omogenea ("AOO") denominata "Unione Terre di Castelli" (codice univoco: A171951). L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA.

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

5. Responsabile della gestione documentale e altri soggetti responsabili

L'Unione Terre di Castelli, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura dirigenziale, il "Responsabile della gestione documentale", dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti di Responsabile per la gestione documentale e di Responsabile della conservazione, di cui rispettivamente ai parr. 3.4 e 4.5 delle Linee guida.

Il Responsabile della gestione documentale dell'Unione Terre di Castelli è stato individuato inizialmente con Deliberazione della Giunta dell'Unione n. 25 del 10.03.2022. Successivamente è stato individuato nuovo Responsabile con Decreto del Presidente dell'Unione n. 3/2023 prot. 13321 del 30/03/2023 nella figura della Dott.ssa Elisabetta Manzini. In caso di vacanza o assenza, il vicario del Responsabile è stato individuato, con deliberazione 25/2022 già citata, nella persona di Giorgia Baccolini (**Allegato2 - Provvedimento di nomina del Responsabile**).

I compiti del Responsabile della gestione documentale (d'ora in avanti anche solo "Responsabile") sono definiti nell'atto di nomina. In particolare, il Responsabile:

- a) è preposto, ai sensi dell'art. 61 TUDA, al servizio di tenuta del protocollo informatico, come della gestione dei flussi documentali e degli archivi della AOO unica dell'Unione;
- 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 singole attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
- d) valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;

- e) vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnature di protocollo, di produzione e conservazione del registro giornaliero di protocollo;
- f) 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;
- g) effettua un periodico censimento degli strumenti software di gestione documentale in uso presso l'Unione e, di concerto con il RTD, ne verifica la conformità alla normativa vigente.

Ulteriori e specifici compiti del Responsabile sono indicati nelle sezioni pertinenti del presente Manuale. Il Responsabile, 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 dell'Unione

Il Sistema informatico di gestione documentale dell'Unione Terre di Castelli si avvale del seguente software di gestione documentale:

- *Prisma*, è il modulo applicativo della suite *Smart*Gov*, erogato in modalità SaaS dalla ditta ADS Automated data systems S.p.A. e resa accessibile mediante Web Service. La soluzione *Prisma*, comprensiva del Sistema di protocollo informatico, consente la gestione dell'*iter* di formazione degli atti degli organi e del personale dell'Amministrazione, nonché la gestione degli obblighi di pubblicazione nell'Albo pretorio online e nella sezione Amministrazione trasparente del sito istituzionale dell'Unione (**Allegato 3 - Manuale utente**);

L'elenco dei software è trattenuto agli atti dal servizio sistemi Informativi e costantemente aggiornato.

7. Abilitazioni di accesso

Le abilitazioni di accesso ai sistemi di gestione documentale e al sistema di protocollo informatico dell'Unione sono assegnate, su richiesta dei diversi responsabili UOR, dal Responsabile dei Servizi Informativi su indicazione del Responsabile, che riconosce a ciascun utente o gruppo di utenti funzioni diversificate in ragione dell'appartenenza a un determinato settore dell'organizzazione o dell'assunzione di specifici ruoli e compiti.

Le tipologie di abilitazioni di accesso al Sistema sono descritte nell'**Allegato 4 (Abilitazioni di accesso)** al presente Manuale.

8. Soggetti delegati alle attività di protocollazione

Le attività di protocollazione in entrata sono affidate al personale addetto al Servizio Segreteria Generale e Protocollo, agli uffici di protocollo decentrati presso i comuni, al Servizio Sociale Territoriale e al Corpo Unico di Polizia Locale, ai quali sono attribuiti specifici profili utente che consentono di accedere al Sistema di protocollo informatico dell'Unione e di effettuare le attività di protocollazione e classificazione dei documenti.

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

Ulteriori deleghe alle attività di protocollazione, ove non previste nel presente Manuale e nei relativi allegati, sono conferite dal Responsabile con proprio provvedimento. L'eventuale delega relativa alle attività di annullamento delle registrazioni (v. par. 33 del presente Manuale) deve essere resa in modo esplicito nel provvedimento di delega.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Sezione prima – Modalità di formazione

9. Modalità di formazione dei documenti informatici

Tutti i documenti dell'Unione Terre di Castelli sono formati in originale come documenti informatici, secondo le modalità individuate nella presente Parte del Manuale.

I documenti informatici dell'Unione 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, oppure formazione delle fatture elettroniche tramite SDI);
- 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 dell'Unione Terre di Castelli dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Microsoft Office: Word, Excel, Access, Powerpoint, ecc.*;
- programmi della suite *Libre Office: Writer, Calc, Base, Impress, ecc.*;

Il testo del documento informatico creato dagli uffici dell'Unione deve essere redatto utilizzando esclusivamente il font Arial 12.

9.2. Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dall'Unione deve recare obbligatoriamente i seguenti elementi:

1. denominazione dell'Amministrazione e Stemma;
2. UOR;
3. data e luogo;
4. numero e data di protocollo o di registrazione (se soggetto a registrazione particolare);
5. riferimenti a procedimento o fascicolo;
6. identificazione e dati dei destinatari (se si tratta di documento in uscita);
7. oggetto del documento;
8. testo;
9. indicazione degli allegati (se presenti);
10. sottoscrizione;
11. numeri di pagina;
12. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita).

9.3. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dall'Unione deve essere scelto tra i seguenti **formati standard**: .rtf, .docx, .odt, .pdf, .xlsx, .ods, .xml.

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 e 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 consenta 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 Sindaco 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). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES o 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);
- 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, memorizzandone il contenuto 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 da un documento originale, sia esso 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 e, 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 in grado di assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti.

Al fine di assicurare 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, deve apporre sulla copia informatica del documento, quale risultante dal processo di scansione, l'attestazione di conformità all'originale da cui essa è stata estratta. Il funzionario, quindi, dovrà apporre la propria firma digitale (o altra tipologia di firma forte) o il sigillo elettronico qualificato dell'ufficio,

previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

“Io sottoscritto/a [nome e cognome – nome ente e ufficio], ai sensi dell’art. 22, comma 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. [indicazione di data e luogo].”

Nel caso sia necessario attestare la conformità all’originale di più copie per immagine da versare in conservazione, in alternativa alla procedura sopra descritta, il funzionario delegato, al fine di attestare la conformità delle copie ai documenti originali, una volta effettuato il raffronto, potrà sottoscrivere un’unica attestazione di conformità, su foglio separato ma collegato alle copie tramite apposizione dell’impronta *hash*, precisando gli elementi identificativi di ciascun documento originale scansionato (almeno “oggetto”, se possibile anche “data” e “autore”).

9.6. Duplicati, copie ed estratti informatici di documenti informatici

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 duplica un documento trasferendolo dall’hard disk del proprio personal 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.

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 (trasformazione di un documento in formato .pdf in un documento in diverso formato, ad esempio, .docx). Tale operazione è anche detta “riversamento” da un formato digitale verso un altro. Affinché la copia conservi la medesima efficacia giuridico-probatoria del documento informatico originale, è necessario attestarne la conformità all’originale. Come per le copie per immagine, dunque, il dirigente o il funzionario all’uopo delegato, che agisce in veste di pubblico ufficiale, dovrà apporre la propria firma digitale (o altra tipologia di firma forte) o il sigillo elettronico qualificato dell’ufficio, previa iscrizione sul documento (a margine o in calce) o in foglio elettronico a esso congiunto della seguente dicitura:

“Io sottoscritto/a [nome e cognome – nome ente e ufficio], 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 [indicazione di data e luogo].”

9.7. Potere di attestare la conformità delle copie

Il responsabile della UOR ha il potere di attestare la conformità delle copie dei documenti originali, formati o acquisiti, ai sensi degli articoli 22 e ss. del CAD. Il potere di attestare la conformità delle copie può essere delegato ad altro personale del servizio, purché la delega risulti da un provvedimento formale del delegante.

9.8. 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 dell'Unione 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. Le istanze così formate sono acquisite dal Sistema di protocollo informatico dell'Unione e costituiscono a tutti gli effetti documenti amministrativi informatici, trattati come documenti in entrata soggetti a registrazione di protocollo.

9.9. Formazione del registro giornaliero e repertori

Il registro giornaliero di protocollo è formato mediante la generazione e raggruppamento in via automatica e memorizzazione in forma statica dell'insieme delle registrazioni effettuate dal sistema di gestione documentale.

I repertori sono creati nei formati standard secondo quanto indicato al paragrafo 9.3 e conservati presso le singole UOR.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

10. Dispositivi di firma elettronica

L'Unione garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica. A tal fine, l'Unione si serve delle seguenti modalità di sottoscrizione dei documenti digitali:

- Firma digitale PAdES (formato .pdf);
- Firma digitale CAdES (formato .p7m);
- Firma digitale XAdES (formato .xml).

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

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del proprio certificato, 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, affinché provveda a costituire un riferimento temporale giuridicamente valido e tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

11. Identificazione univoca del documento informatico

Ogni documento informatico presente nel gestionale documentale è identificato in modo univoco e persistente.

L'identificazione univoca dei documenti può essere effettuata verificando l'impronta crittografica *hash* associata a ciascun documento.

A ogni documento informatico, infatti, corrisponde una e una sola impronta *hash* (pertanto, il duplicato di un documento informatico avrà la stessa impronta *hash* del documento originale, mentre due versioni dello stesso documento, se non identiche, avranno impronte *hash* diverse).

L'impronta crittografica *hash* può essere verificata tramite le apposite funzioni dei software di gestione documentale oppure, per i documenti protocollati, tramite la consultazione dei metadati della segnatura di protocollo.

L'impronta crittografica deve essere basata 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 dallo strumento software utilizzato 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 5 (Guida alla formazione del documento accessibile)** al presente Manuale.

14. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i seguenti metadati previsti per la registrazione di protocollo:

- indicazione dell'amministrazione mittente (Codice IPA identificativo dell'Ente);
- indicazione della AOO mittente (Codice AOO, identificativo dell'Unione nell'Indice dei Domicili digitali);
- indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
- numero progressivo di protocollo (generato automaticamente dal Sistema e registrato in forma non modificabile);

- data di registrazione (come sopra);
- oggetto del messaggio di protocollo;
- classificazione del messaggio di protocollo;
- fascicolo del messaggio di protocollo;
- mittente e destinatario;
- codice dell'unità che ha prodotto il documento;
- codice identificativo dell'unità a cui il documento è assegnato;
- identificazione degli allegati;
- impronta del documento principale e degli eventuali allegati.

Ulteriori metadati facoltativi sono associati per particolari tipologie documentali.

In particolare, ai documenti relativi alle procedure per l'affidamento dei contratti pubblici (provvedimenti, comunicazioni, contratti), devono essere associati metadati relativi al CIG.

I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione, della memorizzazione nel sistema o del versamento in conservazione.

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 essere 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 tramite posta tradizionale, raccomandata, o consegna a mano, 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 dall'indicazione a stampa del nominativo del soggetto responsabile.

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 UOR]. Il documento originale informatico è archiviato nel sistema informatico dell'Unione Terre di Castelli, presso cui è disponibile per l'accesso”*).

Quando possibile, la dicitura deve essere integrata con indicazioni sulle modalità per effettuare l'accesso online al documento informatico.

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).

PARTE QUARTA - GESTIONE DOCUMENTALE

Sezione prima - Flussi documentali esterni

18. Ricezione telematica di documenti informatici in entrata

La ricezione dei documenti informatici (istanze, dichiarazioni, comunicazioni) avviene tramite le caselle PEC dell'Ente e i portali di front office dei servizi on line, messi a disposizione dall'Unione.

Caselle PEC: l'Ente ha attivato la casella PEC istituzionale, la cui gestione operativa è affidata all'Ufficio Protocollo Generale, e ulteriori caselle PEC, affidate alla gestione di settori e servizi, integrate al Sistema di protocollo.

Nel caso di documenti pervenuti su indirizzi di posta elettronica ordinaria del personale dell'Ente, significativi ai fini del procedimento, si provvede alla loro protocollazione, associando la mail pervenuta, alla maschera di protocollo; il personale ricevente è tenuto a inoltrare detta documentazione alle Segreterie di Settore/Servizio, per garantirne la registrazione, attivandosi nel contempo con il mittente al fine di indicare le corrette procedure per successive comunicazioni verso l'Ente.

Portali dei servizi on line: le istanze pervenute all'Ente tramite la compilazione di form appositamente predisposte dall'Ente (istanze telematiche), sono protocollate in forma automatica, e smistate alla scrivania virtuale dell'ufficio competente, attraverso flussi documentali opportunamente configurati.

Per tutti i messaggi con segnature informatica, in arrivo sulle caselle PEC dell'Unione, il Sistema di protocollo attiva un controllo sulla conformità della segnature alla normativa vigente in materia di sigillo elettronico qualificato, apposto sulla segnature informatica di protocollo.

19. Canali di ricezione

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

- caselle PEC: unione@cert.unione.terredicastelli.mo.it;
fatture.unione@cert.unione.terredicastelli.mo.it;
polizia@cert.unione.terredicastelli.mo.it;
servizisociali@cert.unione.terredicastelli.mo.it;
- acquisizione di istanze, redatte anche tramite *form*, formate e trasmesse tramite il portale dei servizi online;
- cooperazione applicativa tra pubbliche amministrazioni;

- altri canali di trasmissione, anche di posta elettronica ordinaria (protocollo@terredicastelli.mo.it), indicati per specifici procedimenti.

L'indirizzo di posta elettronica certificata è abilitato alla ricezione dei documenti provenienti da indirizzi di posta elettronica ordinaria.

L'indirizzo di posta elettronica certificata è riportato 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 dell'Unione comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile della UOR assegnataria della comunicazione o, comunque, il soggetto individuato quale responsabile del procedimento ai sensi dell'art. 5, comma 3, L. n. 241/1990, 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 di norma accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati previsti dall'Allegato 2 alle Linee guida.

Qualora provengano documenti in formati non ammessi legati a singole e specifiche situazioni, si procede comunque alla protocollazione.

A seconda della tipologia di procedimento, il responsabile del procedimento può limitare le tipologie di formati accettati, purché le limitazioni siano ragionevoli e giustificate da obiettive esigenze legate al procedimento. Il responsabile del procedimento verifica il formato dei documenti ricevuti rispetto allo specifico procedimento e comunica al mittente l'eventuale non conformità del documento e/o l'assenza dei requisiti previsti.

L'accettazione di formati non previsti dalle Linee Guida o dalla disciplina del singolo procedimento deve essere consentita nel caso in cui, per obiettive esigenze rappresentate dal mittente, il documento non possa essere riversato in altro formato tra quelli ammessi.

21. Controllo dei certificati di firma

Il Responsabile del procedimento verifica la validità dei certificati di firma e, in caso di certificato scaduto o revocato, lo segnala al personale addetto alla protocollazione, affinché indichi la circostanza in nota alla registrazione di protocollo (v. procedura di

modifica di cui all'art. 33 del Manuale). Il Responsabile, inoltre, valuta 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 di trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD.

Per la trasmissione telematica di documenti a imprese il domicilio digitale è estratto dalla piattaforma regionale AdriER mediante web service, attraverso porta CAD.

Le comunicazioni agli indirizzi estratti da AdriER devono essere effettuate esclusivamente quando sono afferenti a rapporti professionali intercorrenti tra l'Unione e il destinatario.

Quando l'indirizzo PEC del soggetto destinatario non risulti attivo, la circostanza deve essere segnalata alla Camera di Commercio competente per la registrazione nel registro delle imprese.

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

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione o registrazione particolare, secondo le medesime regole per la registrazione di protocollo dei documenti.

23. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni

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.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

24. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire all'Unione attraverso:

- il servizio postale;

- la consegna diretta agli uffici o agli addetti alle attività di sportello;
- il fax, nei soli casi di esclusione dell'applicazione della normativa previsti dall'art. 2, comma 6, D.lgs. n. 82/2005.

Gli orari definiti per la presentazione della documentazione analogica sono indicati sul sito web istituzionale dell'Unione.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

Sezione seconda - Protocollo informatico

25. Sistema di protocollo informatico

L'Unione, per la protocollazione dei documenti in entrata, in uscita e interni, utilizza il Sistema di protocollo informatico *Prisma*. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo di cui all'**Allegato 3** al presente Manuale.

26. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, il Responsabile, nella veste di responsabile del protocollo informatico:

- a. coordina la gestione del Sistema di protocollo informatico;
- b. assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
- c. esercita il controllo generale sui flussi documentali esterni e interni;
- d. assicura la corretta esecuzione delle attività di protocollazione;
- e. autorizza l'attivazione del protocollo di emergenza;
- f. autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
- g. vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli addetti delegati dal Responsabile. La modalità di individuazione dei soggetti delegati alle attività di protocollazione è definita al par. 8 del presente Manuale.

27. 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 imm modificabile 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.

28. 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. Il Registro è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

29. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dall'Ente, 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;
- 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.
- estratti conto bancari, comunicazioni di bonifici bancari.

Non sono soggetti a protocollazione, 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.

30. 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.

31. 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 garantire l'identificazione univoca e certa del documento. 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 inviati;
- 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, sono aggiunti i seguenti metadati modificabili dagli operatori autorizzati:

- g) tipologia di documento;
- h) classificazione (titolo e classe) sulla base del Piano di Classificazione (v. **allegato 6**);
- 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.

32. Modalità di registrazione

La registrazione di protocollo di un documento è eseguita dopo averne verificato l'autenticità, la provenienza e l'integrità.

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. 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.

L'eventuale indicazione dell'ufficio utente, ovvero del soggetto destinatario del documento, va riportata nella segnatura di protocollo.

Gli utenti non abilitati alla protocollazione in entrata, per la **protocollazione della posta elettronica ordinaria**, provvedono a reindirizzare il file .EML contenente messaggio in entrata e a inoltrarlo in allegato all'indirizzo di posta ordinaria protocollo@terredicastelli.mo.it.

33. 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. In particolare, i metadati indicati al par. 31 del presente Manuale, lettere da a) a f), non sono modificabili, ma eventualmente annullabili.

Ogni annullamento della registrazione deve:

- essere autorizzato con comunicazione formale del Responsabile;
- comportare la memorizzazione di data, ora e estremi della comunicazione formale di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile della gestione documentale devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es. la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'ente, la

registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori). Solo il Responsabile ha il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso. Il Responsabile può delegare il personale addetto al Servizio Segreteria Generale e Protocollo ad autorizzare le operazioni di annullamento, che deve risultare in modo esplicito nel provvedimento di delega. In tal caso, la comunicazione formale di autorizzazione resa dal delegato deve indicare gli estremi del provvedimento di delega.

Come previsto dal par. 3.1.5. delle Linee Guida AgID, le uniche informazioni modificabili di una registrazione di protocollo sono quelle relative a:

- classificazione (titolo e classe);
- assegnazione interna all'amministrazione (per competenza o per conoscenza).

Le operazioni di modifica possono essere svolte dal personale addetto alla protocollazione, anche senza previa autorizzazione del Responsabile.

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

34. 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. Negli altri casi, l'associazione degli allegati al documento principale avviene con le modalità indicate al par. 12 del presente Manuale.

Non è ammessa l'associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo.

35. Tempi di registrazione e casi di differimento

La registrazione della documentazione in entrata deve avvenire in giornata o comunque non oltre il giorno lavorativo successivo a quello di arrivo. Ai fini della gestione del protocollo non sono in ogni caso considerati lavorativi il sabato e la domenica.

In presenza di casi eccezionali e imprevisti che non permettano 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).

Il protocollo differito si applica solo ai documenti in entrata e per tipologie omogenee che il Responsabile deve descrivere nel provvedimento. Il provvedimento individua i documenti da ammettere alla registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve essere comunque effettuata.

Al momento della registrazione differita devono essere indicati in nota alla registrazione gli estremi del provvedimento di differimento. In ogni caso, della ricezione del documento informatico da parte dell'Unione, fa fede la ricevuta di consegna generata dal gestore della casella PEC.

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.

36. 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. L'operazione di segnatura va completata con l'apposizione al documento degli elementi necessari alla gestione archivistica dello stesso (anno, titolo, classe).

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").

37. Protocollo riservato

Sono previste particolari forme di riservatezza e di accesso controllato al Sistema di protocollo per:

- documenti contenenti categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento UE 2016/679 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 dell'Unione, costituito dalle registrazioni sul Sistema di protocollo il cui accesso è consentito solamente agli utenti autorizzati.

38. Registro di emergenza

L'utilizzo del registro di protocollo emergenza, ai sensi dell'art. 63 del TUDA, è autorizzato dal Responsabile, o, in assenza, dal suo Vicario, 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 fornisce 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 sia in uscita, di consegnare la documentazione al Servizio Segreteria Generale e Protocollo.

Il registro di protocollo di emergenza è attivato su supporto informatico e redatto mediante un apposito applicativo installato in locale, che permette il riversamento

automatico delle registrazioni. Nei casi in cui non sia possibile l'utilizzo del registro di emergenza su supporto informatico, il Responsabile provvede alla formazione del registro di emergenza su supporto analogico, redatto secondo lo schema di cui all'**allegato 7 (Modello di registro di emergenza)**.

Il registro di protocollo di emergenza ha una numerazione progressiva propria e, di conseguenza, 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.

Al ripristino della piena funzionalità del Sistema di protocollo informatico, il Responsabile provvede alla chiusura del registro di emergenza, annotando il numero delle registrazioni effettuate, la data e l'ora di chiusura, e dà disposizioni per il riversamento delle registrazioni sul registro di protocollo generale.

39. 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 le tipologie documentali riconducibili ai seguenti repertori e registri all'uopo istituiti:

- Repertorio delibere;
- Repertorio determine;
- Repertorio albo pretorio;
- Registro decreti del Presidente dell'Unione;
- Registro ordinanze dirigenziali;
- Repertorio contratti;
- Repertorio convenzioni;
- Repertorio mandati;
- Repertorio reversali;
- Registro sanzioni amministrative;
- Registro atti di Polizia Giudiziaria;
- Permessi ZTL.

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.

Il Responsabile, al fine di dare attuazione ai principi di unicità e onnicomprensività del registro di protocollo, valuta periodicamente l'opportunità di sopprimere le forme di registrazione particolare non necessarie per legge, prevedendo in sostituzione esclusivamente la registrazione di protocollo.

40. Disposizioni sulla protocollazione di documenti analogici

Il personale addetto a effettuare la registrazione di protocollo informatica 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.

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 del Servizio Segreteria Generale e Protocollo rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico.

La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO;
- il mittente;
- l'oggetto;
- numero e descrizione degli allegati se presenti;
- l'indicazione di Responsabilità: UOR e Responsabile del Procedimento Amministrativo cui è assegnato il documento per competenza;
- l'operatore di protocollo che ha effettuato la registrazione.

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.

40.1. 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".

Per i documenti analogici la segnatura è apposta con timbro ed etichetta riportante i dati indicati al par. 36, lett. da a) a e).

Sul documento analogico soggetto ad annullamento della registrazione si deve riportare a margine il numero di protocollo e la data dell'autorizzazione di annullamento. La segnatura (timbro ed etichetta) deve essere barrata con la dicitura "*annullato*".

40.2. Corrispondenza contenente dati sensibili

I documenti contenenti categorie particolari di dati o soggetti a riservatezza, pervenuti in modalità cartacea, dopo essere stati scansionati e allegati alla registrazione effettuata con protocollo riservato, devono essere inseriti in busta chiusa recante la dicitura "contiene dati sensibili" e successivamente consegnati al dirigente (o funzionario titolare di PO) competente in base all'assegnazione.

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

40.4. Corrispondenza cartacea non di competenza dell'Amministrazione

La corrispondenza cartacea che non è evidentemente di competenza dell'Unione (es. altro destinatario) non va aperta e va riconsegnata al Servizio postale; in caso di errata apertura, la busta va richiusa indicando la dicitura "aperta per errore", apponendo timbro datario e riconsegnata al Servizio postale. La corrispondenza cartacea che

invece riporta l'indirizzo corretto sulla busta, ma non è di competenza dell'Unione, a seguito dell'apertura e valutazione, va richiusa indicando la dicitura “aperta e non di competenza”, apponendo timbro datario e riconsegnata al Servizio postale.

Sezione terza – Classificazione, fascicolazione e accesso ai documenti e ai fascicoli informatici

41. Classificazione dei documenti

I documenti formati e acquisiti dall'Unione sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Piano di classificazione (**allegato 6**). 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 dall'Unione è effettuata dal Responsabile dell'UOR o dal personale da questo delegato.

42. 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, secondo le indicazioni fornite nella guida alla fascicolazione di cui all'**allegato 8 (Linee guida alla fascicolazione)**. I fascicoli eventualmente possono essere organizzati in sottofascicoli.

Quando è necessario aprire un nuovo fascicolo informatico, l'utente abilitato alla creazione dei fascicoli provvede all'apertura del fascicolo in cui inserire il documento.

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.

Nelle more dell'implementazione di modalità automatizzate per la creazione e gestione dei fascicoli, organizzate secondo il piano di fascicolazione dell'Unione, gli utenti tenuti alla formazione dei fascicoli informatici assicurano che siano associati almeno i seguenti metadati, distinti per tipologia di fascicolo.

Il fascicolo informatico organizzato **per procedimento amministrativo** deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (procedimento amministrativo);
3. codice IPA Amministrazione titolare (campo "Ruolo");
4. codice IPA Amministrazioni partecipanti (campo "Ruolo");
5. dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato **per affare** deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (affare);
3. codice IPA Amministrazione titolare (campo "Ruolo");
4. codice IPA Amministrazioni partecipanti (campo "Ruolo");
5. dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato **per persona** deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo ("persona fisica" o "persona giuridica");
3. dati anagrafici della persona a cui fa riferimento il fascicolo (almeno nome e cognome per le persone fisiche, denominazione per le persone giuridiche, denominazione e codice IPA per le PA);
4. dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

Il fascicolo informatico organizzato **per attività** deve recare:

1. metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
2. tipologia di fascicolo (attività);
3. dati identificativi del RUP o dell'assegnatario dell'attività (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

43. Fascicolazione Ibrida

Il fascicolo ibrido è composto da documenti relativi ad uno stesso affare o procedimento amministrativo originati da due differenti supporti, uno cartaceo o analogico e un altro informatico, condizione che determina due unità archivistiche di conservazione differenti. L'unitarietà del fascicolo ibrido è garantita dall'indicazione della classe e del numero di fascicolo nella fase di protocollazione: per questa ragione, lo UOR di riferimento riporterà questi dati sul documento analogico oppure sulla copertina del fascicolo.

La gestione in ingresso dei documenti analogici è disciplinata seguendo le procedure indicate nell'articolo 40 del presente Manuale: sarà l'ufficio protocollo, pertanto, ad occuparsi della riproduzione digitale dei documenti analogici, che prevede l'apposizione di una etichetta barcode e l'annotazione "Documento analogico" sul documento.

Nel caso di documenti in uscita, sarà la UOR di riferimento ad incaricarsi della protocollazione, allegando copia analogica del documento

Sezione quarta – Flussi documentali interni

44. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnati alle UO Responsabili preventivamente individuate:

- i documenti di fatturazione acquisiti tramite il Sistema Di Interscambio (SDI);
- i documenti formati attraverso gli strumenti di acquisizione di istanze, comunicazioni e dichiarazioni per l'erogazione dei servizi online messi a disposizione degli utenti.

Ulteriori criteri di assegnazione automatica sono definiti dal Responsabile, sentite le UUOORR interessate.

I documenti non assegnati automaticamente sono assegnati alle UO Responsabili dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione (cfr. **allegato 6**). Quando un documento è di interesse anche per più UUOORR, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

45. Comunicazioni interne

Tutte le comunicazioni interne sono effettuate esclusivamente in modalità telematiche, ivi compresa la pubblicazione di avvisi e comunicazioni a carattere informativo.

Lo scambio di documenti tra il Servizio Segreteria Generale e Protocollo e le diverse UUOORR dell'Unione è effettuato per mezzo del Sistema di gestione documentale o, in alternativa, tramite comunicazioni posta elettronica ordinaria.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn). Comunicazioni e scambi di documenti tra gli uffici possono essere effettuati anche attraverso la rete intranet e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti, tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dall'Unione.

Lo scambio di documenti tra le UUOORR dell'Unione non richiede la protocollazione del messaggio.

Non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, Telegram, ecc.) per lo scambio di documenti nell'ambito dell'attività lavorativa.

46. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dall'Unione che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo l'avvenuta immodificabilità del documento (cfr. par. 15 del presente Manuale). Gli atti oggetto di notificazione tramite pubblicazione ai sensi del Codice di Procedura Civile, una volta ricevuti e scansionati, sono inseriti manualmente dal personale abilitato.

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

47. Sistema di conservazione dei documenti informatici

L'Unione Terre di Castelli, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale del sistema di conservazione di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato al Conservatore PARER (Servizio Polo Archivistico Regionale dell'Emilia-Romagna, d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al **Manuale di conservazione del Polo Archivistico Regionale - ParER (Allegato 9)**, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione (**allegato 10 - Disciplinare tecnico del servizio di conservazione**).

Per opportunità di carattere tecnico, i Mandati di pagamento, le Reversali di incasso prodotti dall'ente, le ricevute tecniche e di esecuzione sono conservate a norma mediante il sistema denominato "Unistorage" integrato presso il conservatore accreditato Unimatica-RGI s.p.a. - Bologna.

48. Responsabile della conservazione

Come precisato al par. 5 del presente Manuale, l'Unione ha designato un unico soggetto che riveste i ruoli di Responsabile della gestione documentale e Responsabile della conservazione.

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD dell'ente.

Il Responsabile, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

49. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dall'Unione e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico;
- gli altri registri e repertori tenuti dall'ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

- a) pacchetti di versamento;
- b) pacchetti di archiviazione;
- c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie documentarie oggetto del servizio di conservazione sono dettagliatamente individuate nel Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici sottoscritto dall'Unione unitamente alla convenzione di affidamento del servizio al Conservatore PARER.

50. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID e ulteriormente definiti nel Disciplinare tecnico del servizio di conservazione (**allegato 10**).

Il Responsabile, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato, purché conforme ai formati indicati adatti alla conservazione nell'allegato 2 alle Linee guida. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal Responsabile attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Seconda del presente Manuale.

51. Modalità e tempi di trasmissione dei pacchetti di versamento

All'inizio di ogni anno ciascuna UOR individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al Responsabile, che provvede alla formazione e alla trasmissione dei pacchetti di versamento, secondo le modalità operative definite nel manuale del Conservatore e nei documenti tecnici sull'affidamento del servizio.

Il Responsabile genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il Responsabile verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, richiede al produttore dell'oggetto di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento annuale, per cui ogni anno entro il mese di febbraio sono versati in conservazione tutti i documenti informatici dell'Unione, anche a fascicolo aperto;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti;
- versamento anticipato, nelle particolari ipotesi che richiedono un versamento in conservazione prima del versamento a cadenza annuale (ad esempio, documenti con certificato di firma in scadenza).

52. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica

I dati e i documenti informatici sono memorizzati nel Sistema di gestione documentale, che provvede all'archiviazione su server cloud qualificato dall' AgID ai sensi della normativa vigente.

Viene conservata su data center dell'Unione documentazione temporanea e di servizio formata negli anni precedenti alla pubblicazione del presente manuale che si intende fascicolare e metadattare.

Le procedure di memorizzazione sono le seguenti:

- a) salvataggio immediato su server di rete collocato presso la Sede dell'Unione;
- b) alla fine di ogni giorno sono create, a cura del Servizio sistemi informativi, copie di backup della memoria informatica dell'Amministrazione, che vengono poi riversate su supporti di memorizzazione tecnologicamente avanzati e

conservati nel Data Center adibito a *Disaster Recovery*, secondo quanto previsto dalle procedure di salvataggio dati descritte all'interno del **Piano di sicurezza informatica (Allegato 11)**.

53. Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati dal Responsabile possono accedere al Sistema tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

54. Selezione e scarto dei documenti

Periodicamente, secondo quanto previsto nel **Massimario di selezione e scarto (v. Allegato 12)** viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, con eventuale invio di proposta alla competente Soprintendenza Archivistica. Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Massimario di selezione e scarto.

55. Conservazione, selezione e scarto dei documenti analogici

La documentazione analogica corrente è conservata dai diversi responsabili del procedimento presso i diversi servizi e uffici fino al trasferimento presso gli Archivi Generali di Deposito dell'Ente.

Il trasferimento della stessa avviene secondo quanto predisposto dall'attuale Piano di Gestione dei Flussi Documentali, adottato con DGU n. 47 del 02.05.2019, che si intende completamente integrato all'interno del presente Manuale I versamenti della documentazione dagli archivi correnti agli Archivi Generali di Deposito avvengono, di norma, due volte l'anno, indicativamente nel corso dei mesi di giugno e dicembre. Il Responsabile, o suo delegato, segnalerà la scadenza in tempo utile ai diversi uffici che, se interessati, dovranno prendere contatto con il referente del Sistema Archivistico Intercomunale entro il mese precedente la data del versamento, comunicando la consistenza generale (in metri lineari o numero di faldoni) della documentazione da trasferire.

Il responsabile del Sistema Archivistico valuterà preventivamente le richieste dei singoli uffici con il personale del Polo Archivistico che dovrà incamerare la documentazione, al fine di garantire un'equa assegnazione degli spazi, in linea con la vigente Convenzione con la Fondazione di Vignola, approvata con DCU n. 12 del 03.03.2016, e relativi ampliamenti degli spazi stessi, come da DGU n. 94 del 02.09.2019. Si prevedono inoltre, qualora se ne ravvisi la necessità, sopralluoghi specifici per visionare la documentazione da trasferire.

Individuata la documentazione da versare agli Archivi Generali di Deposito, ogni ufficio provvederà preventivamente all'eliminazione dai fascicoli interessati di fotocopie, copie di servizio, stampe, appunti, buste, normativa ecc. che non contengono numeri di protocollo (attività di "scarto in itinere", escluso dalle procedure di scarto previste dall'art. 21, c. 1, lett. d) del D.Lgs. 42/2004 ss.mm.ii.).

La correttezza e completezza delle informazioni riportate sui dorsi delle buste/faldoni da versare è a cura dei singoli uffici e servizi e costituisce elemento imprescindibile ai fini del trasferimento. Tali informazioni saranno inserite all'interno di un "Elenco di versamento della documentazione cessata e sfoltita dall'archivio corrente all'archivio di deposito", che costituirà parte integrante di un verbale di versamento sottoscritto dal responsabile della UOR – o suo delegato – e dal referente del Polo Archivistico-storico.

Gli elenchi di versamento saranno conservati presso il Polo Archivistico-storico dell'Ente, a cura delle archiviste dello stesso, insieme al relativo "Registro dei versamenti dall'archivio corrente all'archivio di deposito e dall'archivio di deposito all'archivio storico", organizzato su base cronologica (**Modulistica versamenti documentazione analogica - Allegato n. 13**).

Le successive attività di descrizione della documentazione trasferita e di compilazione degli elenchi di scarto da inviare alla competente Soprintendenza Archivistica da parte del Responsabile della Gestione Documentale sono a cura delle archiviste del Polo, secondo quanto disposto dall'articolo 5 della Convenzione sopra citata. Lo scarto avviene sulla base di quanto disposto dall'articolo 21, c. 1, lett. d) del D.Lgs. 42/2004 ss.mm.ii.

56. Misure di sicurezza e monitoraggio dei documenti digitali

Il Manuale di Conservazione e il Piano della sicurezza del Conservatore descrivono le modalità con cui il fornitore del servizio 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*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti contrattuali previsti negli atti di affidamento del servizio.

PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

57. Sicurezza dei sistemi informatici dell'Unione.

Gli strumenti software indicati al par. 6 del Presente manuale, utilizzati per la formazione e gestione dei documenti informatici, sono resi accessibili al personale dell'Unione tramite servizi cloud (SaaS) qualificati dall'Agenzia per l'Italia Digitale e Data Center Unione. I servizi consentono altresì l'archiviazione dei documenti, prodotti mediante l'utilizzo dei software, nel rispetto degli standard di sicurezza previsti dalla normativa, garantendone così l'integrità e l'immodificabilità ai sensi delle Linee guida (cfr. parr. 2.1.1. e 3.9).

La memorizzazione dei documenti correnti, diversi da quelli formati con l'ausilio dei suddetti strumenti software, è effettuata sui server dell'Unione secondo le modalità indicate al par. 52, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore o della selezione per lo scarto. Le componenti architetturali e di sicurezza del sistema informatico dell'Unione sono descritte nell'**Allegato 11** al presente Manuale.

58. Amministratore di sistema

Il Responsabile del Servizio sistemi informativi svolge altresì il ruolo di Amministratore del Sistema di gestione documentale e provvede al rilascio e alla gestione delle credenziali di accesso al Sistema di gestione documentale, secondo i livelli di abilitazione definiti dal Responsabile; è istituito e mantenuto presso l'Ente l'apposito registro relativo agli amministratori di sistema ed un software che provvede alla registrazione degli accessi.

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

Per l'accesso ai sistemi informatici dell'Unione è necessaria l'assegnazione di un profilo utente, da parte del Responsabile, secondo quanto previsto al par. 8 del presente Manuale.

Ogni profilo è protetto da un sistema di credenziali (username e password). Al momento della creazione del profilo utente, sono attribuiti all'utente lo username e una password temporanea. Al primo accesso dell'utente, viene richiesto l'inserimento di una nuova password, mentre lo username resta invariato.

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. Ciascun dipendente deve associare al proprio profilo una password di almeno otto cifre, che preveda almeno una lettera maiuscola, una lettera minuscola, un numero e un segno (ad esempio: #, !, ?, -, &, ecc.). La password non deve mai coincidere con altre password associate ad altri profili o utenze (ad esempio, non si deve usare la stessa password del proprio account email personale).

L'Amministratore di sistema provvede affinché, periodicamente, per ogni profilo utente sia richiesto il rinnovo della password.

Ogni richiesta diretta al Fornitore per l'accesso – anche temporaneo – ai Sistema o la modifica delle credenziali profilo utente deve essere effettuata direttamente dall'Amministratore di sistema, su comunicazione del Responsabile.

60. Accesso alle postazioni di lavoro, ai locali e agli archivi dell'Unione

Essendosi costituita solamente a partire dal 2001, l'Unione Terre di Castelli non possiede un Archivio Storico, ma solamente un Archivio Generale di Deposito, conservato presso il Polo Archivistico-storico dell'Unione Terre di Castelli, via Papa Giovanni Paolo II 96, Vignola, sulla base alla Convenzione con la Fondazione di Vignola approvata con DCU n. 12 del 03.03.2016. Essa disciplina anche tempistiche e modalità per l'eventuale ritiro di documentazione da parte del personale dell'Ente e per l'evasione di richieste e accessi amministrativi inviati via mail dai diversi uffici e servizi.

Gli orari ed i recapiti del Polo Archivistico sono pubblicati sul sito web dell'Ente