

ETRA S.P.A. SOCIETÀ BENEFIT
MANUALE DI GESTIONE E CONSERVAZIONE DOCUMENTALE

Sommario

PARTE PRIMA – DISPOSIZIONI PRELIMINARI	5
1. Riferimenti normativi	5
2. Premessa metodologica	6
3. Finalità, contenuti e metodologia del documento	6
4. Approvazione, aggiornamento e pubblicazione del Manuale	7
PARTE SECONDA – ORGANIZZAZIONE	8
5. Area organizzativa omogenea e Unità Organizzative	8
6. Responsabili della gestione e conservazione documentale	8
7. Sistema informatico di gestione documentale della Società	9
8. Ufficio Protocollo e UO responsabili delle attività di protocollazione	10
9. Abilitazioni di accesso	11
PARTE TERZA – FORMAZIONE DEI DOCUMENTI	11
Sezione prima – Modalità di formazione	11
10. Modalità di formazione dei documenti amministrativi informatici	11
11. Creazione e redazione tramite software di documenti informatici	12
12. Elementi essenziali del documento amministrativo informatico	12
12.1 Documenti che non hanno natura amministrativa	13
13. Scelta del formato e modalità di sottoscrizione	13
14. Acquisizione di documenti informatici	14
15. Copie per immagine di documenti analogici	15
16. Duplicati, copie ed estratti informatici di documenti informatici	16
17. Acquisizione di istanze tramite moduli online	16
18. Formazione di registri e repertori	17
Sezione seconda – Disposizioni comuni a tutte le modalità di formazione	17
19. Dispositivi di firma elettronica	17
20. Scadenza dei certificati di firma	17
21. Identificazione univoca del documento informatico	18

22.	Associazione degli allegati al documento principale.....	18
23.	Accessibilità del documento informatico	19
24.	Metadati del documento informatico	20
25.	Immodificabilità e integrità del documento informatico	20
Sezione terza - Disposizioni sulla formazione di documenti analogici.....		21
26.	Copie analogiche di documenti informatici.....	21
27.	Casi in cui è ammessa la formazione o l'acquisizione di documenti originali analogici	22
PARTE QUARTA - GESTIONE DOCUMENTALE.....		23
Sezione prima - Flussi documentali esterni		23
28.	Ricezione telematica di documenti informatici in entrata	23
29.	Canali di ricezione	23
30.	Formati accettati	24
31.	Verifica sul formato dei documenti allegati.....	25
32.	Controllo dei certificati di firma.....	25
33.	Trasmissione telematica di documenti informatici in uscita	25
34.	Individuazione del domicilio digitale presso cui effettuare la comunicazione	26
35.	Modalità di consultazione ed estrazione dei domicili digitali contenuti negli elenchi pubblici	27
36.	Disposizioni sui documenti analogici.....	27
Sezione seconda - Protocollo informatico.....		28
37.	Sistema di protocollo informatico	28
38.	Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico	28
39.	Registro generale di protocollo	29
40.	Registro giornaliero di protocollo.....	29
41.	Documenti soggetti a registrazione di protocollo e documenti esclusi	29
42.	Protocollazione di documenti interni.....	31
43.	Disposizioni per particolari tipologie di documenti	31
44.	Registrazione di protocollo.....	31
45.	Modalità di registrazione	32
46.	Protocollazione delle comunicazioni pervenute alle caselle di posta elettronica ordinaria di utenti non abilitati alla protocollazione	33
47.	Annullamento e modifiche della registrazione di protocollo	34
48.	Gestione degli allegati.....	35

49.	Informazioni agli utenti rese dal responsabile del procedimento	36
50.	Tempi di registrazione e casi di differimento	36
51.	Segnatura di protocollo	37
52.	Protocollo riservato	38
53.	Registro di emergenza.....	38
54.	Documenti soggetti a registrazione particolare	39
Sezione terza - Disposizioni sulla protocollazione e gestione dei documenti analogici.....		40
55.	Protocollazione dei documenti analogici	40
56.	Registrazione, segnatura, annullamento	40
57.	Rilascio della ricevuta di avvenuta protocollazione	41
58.	Corrispondenza contenente dati particolari	41
59.	Corrispondenza personale o riservata	42
60.	Corrispondenza cartacea non di competenza della Società.....	43
Sezione quarta – Classificazione e fascicolazione		43
61.	Classificazione dei documenti amministrativi	43
62.	Fascicolazione informatica dei documenti amministrativi	43
Sezione quinta – Flussi documentali interni		44
63.	Assegnazione dei documenti in entrata agli uffici.....	44
64.	Comunicazioni interne	45
65.	Pubblicazioni nell'Albo pretorio e in Società Trasparente.....	45
PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI		46
66.	Sistema di conservazione dei documenti informatici	46
67.	Responsabile della conservazione.....	46
68.	Oggetti della conservazione.....	47
69.	Tempi di conservazione	47
70.	Formati ammessi per la conservazione	48
71.	Modalità e tempi di trasmissione dei pacchetti di versamento	48
72.	Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica (archivio corrente)	49
73.	Accesso al Sistema di conservazione	49
74.	Selezione e scarto dei documenti	49
75.	Conservazione, selezione e scarto dei documenti analogici	49
76.	Misure di sicurezza e monitoraggio del sistema di conservazione	50

PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI	50
77. Sicurezza dei sistemi informatici della Società ETRA S.p.A. Società Benefit ...	50
78. Amministratore di sistema.....	51
79. Uso del profilo utente per l'accesso ai sistemi informatici.....	51
80. Accesso alle postazioni di lavoro, ai locali e agli archivi della Società.....	51
PARTE SETTIMA – DISPOSIZIONI FINALI	52
81. Entrata in Vigore ed Efficacia.....	52

ALLEGATI

Allegato 1.	Atti di nomina RGD, RCD e Vicario
Allegato 2.	Manuali operativi del software “Sistema di gestione documentale”
Allegato 3.	Guida pratica per la creazione di un documento accessibile
Allegato 4.	Piano di classificazione (Titolario)
Allegato 5.	Piano di fascicolazione
Allegato 6.	Modello per registro di protocollo d'emergenza
Allegato 7.	Manuale di conservazione del Conservatore

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 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”) come modificato dal regolamento europeo 2024/1183 (Regolamento “eIDAS 2”);

- 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. Premessa metodologica

Per quanto concerne l'ambito di applicazione della disciplina sulla formazione, gestione e conservazione dei documenti informatici contenuta nel CAD, rileva in particolar modo quanto contenuto all'**art. 2, comma 3, CAD**, ai sensi del quale *“Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto”*.

Etra S.p.A. Società Benefit (d'ora in avanti anche solo “ETRA” o la “Società”), in qualità di soggetto gestore di pubblico servizio, con il presente documento disciplina le modalità di gestione informatica dei procedimenti e di produzione dei documenti digitali, assicurando che tali attività siano conformi alle disposizioni del Codice dell'Amministrazione Digitale (CAD) e delle relative Linee Guida emanate dall'AgID.

In particolare, ETRA si impegna a garantire che la formazione, la gestione e la conservazione dei documenti digitali rispettino gli standard normativi in termini di autenticità, integrità e leggibilità, adottando le tecnologie informatiche necessarie in tutte le fasi procedurali e nella gestione degli archivi.

Il presente Manuale definisce quindi le regole operative applicabili alle attività di gestione documentale svolte da ETRA, nel rispetto della normativa vigente e delle Linee Guida, assicurando la corretta gestione dei documenti digitali con valore probatorio.

3. 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 di ETRA 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 presente Manuale non concerne i documenti degli Enti Locali Soci, di cui ETRA è società strumentale. Per tali documenti, resta in capo ai soci la competenza e la responsabilità per il corretto espletamento delle attività di gestione documentale.

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 della Società.

Con la pubblicazione nella sezione “Società Trasparente” del sito internet istituzionale (sottosezione “Atti Generali”), il Manuale è reso noto anche esternamente alla Società. In quest’ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell’attività istituzionale.

4. Approvazione, aggiornamento e pubblicazione del Manuale

Il presente Manuale e i suoi allegati, come s.m.i., sono approvati, su proposta del Responsabile della gestione documentale e del Responsabile della conservazione documentale di cui al successivo par. 6, con delibera del Consiglio di Amministrazione della Società del 22 aprile 2025 e successiva del 26 giugno 2025.

I successivi aggiornamenti del Manuale e degli allegati devono essere approvati con le medesime modalità. Sono da considerarsi modifiche sostanziali quelle che incidono sulla struttura organizzativa della Società, nonché le modifiche aventi a oggetto i tempi di conservazione dei documenti.

PARTE SECONDA – ORGANIZZAZIONE

5. Area organizzativa omogenea e Unità Organizzative

ETRA si configura come un'unica Area Organizzativa Omogenea ("AOO"), cui è associato il registro unico di protocollo di cui al par. 39 del presente Manuale.

L'AOO e il domicilio digitale associato al registro unico di protocollo sono pubblicati nell'Indice PA, in ottemperanza a quanto previsto dall'art. 47, comma 3, CAD, e sono identificati dal seguente codice univoco: A047E4E.

Le Unità Organizzative ("UO") e le Unità di Processo ("UP") che afferiscono alla AOO sono riportate nell'organigramma di cui all'allegato 3 alla PR 101, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa della Società. Le UO sono individuate in modo da rispecchiare l'organigramma della Società.

6. Responsabili della gestione e conservazione documentale

La Società, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato due figure, dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale e del Responsabile della conservazione di cui rispettivamente ai paragrafi 3.4 e 4.5 delle Linee guida.

I Responsabili della gestione documentale e della conservazione, così come il vicario del Responsabile della gestione documentale, per i casi di vacanza o assenza, sono individuati con delibera del Consiglio di Amministrazione della Società UO(**Allegato 1**).

I compiti dei Responsabili della gestione e della conservazione documentale (d'ora in avanti anche solo, rispettivamente, "**RGD**" e "**RCD**". Il RGD e il RCD, congiuntamente, i "**Responsabili**") sono definiti nell'atto di nomina e nel presente Manuale. In particolare,

il RGD:

- a. provvede, previo parere del Responsabile per la Protezione dei Dati personali (Data Protection Officer - DPO), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
- b. monitora i processi e le attività che governano le fasi di formazione e gestione dei documenti informatici;
- c. valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;

- d. 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;
- e. richiede al referente della sicurezza informatica di ETRA un periodico censimento degli strumenti *software* di gestione documentale in uso presso la Società e la verifica di conformità degli stessi alla normativa vigente;

il RCD:

- f. monitora i processi e le attività che governano le fasi di versamento in conservazione dei documenti informatici;
- g. assicura la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione;
- h. provvede, sotto il profilo organizzativo e gestionale, ad assicurare l'interfacciamento e il collegamento del *software* di gestione documentale aziendale con il sistema di conservazione digitale dei documenti informatici gestito dal Conservatore e comunica a quest'ultimo i nominativi e le funzioni dei soggetti abilitati all'accesso al sistema di conservazione;
- i. verifica il corretto svolgimento dell'attività di conservazione, anche eventualmente consultando o estraendo i documenti depositati e le prove di conservazione, secondo le modalità previste nella documentazione tecnica relativa all'affidamento del servizio.

Per l'espletamento delle funzioni di cui alla lettera (d) che precede, la UO Amministrazione del Personale, Budget comunica al RGD ed al Referente Privacy le nuove assunzioni, spostamenti, cessazioni, affinché il RGD possa, a seconda dei casi, autorizzare o disconnettere le abilitazioni, dando all'uopo disposizione al competente Amministratore di Sistema.

Ferma restando la propria responsabilità nello svolgimento dei compiti affidati, i Responsabili possono delegare il personale posto sotto la propria direzione per lo svolgimento di una o più attività.

7. Sistema informatico di gestione documentale della Società

1. La Società, per la gestione della corrispondenza in entrata ed in uscita, si avvale di un apposito sistema *software* gestionale (d'ora in avanti il "**Sistema**"), che garantisce le seguenti funzionalità:

- (i) protocollazione dei documenti e tenuta del protocollo informatico;
- (ii) invio dei documenti informatici a caselle PEC e ordinarie;
- (iii) acquisizione dei documenti informatici provenienti da caselle PEC e ordinarie;
- (iv) sistema di *workflow* per l'assegnazione dei documenti informatici agli uffici.

2. Dalla Data di Efficacia Differita (come sotto definita), il Sistema garantirà le seguenti ulteriori funzionalità, integrate con quelle di cui da sub 1(i) a 1(iv):

- (i) sistema di *workflow* per lo scambio e la lavorazione dei documenti da parte degli uffici;
- (ii) creazione e gestione dei fascicoli informatici;
- (iii) gestione dell'iter di approvazione degli atti amministrativi;
- (iv) pubblicazione degli atti nella sezione società trasparente del sito istituzionale della Società.

La puntuale descrizione delle componenti e delle funzionalità dei software di cui si compone il Sistema è rinvenibile nei relativi manuali operativi di cui all' **Allegato 2** al presente Manuale.

8. Ufficio Protocollo e UO responsabili delle attività di protocollazione

La protocollazione dei documenti in entrata è gestita in maniera centralizzata dal personale dell'Unità di Processo denominata "Protocollo" (di seguito anche "**Ufficio Protocollo**" o "**PROT**"), facente parte della UO Affari Societari e Legali. L'Ufficio Protocollo è responsabile dell'organizzazione e della gestione dei servizi di protocollazione e flussi documentali, inclusi smistamento e assegnazione della corrispondenza. Nello specifico, il PROT è identificato come Unità di Processo incaricata della protocollazione generale di tutta la corrispondenza in entrata e provvede a distribuire i protocolli agli uffici o alle aree competenti.

In linea con la nuova organizzazione, si prevede il collegamento al gestionale unico di protocollazione di altre 4 caselle PEC dedicate una all'Ufficio Legale, una all'Ufficio Amministrazione del Personale e due all'Area Commerciale (di seguito, il **Protocollo Diffuso**)¹. Tali caselle saranno accessibili esclusivamente dalla Coordinatrice e dal responsabile dell'Ufficio Protocollo, oltre che – su specifica autorizzazione del RGD - da personale abilitato delle predette 4 Unità Operative/Area interessate, che per le specifiche attività di protocollazione, risponderà funzionalmente al responsabile dell'Ufficio Protocollo. La protocollazione della posta in entrata ed in uscita a/di tali caselle PEC sarà effettuata attribuendo il numero di protocollo generale, e dunque secondo l'ordine generativo generale di tale numerazione.

Per quanto riguarda la protocollazione dei documenti informatici in uscita, tutti i dipendenti a cui è assegnata un'utenza per l'abilitazione d'accesso al Sistema informatico di gestione documentale della Società sono abilitati alla c.d. "predisposizione in uscita", sul Sistema medesimo, dei documenti, che poi saranno protocollati ed inviati a cura di PROT o del Protocollo Diffuso, con esclusione degli

¹ Ufficio Legale: ufficiolegale@pec.etraspa.it; Ufficio Personale: personale@pec.etraspa.it; Area Commerciale: contenzioso.crediti@pec.etraspa.it; recuperocrediti@pec.etraspa.it

utenti a cui sono attribuite funzioni di mera consultazione. La protocollazione in uscita, dunque, è affidata al personale dell'Ufficio Protocollo, nonché a quello autorizzato al Protocollo Diffuso.

Il RGD, con proprio provvedimento, può individuare ulteriori UO responsabili per la protocollazione in entrata e in uscita, che dunque faranno parte del Protocollo Diffuso.

Ciascun dirigente e/o responsabile di servizio provvede a individuare, all'interno delle unità organizzative poste sotto la propria direzione, ed a comunicare al RGD, per le finalità di cui al successivo paragrafo 9, i delegati alle attività di "predisposizione in uscita", sul Sistema informatico, dei documenti che PROT o il Protocollo Diffuso dovranno poi protocollare ed inviare, tra il personale in possesso di adeguate competenze in materia.

Sulle regole da seguire per la gestione dei flussi documentali, in ingresso e in uscita, e per la protocollazione o diversa modalità di registrazione dei documenti della Società, si rinvia alle indicazioni contenute nella Parte Quarta del presente Manuale.

9. Abilitazioni di accesso

Le abilitazioni di accesso degli utenti alle componenti del Sistema informatico di gestione documentale della Società sono assegnate personalmente a ciascun dipendente dalla UO ICT, previa autorizzazione del RGD rilasciata su richiesta del responsabile della UO a cui il dipendente appartiene.

In caso di nuove assunzioni, spostamenti e/o cessazione del rapporto di lavoro, sarà onere del dirigente dell'area Personale Relazione Cultura darne comunicazione al RGD affinché questi a seconda dei casi, sentito il responsabile del relativo ufficio, disponga l'abilitazione o l'interruzione della abilitazione di accesso.

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

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Sezione prima – Modalità di formazione

10. Modalità di formazione dei documenti amministrativi informatici

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

I documenti informatici degli uffici della Società 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 365*, *Google Workspace* 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 oppure mediante l'utilizzo della funzione del sistema operativo "duplica");
- 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);
- e) intelligenza artificiale.

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

11. Creazione e redazione tramite software di documenti informatici

Per la creazione dei documenti informatici mediante redazione, gli uffici della Società dispongono di strumenti software con funzioni di text editing, anche integrati con gli applicativi gestionali per la formazione di documenti e atti amministrativi.

Il testo del documento informatico creato dagli uffici della Società deve essere redatto, su carta intesta della Società, tempo per tempo diffusa e reperibile nella sezione "Documenti Utili" presente in Intranet, utilizzando esclusivamente uno dei seguenti font: Arial e Verdana.

12. Elementi essenziali del documento amministrativo informatico

Ogni documento amministrativo informatico creato e redatto dalla Società deve recare i seguenti elementi:

1. denominazione della Società;

2. autore e ufficio responsabile;
3. oggetto del documento;
4. riferimenti a procedimento o fascicolo;
5. sottoscrizione;
6. data e luogo;
7. numeri di pagina²;
8. indicazione degli allegati (se presenti);
9. identificazione e dati dei destinatari (se si tratta di documento in uscita);
10. dati della Società (compresi p.iva, indirizzo e recapiti, se si tratta di documento in uscita);
11. mezzo di spedizione (se documento in uscita).

Per determinate tipologie di atti l'operatore deve utilizzare i modelli resi disponibili tramite *workflow* all'interno del software di gestione documentale.

12.1 Documenti che non hanno natura amministrativa

I documenti privi di natura amministrativa (ad esempio, atti di gestione del personale, scritture private, libri sociali, atti degli organi societari ecc.) devono recare i medesimi elementi, ad eccezione di eventuali riferimenti al procedimento amministrativo. Si precisa, come meglio chiarito al **par. 27**, che per ragioni di efficienza e organizzazione, la formazione in originale informatico costituisce la prassi che tutti gli uffici sono tenuti a seguire, tranne nel caso in cui motivate ragioni impongano di continuare a formare originali analogici.

13. Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico creato dalla Società, oppure esportato da Piattaforma SAS e salvato nei sistemi della Società, deve essere scelto tra i seguenti **formati standard**: **.pdf, .pdf/a, .xml, .odt, .docx, .xlsx, .ods., .doc; .xsl; .zip; .p7m**. 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, .heic; .heif**;
- per i **dati strutturati** devono essere adottati i seguenti formati: **.sql, .csv., .accdb**.³

² Salvo che l'inserimento del numero di pagina non si renda possibile a causa di caratteristiche di impaginazione e grafiche (ad. es., per documenti progettuali)

³ Oltre ai seguenti formati: 1) previsti nell'Allegato 2 "Formati dei file e riversamento" delle Linee Guida (l'Allegato 2): ifc, json, kml, shp, txt, dxf, bmp, mpeg e mp4; e 2) non previsti nell'Allegato 2: (i) .rvt, .rcp, .rcs, .fls, .ptx, .ptg, .ppt, .dwg, e (ii) .obj, .bcf, .qgz, .cfg, .qml, .gpkg, .las, .xyz, .e57, .ids, .dbf.

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 i formati *standard* previsti nell'Allegato 2 alle Linee guida dell'AgID ed adottato osservando le raccomandazioni ivi contenute. Per tale ragione, ove si necessiti di utilizzare un formato differente da quelli di cui al presente paragrafo 3, dovrà essere richiesto preventivamente alla UO ICT di verificare se esso rientra tra i formati *standard* previsti nel citato Allegato 2 e rispetti le raccomandazioni prescritte nella Linee Guida AgID e potrà essere utilizzato solo se tale verifica dia esito positivo.

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 .doc 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 degli organi societari, i contratti, gli atti formati nell'ambito dell'attività di carattere amministrativo, ecc.), 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 preferibilmente con firma PADES.

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

14. Acquisizione di documenti informatici

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

- a) acquisizione di un duplicato 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 duplica un file trasferendolo 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, memorizzando la copia in formato digitale);

I Formati sub 2: (i) sono formati sotto licenza proprietaria leggibili da software proprietari e (ii) sono formati aperti come definiti all'art. 68, comma 3 del CAD; (i) e (ii) sono formati utilizzati dall'area tecnica della Società per la gestione del sistema informativo territoriale e per l'attività di progettazione delle reti e degli impianti, impiegati in particolare per i modelli grafici, modelli informativi, dataset/listato, Elaborati grafici, presentazioni.

- c) acquisizione della copia informatica di un documento analogico (ciò avviene, ad esempio, quando un documento analogico di testo 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), può essere necessario assicurarne l'efficacia giuridico-probatoria, attraverso l'associazione o l'apposizione dell'attestazione di conformità della copia al documento originale. A tal fine, occorre seguire le modalità indicate nei paragrafi successivi (cfr. **parr. 15 e 16**).

In caso di acquisizione di un duplicato informatico (v. *supra*, lett. a), ai sensi dell'art. 23-bis del CAD, il documento acquisito ha la stessa efficacia giuridico-probatoria del documento informatico originale, pertanto, non è mai richiesta l'attestazione di conformità.

15. 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.

Di norma, i documenti cartacei trasmessi alla Società sono scansionati e acquisiti in copia digitale "semplice", per esigenze di uso lavoro e consultazione.

Tuttavia, nel caso in cui si debba garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale⁴, potrà essere effettuata l'attestazione di conformità della copia per immagine all'originale:

- a. da un pubblico ufficiale (notaio o responsabile del procedimento amministrativo formalmente designato), tramite apposizione dell'attestazione di conformità in calce al documento o su foglio separato ma congiunto al documento, poi firmato digitalmente⁵;
- b. oppure, mediante la certificazione del processo di dematerializzazione, in conformità a quanto previsto dall'allegato 3 delle Linee guida AgID.

⁴ In particolare, come già precisato al p.to 26 del Manuale, è necessario assicurare l'efficacia giuridico-probatoria delle copie informatiche di documenti analogici nei seguenti casi:

- quando il documento riveste rilevanza legale o probatoria, ad esempio contratti, atti pubblici, atti amministrativi o certificati;
- qualora il documento debba essere utilizzato in un procedimento giudiziario o amministrativo, quale elemento probatorio o a supporto di una decisione;
- se la copia informatica sostituisce l'originale per legge o per prassi consolidata, come nel caso di documenti notificati o copie di atti depositati;
- quando il documento deve essere inviato o conservato secondo modalità che garantiscano la conformità e l'integrità rispetto all'originale, assicurando l'autenticità del contenuto e la sua idoneità probatoria.

⁵ La dicitura di conformità da utilizzare è la seguente: "Si attesta che la presente copia per immagine è conforme all'originale analogico ai sensi dell'art. 22, comma 2, del D.Lgs. n. 82/2005".

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.

16. 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 effettua un download, oppure, quando si duplica un documento nella memoria del proprio computer o verso dispositivo di archiviazione esterno). 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.

L'identità tra due documenti informatici è rilevabile tramite il raffronto delle impronte *hash*. L'impronta *hash* di un documento informatico è una sequenza di lettere e cifre (lunga solitamente 64 caratteri), ottenuta applicando un particolare algoritmo di calcolo alla sequenza di bit che formano il *file* (per la verifica delle impronte *hash* è possibile utilizzare le funzioni del sistema di gestione documentale o appositi *software*).

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 documenti 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 abbia la medesima efficacia giuridico-probatoria, è necessario attestare la conformità della copia all'originale.

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.

17. 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 dalla Società, resi accessibili

previa identificazione dell'utente tramite le credenziali rilasciate agli utenti identificati dalla Società.

I dati immessi dall'istante sono memorizzati su supporto informatico. Le istanze e le dichiarazioni così formate costituiscono a tutti gli effetti documenti amministrativi informatici, acquisiti in interoperabilità dal Sistema di protocollo informatico e trattati come documenti in entrata soggetti a registrazione di protocollo, secondo le modalità definite nella Parte Quarta del presente Manuale.

18. Formazione di registri e repertori

I registri e repertori tenuti dalla Società, 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. Restano salve le speciali disposizioni che prescrivono la formazione di registri e repertori come documento originale analogico.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

19. Dispositivi di firma elettronica

ETRA garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma digitale o firma elettronica qualificata.

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.

Dall'entrata in vigore del Manuale: (i) ciascun titolare di un dispositivo di firma elettronica comunicherà alla UO ICT la data di scadenza del rispettivo certificato di firma; (ii) la UO ICT censirà le predette scadenze al fine del loro monitoraggio, e; (iii) la UO ICT provvederà al rinnovo dei certificati prima della scadenza della loro validità.

20. Scadenza dei certificati di firma

La UO ICT verifica periodicamente la validità e la data di scadenza del certificato di firma del dispositivo di firma elettronica attribuito ai dipendenti di ETRA, al fine di provvedere tempestivamente al rinnovo. Per tale finalità, dall'entrata in vigore del presente Manuale: (i) ciascun titolare di un dispositivo di firma comunicherà alla UO ICT la data di scadenza del rispettivo certificato di firma; (ii) la UO ICT censirà le

predette scadenze al fine del loro monitoraggio, e; (iii) la UO ICT provvederà al rinnovo dei certificati prima della scadenza della loro validità.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, la UO ICT ne dà comunicazione al titolare del dispositivo di firma, affinché quest'ultimo provveda a costituire un riferimento temporale giuridicamente valido 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.

21. 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 del numero di protocollo o, per i documenti soggetti a registrazione particolare (cfr. **par. 54**), del numero del registro o repertorio sostitutivo del protocollo.

Per i documenti informatici soggetti a registrazione di protocollo, inoltre, è prevista l'associazione dell'impronta *hash* del file, effettuata al momento della registrazione tramite le apposite funzioni del Sistema di protocollo informatico della Società. 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).

22. Associazione degli allegati al documento principale

Gli allegati vengono collegati in modo univoco al documento informatico principale attraverso un sistema di associazione basato sulle impronte *hash*. In particolare, ogni allegato viene elaborato da un algoritmo di *hashing* che genera una stringa univoca (l'impronta *hash*), che rappresenta in modo univoco il contenuto di quel documento. Questa stringa è come un "codice identificativo digitale" unico per il file allegato: anche una minima modifica del contenuto dell'allegato cambierebbe completamente l'impronta *hash*, rendendo evidente qualsiasi alterazione.

Le impronte *hash* degli allegati vengono quindi associate e integrate al documento informatico principale. Questo processo garantisce:

- i) integrità: è possibile verificare in ogni momento che il contenuto degli allegati non sia stato modificato, poiché eventuali variazioni genererebbero un'impronta *hash* diversa rispetto a quella originariamente associata;
- ii) univocità: gli allegati possono essere identificati e riconosciuti in modo certo e inconfondibile in relazione al documento principale, impedendo errori o sostituzioni;
- iii) validità legale: questa modalità di associazione contribuisce a garantire la conformità alle normative sulla gestione dei documenti informatici, come richiesto dal Codice dell'Amministrazione Digitale (D.lgs. 82/2005) e dalle regole tecniche sulla formazione e gestione dei documenti digitali.

In altre parole, l'impronta *hash* funge da "impronta digitale" degli allegati e consente di stabilire un legame inscindibile e verificabile tra ciascun allegato e il documento principale, assicurando che l'intero fascicolo digitale mantenga la sua autenticità e affidabilità nel tempo.

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.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso (o, in alternativa, su foglio separato) l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta *hash*. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto immodificabile (ad esempio, dopo l'apposizione della firma digitale – cfr. **par. 25** del presente Manuale).

23. 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 3** al presente Manuale.

24. 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, secondo le indicazioni dei responsabili dei servizi e in conformità alle Linee guida.

L'associazione dei metadati al documento è effettuata tramite le apposite funzioni per la formazione degli atti del Sistema di gestione documentale. A tal fine, il responsabile della UO ICT verifica la conformità degli strumenti software utilizzati e, eventualmente, richiede al fornitore i necessari interventi evolutivi, all'uopo informando il RGD.

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

25. 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 della Società 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 garantita la conformità agli standard indicati nelle Linee guida (cfr. allegato 4 delle LL.GG.) e il rispetto delle misure di sicurezza;
- per tutte le tipologie documentali, dal versamento nel sistema di conservazione, conforme alle Linee guida e, in caso di esternalizzazione del servizio, alla determina AgID n. 455/2021, recante *Regolamento sui criteri per la fornitura di servizi di conservazione dei documenti informatici*.

Pertanto, è essenziale che tutti i documenti rilevanti per la Società siano versati in conservazione, secondo i tempi e le modalità descritte nella Parte Quinta del presente Manuale.

Si considerano "rilevanti" per la società i seguenti documenti:

- **documenti contabili e fiscali** (fatture elettroniche, libri e registri obbligatori, dichiarazioni fiscali, prove documentali di operazioni finanziarie, estratti conto bancari e ricevute);
- **atti societari** (atto costitutivo e statuto, verbali delle assemblee e del consiglio di amministrazione, delibere societarie, contratti e procure e deleghe);
- **documenti del personale** (contratti di lavoro, cedolini paga, registro presenze, documentazione relativa a malattie, infortuni e maternità e comunicazioni obbligatorie ai centri per l'impiego);⁶
- **documenti relativi alla sicurezza sul lavoro** (piani di emergenza e evacuazione, attestati di formazione e certificazioni del personale, verbali e relazioni periodiche del medico competente);
- **documenti relativi alla privacy e alla protezione dei dati personali** (Registro dei trattamenti ai sensi del GDPR, consensi informati raccolti, nomine e istruzioni a responsabili e autorizzati al trattamento);
- **documenti amministrativi e operativi** (documentazione legata agli appalti e forniture, autorizzazioni, licenze e certificati, progetti, report tecnici, e manuali operativi).

Il RCD assicura che i documenti informatici a cui è apposta una firma elettronica siano versati in conservazione prima che scada il certificato di firma.

Sezione terza - Disposizioni sulla formazione di documenti analogici

26. 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 stesso⁷. Quando il

⁶ Il libro unico del lavoro (cedolini+presenze) è oggetto di archiviazione ottica sostitutiva tramite CREDEMTEL. Le pratiche Inps/Inail/comunicazioni obbligatorie sono protocollate ed archiviate direttamente dalle/nelle piattaforme di riferimento.

⁷ Il soggetto responsabile è colui che materialmente o formalmente attesta la conformità del documento analogico all'originale digitale. La sua identificazione deve essere chiara e riportata nella certificazione di

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 sottoscrittore.

La copia analogica, 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 la Società (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 della Società ETRA S.p.A., presso cui è disponibile per l’accesso. NOME/COGNOME/UO di appartenenza di chi appone la dicitura di conformità”*).

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

27.Casi in cui è ammessa la formazione o l’acquisizione di documenti originali analogici

Fermo restando l’obbligo di produrre i propri documenti amministrativi in originale informatico, nella prospettiva di una gestione omogenea e integrata dell’archivio della Società, il personale è tenuto a preferire gli strumenti informatici per la formazione di tutti i documenti prodotti. Documenti in originale analogico potranno essere prodotti o acquisiti solo nel caso in cui il soggetto che li sottoscrive non sia munito di un dispositivo di firma digitale. Inoltre, è legittimo formare o acquisire documenti in originale analogico:

- a) quando si acquisisce un documento analogico, consegnato a sportello o a mezzo posta, e il richiedente è un soggetto privato che non agisce in qualità di professionista;
- b) in tutti i casi in cui per legge o regolamento il documento deve essere formato e/o rilasciato in formato cartaceo;
- c) in tutti i casi in cui il documento debba poi essere notificato in cartaceo a mezzo Ufficiale Giudiziario.

conformità. Gli elementi da includere sono: • nome e cognome del responsabile; • ruolo e qualifica del soggetto, specificando il contesto organizzativo (ad esempio, funzionario delegato, responsabile della gestione documentale); • eventuale abilitazione o autorizzazione a svolgere tale attività, se prevista dalla normativa interna o esterna; • firma autografa o digitale, ove richiesto, per formalizzare l’attestazione di conformità.

PARTE QUARTA - GESTIONE DOCUMENTALE

Sezione prima - Flussi documentali esterni

28. 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.

I documenti informatici trasmessi per via telematica nell'ambito di procedimenti amministrativi (cfr. par. 12), quali istanze, dichiarazioni e comunicazioni devono ritenersi valide a tutti gli effetti di legge nei casi previsti dall'art. 65, CAD. È fatto salvo il caso di individuazione di particolari modalità di trasmissione nell'ambito del procedimento (ad es. gare su piattaforma di *e-procurement*).

È vietata l'acquisizione o la trasmissione di documenti soggetti a protocollazione, e relativi allegati, tramite canali diversi da quelli previsti dalla Società (ad es. strumenti personali per il trasferimento dei file, caselle di posta ordinaria aziendale, etc.). Ove fossero trasmessi alla Società documenti soggetti alla protocollazione, e relativi allegati, tramite invio a caselle di posta ordinaria aziendale diverse da quelle di cui all'art. 29, tali documenti, unitamente ai loro allegati ed alla mail di trasmissione, dovranno essere inoltrati alle caselle di posta di cui al citato art. 29 e protocollati da PROT, secondo le modalità indicate al successivo art. 46.

29. Canali di ricezione

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

- casella PEC di PROT: protocollo@pec.etraspa.it;
- casella PEC di PROT: protocollo1@pec.etraspa.it (per ricezioni/invii massivi);
- casella di posta ordinaria di PROT: info@etraspa.it;
- casella di posta ordinaria di PROT: disservizirifiuti@etraspa.it;
- caselle di cui all'art. 8;
- altri canali di trasmissione indicati per specifici procedimenti.

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

Nel caso in cui un soggetto tenuto a effettuare comunicazioni di rilievo pubblicistico esclusivamente in via telematica (imprese, professionisti e cittadini, quando

espressamente previsto dalla disciplina del procedimento⁸; altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici della Società comunicazioni e documenti in modalità analogica, questi non saranno ritenuti correttamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell'UO 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 le modalità di trasmissione corrette. La comunicazione, quando reperibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-bis, 6-ter o 6-quater del CAD (INI-PEC, IPA, INAD, v. sul punto **par. 34** sull'individuazione del domicilio digitale).

30. 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, .doc, .xsl, .zip, .p7m**. 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, .heic, .heif**;
- per i **dati strutturati** devono essere preferibilmente accettati i seguenti formati: **.sql, .csv, .accdb**.

Per singoli processi possono essere accettati, previa autorizzazione del responsabile della UO ICT, anche altri 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.

È possibile protocollare un documento in qualunque formato, purché sia accompagnato da una copia informatica del documento in uno dei formati ammessi.

⁸ Si tratta di un riferimento a:

- a. procedimenti amministrativi specifici per i quali la disciplina del procedimento stabilisce modalità di comunicazione telematica obbligatoria, per esempio:
 - in ambito edilizio, tramite l'utilizzo di sportelli unici digitali.
 - nella presentazione di domande o istanze a enti pubblici, come avviene per il SUAP (Sportello Unico per le Attività produttive) o per il SUE (Sportello Unico per l'Edilizia).
 - per la partecipazione a gare e appalti pubblici, attraverso piattaforme telematiche di e-procurement.
- b. obblighi specifici per imprese e professionisti:
 - obbligo di PEC (Posta Elettronica Certificata): Imprese e professionisti iscritti a ordini o albi sono tenuti a comunicare esclusivamente tramite PEC (art. 16 del D.lgs. 185/2008 e art. 37 del D.lgs. 76/2020);
 - fatturazione elettronica: Imposta obbligatoriamente per le operazioni verso la PA e, in molti casi, anche tra privati (art. 1, comma 3, D.lgs. 127/2015).

Qualora pervengano documenti in formati non conosciuti o non gestiti, non si procederà alla protocollazione e PROT o il Protocollo Diffuso comunicheranno al mittente: (i) la mancata protocollazione in ingresso stante la mancata accettazione del formato; e; (ii) l'indicazione dei formati accettati.

L'accettazione di formati non previsti dal Manuale o 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 può essere riversato in altro formato tra quelli ammessi.

31. Verifica sul formato dei documenti allegati

L'eventuale presenza di allegati al documento principale in formati non ammessi deve essere verificata da PROT, il quale provvede a comunicare al mittente la non conformità del documento e/o l'assenza dei requisiti previsti per l'utilizzo ai fini del procedimento amministrativo.

L'accettazione di 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.

32. 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 al **par. 47** del presente Manuale). Il responsabile del procedimento, inoltre, valuta le azioni da intraprendere a seconda della tipologia di procedimento.

33. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, tramite le caselle di cui all'art. 8, salvo il caso di trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD o in caso di notifica degli stessi a mezzo di un Ufficiale Giudiziario.

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.

Per la trasmissione di documenti tramite PEC, se il documento principale non ha un contenuto sufficientemente esplicativo (ad esempio, un provvedimento, un

certificato, ecc.) deve essere predisposta una nota di accompagnamento alla trasmissione.

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC o, qualora il destinatario non disponga di un indirizzo di posta certificata, a mezzo raccomandata A.R.

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

34. Individuazione del domicilio digitale presso cui effettuare la comunicazione

La notificazione o comunicazione **a un soggetto privato** (cittadino o ente privato, ad es. associazione), 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 speciale per particolari atti, procedimenti o affari, all'indirizzo PEC espressamente dichiarato dal cittadino;
- II. in assenza di elezione di domicilio digitale speciale, al domicilio digitale generale eletto nell'INAD (Indice Nazionale dei Domicili digitali), accessibile all'URL domiciliodigitale.gov.it. La consultazione e l'estrazione automatica dei domicili digitali deve essere effettuata con le modalità di cui al paragrafo successivo;
- III. in assenza di alcun domicilio digitale eletto, al domicilio fisico, trasmettendo la copia cartacea del documento. Se si tratta di documento sottoscritto dall'organo di rappresentanza della Società, la copia analogica deve essere prodotta in conformità a quanto previsto ai parr. 25 e 26 del presente Manuale.

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 la Società e il destinatario.

Quando l'indirizzo PEC del soggetto destinatario (professionista o impresa) non risulti attivo, si provvede alla notificazione al domicilio fisico. Inoltre, la circostanza deve essere segnalata, da PROT o dal Protocollo Diffuso, alla Camera di Commercio competente per la registrazione nel registro delle imprese o al soggetto competente per la tenuta dell'albo o registro presso cui il professionista è tenuto all'iscrizione.

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

Nei casi in cui dalla comunicazione dipende il decorso, la sospensione o l'interruzione di termini di legge o, comunque, quando il suo contenuto impegni la Società verso l'esterno, la trasmissione è sempre effettuata via PEC, o laddove il destinatario non disponga di un indirizzo di posta certificata, a mezzo raccomandata A.R.

35.Modalità di consultazione ed estrazione dei domicili digitali contenuti negli elenchi pubblici

La consultazione degli elenchi pubblici INAD, INI-PEC e IPA è sempre garantita liberamente, senza necessità di autenticazione dell'utente.

In caso di notificazioni massive con estrazioni multiple, è opportuno ricorrere all'estrazione dei domicili digitali in modalità applicativa, cioè in interoperabilità tra elenco pubblico e Sistema di gestione documentale.

I domicili digitali devono essere acquisiti nel momento stesso in cui si intende utilizzarli, al fine di assicurare la qualità del dato, nonché di limitare il trattamento di dati personali. Pertanto, non devono essere archiviate estrazioni statiche dei domicili digitali presenti negli elenchi al fine di costituire una banca dati anagrafica del Sistema di gestione documentale della Società.

La prova circa l'effettiva esistenza di un dato domicilio digitale in un dato momento è conservata dal gestore dell'elenco pubblico.

36.Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire alla Società attraverso:

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

I documenti provenienti dal servizio postale tradizionale o da corrieri autorizzati o da Ufficiali Giudiziari sono consegnati all'Ufficio Protocollo o al personale di sportello autorizzato a protocollare presso le sedi territoriali, che provvede alla registrazione e, laddove non si proceda alla creazione di una copia digitale con attestazione di conformità, al deposito dei documenti nell'apposito casellario in cui vengono ritirati a cura dei singoli uffici.

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 e dal numero di utenti presenti in quel momento.

Nel caso di presentazione che necessitino di protocollazione immediata, l'operatore dell'Ufficio Protocollo provvede alla protocollazione contestualmente alla presentazione della pratica. Nel caso di ricezione dei documenti informatici, l'informazione al mittente dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dalla Società.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti. Pertanto, all'atto della protocollazione, dovrà procedersi alla formazione di un'unica copia digitale della busta e del documento contenuto nella busta medesima.

La ricezione di documenti a mezzo fax provenienti dalle pubbliche amministrazioni è esclusa (come previsto dall'art. 47, comma 2, lett. c del CAD).

Sezione seconda - Protocollo informatico

37. Sistema di protocollo informatico

ETRA, per la protocollazione dei documenti, utilizza un Sistema di protocollo informatico che, dalla Data di Efficacia Differita, sarà integrato con il Sistema di gestione documentale. La puntuale descrizione funzionale e operativa del Sistema di protocollo informatico è illustrata nel manuale di utilizzo di cui all'**allegato 2**.

È vietata l'acquisizione o la trasmissione di documenti soggetti a protocollazione e relativi allegati tramite canali diversi da quelli messi a disposizione dalla Società (ad es. strumenti personali per il trasferimento dei file).

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

La corretta tenuta del protocollo informatico è garantita dal RGD. In particolare, il RGD, con il supporto operativo del responsabile della UP PROT (laddove le due figure non coincidano):

- 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 utenti delegati dal RGD. La modalità di individuazione dei soggetti delegati alle attività di protocollazione è definita al **par. 8** del presente Manuale.

39. 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.

40. 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.

41. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dalla Società, 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, scambi di comunicazioni informali con legali esterni o con l'AdER 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;
- comunicazioni automatiche inviate alle caselle di posta PEC o ordinaria della Società, che attestano l'avvenuta ricezione/protocollazione ad opera del destinatario dalla corrispondenza inviata dalla Società.

Possono inoltre essere esclusi dalla registrazione di protocollo, qualora ciò comporti un oggettivo ostacolo alla efficiente ed efficace operatività degli Uffici:

- fatture attive e passive, comprese le bollette emesse verso gli utenti⁹;
- solleciti di pagamento massivi;
- proposte di piano di rientro (resta fermo che il piano di rientro definitivo sottoscritto e trasmesso dovrà essere protocollato);
- ordini di acquisto/conferme d'ordine di modico valore, comunque inferiore a 40k/€¹⁰;
- il libro unico del lavoro (cedolini+presenze), le pratiche Inps/Inail/comunicazioni obbligatorie (v. nota 6); contratti a sportello muniti di firma grafometrica dell'utente / con OTP / firma digitale del delegato ETRA;
- documenti relativi alla sicurezza sul lavoro, che transitano sulla piattaforma 626¹¹.

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.

⁹ La possibilità di esclusione opera solo se tali documenti sono già censiti e salvati su apposite piattaforme ufficiali.

¹⁰ Da inviarsi/riceversi comunque mezzo posta elettronica certificata;

¹¹ Piani di emergenza e evacuazione, attestati di formazione e certificazioni del personale, verbali e relazioni periodiche del medico competente.

42. Protocollo 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 della Società o qualsiasi altro documento dal quale possano nascere diritti, doveri, o legittime aspettative di terzi.¹²

43. Disposizioni per particolari tipologie di documenti

La protocollazione della documentazione di gara, delle offerte e degli ulteriori documenti/atti/certificati/comunicazioni afferenti alla gara (sia pre che post aggiudicazione)¹³, nonché delle richieste di preventivo, dei preventivi e dei contratti afferenti agli affidamenti diretti, purché scaricabili dalle piattaforme e-procurement dei mercati elettronici della Pubblica Amministrazione, della Regione o da altre piattaforme usate dalla Società, non è necessaria.

44. 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;

¹² Documenti interni, bozze e comunicazioni informali possono essere esclusi, mentre atti con rilevanza esterna o che necessitano di un valore probatorio devono essere protocollati. Un documento ha rilevanza esterna quando produce effetti nei confronti di soggetti terzi, come nel caso di comunicazioni ufficiali inviate ad altri enti, contratti, autorizzazioni o atti amministrativi, che incidono su diritti e obblighi di persone fisiche o giuridiche. La protocollazione in questi casi assicura una data certa alla formazione, ricezione o trasmissione del documento, consentendo di ricostruire il flusso documentale e di dimostrare, se necessario, l'effettivo invio o ricevimento di un atto. Un atto assume, invece, valore probatorio quando può essere utilizzato come prova in un eventuale procedimento giudiziario o amministrativo. La registrazione ufficiale serve in questo caso a certificare l'esistenza del documento in una determinata data, evitando contestazioni sulla sua autenticità, provenienza o integrità. Documenti come verbali di riunioni con decisioni vincolanti, denunce, segnalazioni o lettere di messa in mora rientrano in questa categoria, poiché potrebbero essere determinanti per dimostrare un fatto o un diritto.

¹³ Pre Aggiudicazione: documentazione di gara; offerte: richieste di soccorsi istruttori, documentazione probatoria dei requisiti speciali; Post aggiudicazione: documentazione probatoria dei requisiti di esecuzione e generali, documenti per la verifica sussistenza requisiti di idoneità tecnica; documenti ottenuti tramite banche dati di autorità terze; cauzioni provvisorie e definitive; tutti gli ulteriori documenti comunque connessi agli appalti e purché inviati/ricevuti per il tramite della piattaforma e-procurement.

- d) oggetto del documento, campo da valorizzare secondo la seguente chiave descrittiva: oggetto riportato sul documento da protocollare in ingresso e/o in uscita;
- 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 4**);
- 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.

45. 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.

Come precisato e ribadito dall'AgID (cfr. il [Vademecum](#) pubblicato a ottobre 2022), al fine di garantire l'interoperabilità tra AOO, la produzione di un documento segue il seguente **processamento**:

- I. Formazione del documento principale ed eventuali allegati (la formazione del documento principale e degli eventuali allegati si conclude con la firma elettronica degli stessi);
- II. Calcolo dell'impronta (*hash*) del documento principale e degli eventuali allegati;
- III. Generazione del numero di protocollo da assegnare al messaggio di protocollo;
- IV. Formazione della segnatura di protocollo (che deve rispettare l'XML Schema indicato nelle LLGG utilizzando le impronte del documento principale e degli eventuali allegati);
- V. Apposizione di un "sigillo elettronico qualificato" alla segnatura di protocollo per garantire l'integrità e autenticità.

La segnatura di protocollo non potrà essere apposta su un documento firmato digitalmente. Pertanto, per le comunicazioni in uscita, all'atto della relativa predisposizione sul Gestionale di Protocollazione, si dovrà: (i) inserire, come documento principale, una mera copia per immagine (i.e. PDF) della comunicazione firmata digitalmente, sulla quale sarà apposta la segnatura di protocollo, e; (ii) inserire tra gli allegati il documento firmato digitalmente.

46. 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 scaricare il file .EML contenente messaggio in entrata e a inoltrarlo in allegato all'indirizzo di posta ordinaria dell'Ufficio Protocollo, esplicitando nel testo la richiesta di protocollare. In tali casi, dunque, l'operatore addetto al protocollo provvede alla protocollazione del messaggio inoltrato in allegato (e non del messaggio di inoltro), assicurandosi che siano registrati i relativi dati.

Al fine di evitare doppie registrazioni dello stesso documento, prima dell'inoltro per la registrazione, l'operatore deve verificare che nella comunicazione è stato indicato anche il recapito PEC. In tali casi, infatti, non serve provvedere all'inoltro per la protocollazione.

Per le medesime finalità di cui al capo che precede, prima della protocollazione, gli operatori addetti al Protocollo Centrale ed a quello Diffuso dovranno verificare se nella comunicazione siano state indicate due o più delle caselle di posta di cui all'art. 29. In tal caso, dovrà essere protocollata:

- Per la medesima comunicazione diretta contemporaneamente a tutti gli indirizzi di posta del Protocollo Centrale (e cioè per la medesima comunicazione inviata contemporaneamente a protocollo@pec.etraspa.it;

- info@etraspa.it; disservizirifiuti@etraspa.it e protocollo1@pec.etraspa.it): solo la comunicazione ricevuta alla casella PEC protocollo@pec.etraspa.it;
- Per la medesima comunicazioni diretta contemporaneamente ai seguenti indirizzi di posta del Protocollo Centrale: protocollo@pec.etraspa.it; info@etraspa.it; disservizirifiuti@etraspa.it; solo la comunicazione ricevuta alla casella PEC protocollo@pec.etraspa.it;
 - Per la medesima comunicazione diretta contemporaneamente ai seguenti indirizzi di posta del Protocollo Centrale: info@etraspa.it; disservizirifiuti@etraspa.it e protocollo1@pec.etraspa.it; solo la comunicazione ricevuta dalla casella dalla casella PEC protocollo1@pec.etraspa.it;
 - Per la medesima comunicazione diretta contemporaneamente ai seguenti indirizzi di posta del Protocollo Centrale: protocollo@pec.etraspa.it; protocollo1@pec.etraspa.it; solo la comunicazione ricevuta alla casella PEC protocollo@pec.etraspa.it;
 - Per la medesima comunicazione diretta contemporaneamente ai seguenti indirizzi di posta del Protocollo Centrale: info@etraspa.it; disservizirifiuti@etraspa.it; solo la comunicazione ricevuta dalla casella dalla casella info@etraspa.it;
 - Per la medesima comunicazione diretta contemporaneamente ai seguenti indirizzi di posta del Protocollo Centrale: info@etraspa.it e protocollo1@pec.etraspa.it; solo la comunicazione ricevuta dalla casella PEC protocollo1@pec.etraspa.it;
 - Per la medesima comunicazione diretta a tutti o alcuni degli indirizzi di posta del Protocollo Centrale ed a tutti o alcuni gli indirizzi di posta del Protocollo Diffuso, solo la comunicazione ricevuta dalla casella PEC del Protocollo Diffuso competente per materia.

Qualora una comunicazione sia erroneamente inviata solo ad una casella pec del Protocollo Diffuso, anche se la comunicazione medesima non afferisce alle attività proprie dell'Area/Unità a cui quella casella pec di protocollo diffuso afferisce, il Protocollo Diffuso dovrà comunque protocollare quella comunicazione e poi smistarla il giorno stesso della ricezione al Protocollo Generale affinché quest'ultimo ne curi il corretto smistamento.

47. 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 di 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. Come per ogni atto pubblico, la formazione richiede solennità e, dunque, la massima accortezza e precisione.

Ogni annullamento della registrazione deve:

- essere autorizzato con provvedimento del RGD. Il provvedimento, dunque, deve risultare da comunicazione formale;
- comportare la memorizzazione di data, ora e estremi del provvedimento di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al RGD devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad es., registrazione di informazioni errate, doppia registrazione, erronea registrazione di documenti non destinati alla Società). Nell’inviare il documento già oggetto di precedente registrazione, poi annullata, nelle note di trasmissione si dovrà dichiarare che: *“Il presente documento sostituisce il documento prot. n. [...] di data [...]”*.

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.

48. 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.

Non è ammessa l’associazione al documento informatico già registrato di allegati non indicati nella registrazione di protocollo. L’associazione di allegati successivamente alla registrazione non può essere effettuata, dunque in tali casi è

necessario procedere ad annullamento ed a nuova registrazione, attraverso la procedura di cui al precedente paragrafo.

49. Informazioni agli utenti rese dal responsabile del procedimento

Ogni responsabile del procedimento deve curare la **corretta informazione degli utenti**, fornendo tutte le informazioni necessarie relative a:

- **dimensione massima** degli allegati;
- **formato** dei documenti informatici trasmessi in allegato;
- **modalità di trasmissione** ed i relativi canali predisposti per lo specifico procedimento.

Anche per gli allegati, così come per il documento principale soggetto a protocollazione, è vietata l'acquisizione o la trasmissione tramite strumenti personali per il trasferimento dei file diversi da quelli messi a disposizione dalla Società.

50. Tempi di registrazione e casi di differimento

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

Al fine di consentire il rispetto della predetta tempistica, ove la corrispondenza in entrata sia stata erroneamente smistata ad un Ufficio non competente, quest'ultimo dovrà – lo stesso giorno di ricezione - segnalare tale anomalia al Protocollo Centrale, indicando (ove noto) l'Ufficio competente, affinché l'Ufficio Protocollo possa procedere alla riassegnazione della corrispondenza.

In casi eccezionali ed imprevisti, o per eccessivi carichi di lavoro, 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 RGD 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 RGD 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 della Società, 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.

51. 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 nell'ambito delle fasi di processamento della registrazione di protocollo, come indicate al precedente **par. 45**.

I requisiti necessari di ciascuna segnatura di protocollo sono:

- a. indicazione del 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.

Il file XML di segnatura viene sottoscritto con il sigillo elettronico qualificato della Società, che garantisce integrità del file e alla certezza del mittente.

Per garantire l'interoperabilità dei documenti informatici trasmessi alle Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti in un file XML conforme alle indicazioni previste al p. 2 e ss. dell'Allegato 6 alle Linee guida dell'AgID e, in particolare, nel rispetto dello schema di cui all'Appendice A (v. p. 4.1. "Segnatura di protocollo XML Schema").

52. Protocollo riservato

La gestione del protocollo riservato può essere utilizzata per i documenti che richiedono una trattazione riservata in quanto dalla loro visibilità si ritiene possano derivare un pregiudizio a terzi o al buon andamento dell'attività societaria.

Ove implementata, la registrazione di un documento nel protocollo riservato è effettuata dal RGD o dal RPCT, in conformità all'autorizzazione generale conferita – da parte del Consiglio di Amministrazione - con l'atto approvativo del Manuale. L'accesso ai documenti così registrati è consentito unicamente ai soggetti formalmente autorizzati.

53. Registro di emergenza

L'utilizzo del registro di protocollo di emergenza è autorizzato dal RGD, 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 per 5 (cinque) giorni lavorativi. In tali casi, il RGD 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.

Al ripristino della piena funzionalità del Sistema di protocollo informatico, il RGD 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.

Per le ipotesi di sospensione del servizio dovute a guasti del Sistema di protocollo informatico, il RGD provvede alla formazione del registro di emergenza su supporto analogico, redatto secondo lo schema di cui all'**Allegato 6** al presente Manuale.

54. 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:

- determine del Presidente;
- determine del Direttore Generale;
- determine dei Procuratori e dei Responsabili Unici del Procedimento (RUP);
- contratti d'appalto;
- Registro di Repertorio di cui all'art. 67 TUR.

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, quando sono informatizzati, devono essere conservati con modalità analoghe a quelle del registro giornaliero di protocollo informatico.

Il RGD, 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.

Sezione terza - Disposizioni sulla protocollazione e gestione dei documenti analogici

55. Protocollazione dei 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 regola, allo scopo e prima di procedere alla registrazione di tale documentazione analogica, dovrà procedersi a fare di essa una copia per immagine su supporto informatico (scansione in formato pdf/A), sulla quale andrà apposta l'attestazione di conformità secondo quanto previsto al par. 15. Al termine di tale operazione, la documentazione analogica potrà essere distrutta, salva la necessità di riportare – su apposito registro – gli estremi del documento analogico distrutto.

La copia per immagine di documenti firmati, se sprovvista di attestazione di conformità, apposta ai sensi della normativa vigente (v. le procedure definite al **par. 14** del presente Manuale), può essere adoperata solo per uso lavoro.

Fermo quanto previsto al secondo capoverso del presente paragrafo, resta salva la possibilità residuale di procedere alla registrazione dei documenti analogici mediante la preventiva segnatura degli stessi, con timbro ed etichetta riportante i dati indicati al par. 44. In tale ipotesi, però, il documento analogico dovrà essere conservato e inserito nelle apposite cassette di smistamento agli uffici destinatari competenti.

56. 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 “MITTENTE ANONIMO”.

I documenti in cui vi è l'indicazione del mittente, ma manca la sottoscrizione, vengono protocollati e viene annotato nelle informazioni “DOCUMENTO NON SOTTOSCRITTO”.

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 o stringa di protocollazione) deve essere barrata con la dicitura “*annullato*”.

57. Rilascio della ricevuta di avvenuta protocollazione

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.

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: UO 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.

58. Corrispondenza contenente dati particolari

Le comunicazioni in entrata e i documenti ad esse acclusi contenenti categorie particolari di dati e/o dati giudiziari, ai sensi del GDPR, riferiti al mittente e/o a suoi familiari/conviventi/terzi (di seguito, la **Corrispondenza Sensibile**), inviati ad ETRA, qualora siano qualificati dall'Ufficio competente come essenziali per la corretta gestione ed evasione della pratica a cui essi si riferiscono, dovranno essere regolarmente protocollati e smistati/assegnati all'Ufficio competente. Diversamente, PROT e il Protocollo Diffuso non dovranno procedere alla loro protocollazione/smistamento/assegnazione, dovendo viceversa procedere alla loro distruzione/cancellazione immediata, dandone comunicazione al mittente.

In particolare:

- (i) Non dovranno essere protocollate/smistate le comunicazioni con cui il mittente trasmette, in allegato, Certificati ISEE. Tali comunicazioni, con annessa documentazione allegata, dovrà essere cancellata/distrutta, posto che per la gestione delle pratiche connesse (accesso alla riduzione

tariffaria ai sensi del Regolamento Unificato di Gestione dei Rifiuti) è sufficiente la trasmissione della sola Modulistica *standard* predisposta da ETRA e compilata/firmata dal mittente interessato, unitamente al relativo documento di riconoscimento;

- (ii) Dovranno essere protocollate/smistate agli Uffici competenti le comunicazioni contenenti, nel testo, categorie di dati particolari e/o giudiziari, o a cui siano acclusi atti/provvedimenti giudiziari (i.e. sentenze di divorzio) e/o atti di nomina di amministratori di sostegno e/o tutori legali, posto che per la gestione delle pratiche connesse (vulture, nuove attivazioni, esclusioni) è necessaria la loro acquisizione, esame ed archiviazione.

Qualora alle Comunicazioni Sensibili siano acclusi documenti diversi da quelli sopra elencati (e cioè diversi da ISEE, Atti/Sentenze di divorzio; Atti di Nomina di Amministratori di Sostegno e/o Tutori Legali) che contengono categorie di dati particolari e/o giudiziari, PROT e il Protocollo Diffuso procederanno comunque alla loro protocollazione e smistamento/assegnazione all'Ufficio Competente, indicando nel campo 'Note' della pratica di protocollo la dicitura "Contiene dati particolari/giudiziari ai sensi del GDPR", affinché l'Ufficio Competente possa valutare se l'acquisizione di tali documenti sia o meno essenziale per la gestione/evasione della connessa pratica e, in caso negativo, possano procedere alla immediata cancellazione/distruzione degli stessi, dando indicazioni scritte in tal senso anche a PROT e al Protocollo Diffuso di procedere all'annullamento della pratica di protocollazione.

Fermo quanto sopra, nel rispetto di quanto previsto dal GDPR, ETRA dovrà: (1) fornire adeguata Informativa ex art. 13 del GDPR medesimo al fine di rendere edotti gli interessati del fatto che la Società tratterà anche categorie particolari di dati e/o dati giudiziari; (2) autorizzare formalmente il personale preposto al trattamento dei dati de quo; (3) conservare tali dati per il tempo strettamente necessario al raggiungimento delle finalità per cui gli stessi sono stati acquisiti/trattati.

59. Corrispondenza personale o riservata

La corrispondenza nominativamente intestata e/o quella diretta ai titolari di cariche istituzionali deve essere consegnata ai destinatari priva di registrazione ed eventualmente protocollata solo successivamente, su disposizione del destinatario, ove afferente ad affari aziendali.

60. Corrispondenza cartacea non di competenza della Società

Qualora pervenga, tramite posta tradizionale, un documento cartaceo che non è evidentemente indirizzato alla Società (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 predetta fattispecie sia erroneamente registrato al protocollo, questi è spedito a chi di competenza, oppure restituito al mittente, con una lettera di trasmissione protocollata.

Sezione quarta – Classificazione e fascicolazione

61. Classificazione dei documenti amministrativi

I documenti amministrativi formati e acquisiti dalla Società sono classificati mediante indicazione del titolo e della classe secondo i criteri previsti nel Piano di classificazione (Titolario) di cui all'**Allegato 4**.

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 dalla Società è effettuata dal responsabile dell'UO o dal personale da questo delegato.

62. Fascicolazione informatica dei documenti amministrativi

Al fine di garantire la consultazione dei documenti amministrativi informatici, questi sono raccolti in fascicoli informatici, secondo il Piano di fascicolazione di cui all'**Allegato 5**.

I documenti soggetti a protocollazione sono inseriti nel pertinente fascicolo tramite le apposite funzioni del Sistema di gestione documentale. Quando è necessario aprire un nuovo fascicolo informatico, l'utente abilitato alla creazione dei fascicoli della UO che ha prodotto il documento provvede all'apertura del fascicolo in cui inserire il documento.

Per i documenti in entrata, quando occorre provvedere all'apertura di un nuovo fascicolo informatico, il personale addetto alla protocollazione si limita ad assegnare i documenti alla UO competente che provvederà alla fascicolazione.

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. A tal fine, il RGD verifica che il software del sistema di gestione documentale che consente la creazione dei fascicoli informatici sia adeguato alla normativa tecnica vigente e, all'occorrenza, ne richiede l'adeguamento. Si ricorda che, a prescindere dalla tipologia, il fascicolo in ogni caso deve recare almeno i seguenti metadati:

- metadati identificativi del tipo di aggregazione (campo "TipoAggregazione" = Fascicolo; campo "IdAggregazione" = codice identificativo);
- tipologia di fascicolo (ad es. procedimento amministrativo, affare, persona fisica, ecc.);
- codice IPA Amministrazione titolare (campo "Ruolo");
- codice IPA Amministrazioni partecipanti (campo "Ruolo");
- dati identificativi del RUP (nome, cognome, codice IPA dell'Amministrazione di appartenenza, domicilio digitale).

Sezione quinta – Flussi documentali interni

63. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate.

Ulteriori criteri di assegnazione automatica sono definiti dal RGD, sentite le UO interessate.

I documenti non assegnati automaticamente sono assegnati dal personale addetto alla protocollazione, in base all'oggetto del documento e alla classificazione, alle UO responsabili "per competenza".

Quando un documento è di interesse anche per più UO, si provvede a più assegnazioni, sia “per competenza” che “per conoscenza”.

I documenti interni devono essere assegnati e consultati attraverso il Sistema di gestione documentale e la componente Sistema di protocollo informatico.

64. 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 le diverse UO della Società è effettuato principalmente per mezzo di posta elettronica ordinaria, cartelle condivise online o in intranet o del sistema di *workflow* del Sistema di gestione documentale.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando una comunicazione è indirizzata a più destinatari e, 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).

In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dalla Società. Non è consentito l'utilizzo di servizi di messaggistica istantanea (es. Whatsapp, Telegram, ecc.) per lo scambio di documenti nell'ambito dell'attività lavorativa.

65. Pubblicazioni nell'Albo pretorio e in Società Trasparente

Tutti gli atti prodotti dalla Società che, ai sensi della normativa vigente, sono soggetti a pubblicazione, sono trasmessi per la pubblicazione solo dopo che il documento sia divenuto imm modificabile (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.

Tutti gli atti prodotti da ETRA che, ai sensi della normativa vigente, sono soggetti a pubblicazione nella sezione Società Trasparente del sito istituzionale, sono trasmessi per la pubblicazione dagli utenti abilitati solo dopo che il documento sia divenuto imm modificabile, salvo quelli che per disposizioni normativa e/o regolamentare debbano esser pubblicati in formato editabile (come a titolo esemplificativo e non esaustivo, la relazione annuale del RPCT che, per disposizione dell'ANAC, deve esser pubblicata in formato .xsl).

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

66. Sistema di conservazione dei documenti informatici

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

Il servizio di conservazione dei documenti informatici della Società è stato affidato a un conservatore accreditato dall'AgID (d'ora in avanti anche solo "Conservatore").

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 Conservatore di cui all'**Allegato 7** al presente Manuale, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione.

67. Responsabile della conservazione

Il RCD è stato individuato da ETRA con il provvedimento di cui all'**Allegato 1** al presente Manuale.

Il RCD svolge tutti i compiti previsti dal richiamato par. 4.5 delle Linee guida che non siano stati espressamente affidati al Conservatore. In particolare, il RCD:

- a) assicura, la produzione e la trasmissione dei pacchetti di versamento al sistema di conservazione;
- b) esegue il monitoraggio in merito al corretto funzionamento del sistema di conservazione dei documenti informatici, provvedendo altresì a segnalare tempestivamente al conservatore gli eventuali guasti e le proposte di miglioramento del sistema medesimo;
- c) provvede, sotto il profilo organizzativo e gestionale, ad assicurare l'interfacciamento e il collegamento del proprio sistema con il sistema di conservazione digitale dei documenti informatici gestito dal Conservatore;
- d) comunica al Conservatore i nominativi e le funzioni del personale abilitato all'accesso al sistema di conservazione, per verificare il corretto svolgimento dell'attività di conservazione e per consultare ed eventualmente estrarre i documenti depositati e le prove di conservazione, secondo le modalità previste nella documentazione tecnica relativa all'affidamento del servizio.

Resta fermo che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al RCD, chiamato altresì a svolgere le necessarie attività di verifica e controllo sulla corretta esecuzione del servizio di conservazione da parte del Conservatore.

Il RCD provvede altresì, al costante aggiornamento delle disposizioni di cui alla presente Parte del Manuale.

68. Oggetti della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati e acquisiti dalla Società e i rispettivi metadati, conformi all'allegato 5 alle Linee guida dell'AgID;
- i fascicoli informatici della Società e rispettivi metadati, conformi all'allegato 5 alle Linee guida dell'AgID;
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dalla Società.

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 RCD o i suoi delegati provvedono 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 di documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel manuale utente del Sistema di gestione documentale e nel Manuale del Conservatore.

69. Tempi di conservazione

È compito del RCD e del DPO nominato dalla Società provvedere alla definizione del Piano di conservazione della Società medesima, in cui siano individuati tutti i documenti informatici che devono essere conservati e i relativi tempi di conservazione, in conformità con quanto previsto nel Registro del Trattamento.

70. Formati ammessi per la conservazione

I formati ammessi per la conservazione sono individuati nell'**allegato 2 alle Linee guida dell'AgID**. Prima di individuare un formato tra quelli versati in conservazione occorre dunque verificare che sia tra quelli ivi menzionati e che non vi siano raccomandazioni contrarie all'utilizzo per la conservazione da parte del conservatore.

Il RCD, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal RCD attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Terza del presente Manuale.

71. Modalità e tempi di trasmissione dei pacchetti di versamento

Entro il 31 gennaio di ogni anno ciascuna UO individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al RCD, 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 RCD 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 RCD della conservazione 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 della Società, anche a fascicolo aperto, riferiti all'anno precedente;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il RCD 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).

72. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica (archivio corrente)

La memorizzazione dei documenti correnti (in transito sul gestionale) è effettuata in *cloud*, nel *repository* del Sistema di gestione documentale, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore o della selezione per lo scarto.

73. Accesso al Sistema di conservazione

Gli utenti espressamente autorizzati dal RCD 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 e le configurazioni specifiche adottate.

74. Selezione e scarto dei documenti

Periodicamente, a cadenza almeno annuale, viene effettuata la procedura di selezione della documentazione da proporre allo scarto, in conformità alle tempistiche di conservazione definite al **par. 69** del presente Manuale, ed attivato il procedimento amministrativo di scarto documentale.

In particolare, l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione del Conservatore e trasmesso al RCD della Società, il quale verifica il rispetto dei termini temporali stabiliti dal Piano di conservazione.

Le modalità operative per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Manuale del Conservatore (v. **Allegato 7**). L'operazione di scarto viene tracciata sul sistema mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

75. Conservazione, selezione e scarto dei documenti analogici

La documentazione analogica corrente è conservata a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

I documenti analogici della Società sono conservati nei locali della Società. Il responsabile della UO competente cura il versamento nell'archivio di deposito delle unità archivistiche non più utili per la trattazione degli affari in corso, individuate dagli uffici produttori. I fascicoli non soggetti a operazioni di scarto sono conservati nell'archivio di deposito secondo i termini di legge, per poi essere trasferiti nell'archivio storico per la conservazione permanente. Delle operazioni di trasferimento deve essere lasciata traccia documentale.

Periodicamente il RCD valuta l'opportunità, anche sotto il profilo economico, di provvedere al riversamento in formato digitale di tutti o parte dei documenti analogici presenti negli archivi.

76. Misure di sicurezza e monitoraggio del sistema di conservazione

Il Manuale di conservazione e il piano della sicurezza del Conservatore descrivono 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*.

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

Il RCD 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 previsti nell'atto di affidamento del servizio.

PARTE SESTA – SICUREZZA E PROTEZIONE DEI DATI PERSONALI

77. Sicurezza dei sistemi informatici della Società ETRA S.p.A. Società Benefit

Gli strumenti software del Sistema informatico di gestione documentale, utilizzati per la formazione e gestione dei documenti informatici, sono resi accessibili al personale della Società tramite servizi che consentono l'archiviazione dei documenti, prodotti mediante l'utilizzo dell'applicativo, 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 della Società, in attesa dell'archiviazione tramite versamento al sistema di conservazione del Conservatore, o della selezione per lo scarto.

78. Amministratore di sistema

Il ruolo di Amministratore del Sistema di gestione documentale della Società è svolto dal responsabile della UO ICT, che a tal fine può delegare altro dipendente aziendale. Il personale delegato svolge i compiti operativi relativi alla gestione delle abilitazioni di accesso di cui al **par. 9** (quali il rilascio, la revoca, l'attribuzione di particolari privilegi, ecc.), previa autorizzazione del RGD, in base alle richieste dei responsabili di servizio.

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

La gestione tecnica degli utenti abilitati ad accedere al protocollo informatico, in base alla pianta organica della Società e sulla base delle indicazioni dei responsabili competenti e del RGD, è affidata al responsabile della UO ICT o suo delegato.

In particolare, per l'accesso ai sistemi informatici della Società è necessaria l'assegnazione di un profilo utente formalmente autorizzata dal RGD.

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. Le richieste concernenti il recupero delle credenziali devono essere effettuate per iscritto al RGD, che le accetta con formale comunicazione.

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.).

Il Sistema è configurato in modo che a cadenza periodica (almeno trimestrale), per ogni profilo utente sia richiesto il rinnovo della password.

80. Accesso alle postazioni di lavoro, ai locali e agli archivi della Società

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.).

Gli archivi storici della Società sono collocati nelle seguenti sedi societarie di: Cittadella (PD), Via del Telarolo n. 9; Camposampiero (PD), Via Edison n. 8; Vigonza (PD), Via Grandi n. 52; Bassano del Grappa (VI), Largo Parolini n. 82/b; Asiago (VI), Via Fratelli Rigoni Guido e Vasco n. 19; Bassano del Grappa (VI), C. Colombo n. 96; Cittadella (PD), Via Niccolò Copernico n. 2; Rubano (PD), Via Luigi Galvani n. 1/A; Sommacampagna (VR), Via della Tecnica n. 22;

in locali opportunamente chiusi al pubblico, le cui chiavi di accesso sono custodite dal personale addetto. La consultazione avviene esclusivamente in presenza del personale.

Per quanto riguarda l'accesso ai locali che ospitano i data center aziendali, si rinvia alle previsioni del Piano di sicurezza.

PARTE SETTIMA – DISPOSIZIONI FINALI

81. Entrata in Vigore ed Efficacia

Il presente Manuale entrerà in vigore e diverrà efficace dall'1.07.2025 e dovrà essere pubblicato sul sito istituzionale di ETRA S.p.A. Società *Benefit*, nella sezione Società Trasparente.

Fermo quanto sopra, gli articoli 7, 9, 37, 38 e 79, nonché gli articoli 36, 40, 45, 48, 53, 54, 57, 62, 63 e 77, limitatamente alle disposizioni che presuppongono l'implementazione del Gestionale Integrato di protocollazione e gestione documentale, diverranno efficaci a decorrere dalla data che sarà individuata con apposito provvedimento, successiva all'effettiva messa in esercizio del suddetto Gestionale, entro il **30/06/2027**.

Il Manuale dovrà essere messo a disposizione del personale interno, anche tramite intranet o gestionale documentale.

3	29/06/2026	Revisione della procedura di gestione di comunicazioni e documenti che possono contenere anche dati particolari di cui all'art. 58	ASL Firmato digitalmente da: FRANCESCA PRISCO Data: 29/06/2026 09:43:16	DG Firmato digitalmente da: Domenico Lenzi Data: 06/07/2026 15:53:53 Domenico Lenzi
Rev.	Data	Descrizione modifiche	Redazione	Approvazione