DSU TOSCANA

Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio e all'accesso ai documenti informatici

Revisione 11.0 del 29/04/2023

AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

sede legale
Viale A. Gramsci, 36 – 50132 Firenze
www.dsu.toscana.it
info@dsu.toscana.it
C.F. 94164020482 – P.I. 05913670484

DSU TOSCANA

Sommario

Allegati

DSU TOSCANA

Elenco delle ultime revisioni

Revisione	Principali modifiche	Autore della revisione
Rev. 05 del 3 dicembre 2012	Rielaborazione completa da parte del nuovo responsabile del protocollo informatico a seguito di confronto con il Settore "Servizi generali e semplificazione dei processi" della Regione Toscana	Marco Aleksy Commisso
Rev. 06 del 7 aprile 2014	Aggiornamento dei riferimenti normativi Aggiornamento della documentazione di natura contabile esclusa dalla protocollazione Specificazione delle modalità di registrazione, per la documentazione soggetta a registrazione particolare Aggiornamento allegati	Marco Aleksy Commisso
Rev. 07 del 12 ottobre 2015	Adeguamento alle Regole Tecniche del protocollo informatico di cui al D.P.C.M. 3 dicembre 2013 Revisione aspetti operativi del ciclo di lavorazione dei documenti analogici ed Informatici Revisione allegati al documento	Marco Aleksy Commisso
Rev. 08 del 31 dicembre 2020	Rielaborazione completa a seguito dell'approvazione delle nuove Linee Guida AGID Revisione aspetti operativi del ciclo di lavorazione dei documenti analogici ed Informatici Revisione allegati al documento	Marco Aleksy Commisso
Rev. 09 del 30 marzo 2021	Aggiunta allegato "Massimario di selezione e scarto rev. 01" a seguito di approvazione della Soprintendenza Archivistica della Regione Toscana Precisazione ruolo UOP/Gestione Atti in visibilità documenti	Marco Aleksy Commisso
Rev. 10 del 27 maggio 2022	Aggiornamento organigramma a seguito approvazione nuova macrostruttura organizzativa aziendale Integrazione repertori Altre integrazioni/correzioni minori	Marco Aleksy Commisso
Rev. 11 del 29 aprile 2023	Aggiornamento fonti normative Inserito indirizzi PEC non adibiti alla ricezione di documentazione soggetta a protocollazione	Marco Aleksy Commisso

Revisione	Principali modifiche	Autore della revisione
	Aggiornamento figure coinvolte nella gestione operativa e nella sicurezza dei flussi documentali Aggiornamento Piano per la sicurezza informatica e la tutela dei dati personali Aggiornamento modalità di ricezione dei documenti informatici Aggiornamento casistiche particolari nella gestione della ricezione e protocollazione dei documenti Aggiornamento criteri di visibilità dei documenti Recepimento “Raccomandazioni di Aurora” per la qualità delle informazioni memorizzate	

DSU TOSCANA

CAPITOLO 1 - PRINCIPI GENERALI

1.1 Contesto normativo

Il 1° gennaio 2022 sono entrate in vigore le "*Linee Guida sulla formazione, gestione e conservazione dei documenti informatici*" (di seguito, "Linee Guida") emanate dall'Agenzia per l'Italia Digitale (di seguito: AGID). (Termine così prorogato con Determinazione AGID n. 371/2021).

Di conseguenza:

a) le disposizioni contenute nel Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante "*Regole tecniche per il protocollo informatico*", sono abrogate ad eccezione delle seguenti:
   - art. 2 comma 1: Oggetto e ambito di applicazione;
   - art. 6: Funzionalità;
   - art. 9: Formato della segnatura di protocollo;
   - art. 18 commi 1 e 5: Modalità di registrazione dei documenti informatici;
   - art. 20: Segnatura di protocollo dei documenti trasmessi;
   - art. 21: Informazioni da includere nella segnatura

b) la circolare n. 60 del 23 gennaio 2013 dell'AGID in materia di "*Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni*" è abrogata e sostituita dall'allegato 6 delle Linee Guida denominato "*Comunicazione tra AOO di documenti amministrativi protocollati*".

Ulteriori norme di riferimento (in ordine cronologico)

- Legge 7 agosto 1990, n. 241: Nuove norme sul procedimento amministrativo;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 (come modificato dal Decreto Legislativo 10 agosto 2018, n. 101): Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Legge 9 gennaio 2004, n. 4: Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;
- Decreto Legislativo 22 gennaio 2004, n. 42: Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- Decreto del Presidente della Repubblica 1 marzo 2005, n. 75: Regolamento di attuazione della legge 9 gennaio 2004, n. 4, per favorire l'accesso dei soggetti disabili agli strumenti informatici;
- Decreto Legislativo 7 marzo 2005 n. 82: Codice dell'amministrazione digitale;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013: Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi

degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;

- Decreto Legislativo 14 marzo 2013, n. 33: Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013: Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Circolare n. 62 del 30 aprile 2013 AGID: Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD;
- Regolamento UE 2014/910 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
- Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Circolare 18 aprile 2017, n. 2/2017 AGID recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Circolare 9 aprile 2018, n. 2/2018 AGID recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- Circolare 9 aprile 2018, n. 3/2018 AGID recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- Regolamento UE 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
- Linee guida AGID del 27 febbraio 2019 relative all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi;
- Linee guida AGID del 20 giugno 2019 contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate;
- Linee guida AGID del 23 aprile 2020 contenenti le Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD;
- Linee guida AGID del 7 luglio 2022 relative all'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese;
- Linee guida AGID del 21 dicembre sull'accessibilità degli strumenti informatici.

1.2 Definizioni e acronimi

Si riportano di seguito le definizioni e gli acronimi principali, utilizzati nel presente Manuale:

1.2.1 Definizioni

TERMINE	DEFINIZIONE
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività. Un archivio informatico è costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'Ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del TUDA. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato
Documento analogico	Ogni rappresentazione, non informatica del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

TERMINE	DEFINIZIONE
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
Formato (del documento informatico)	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Gestione documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture

TERMINE	DEFINIZIONE
Metadati	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del TUDA
Piano della sicurezza informatica	Documento informatico che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) 2014/910 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
Repertorio dei fascicoli	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del TUDA
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)

TERMINE	DEFINIZIONE
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del TUDA
Servizi aziendali	Gli uffici dell'AOO che utilizzano i servizi messi a disposizione dal sistema di protocollo informatico
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

1.2.2 Acronimi

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea. L'AOO dell'Azienda è denominata: AOODSUTOSCANA
CAD	Il Decreto Legislativo 7 marzo 2005 n. 82 recante "*Codice dell'amministrazione digitale*"
IPA	Indice delle Pubbliche Amministrazioni
RCD	Il Responsabile della conservazione digitale
RGD	Il Responsabile della gestione documentale
SPID	Sistema Pubblico di Identità Digitale

ACRONIMO	DEFINIZIONE
TUDA	Il Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 recante "*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*"
UOP	Unità Organizzativa di Protocollo

1.3 Obiettivi del manuale di gestione

Il Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale di cui all'art. 17 del CAD e acquisito il parere del Responsabile della protezione dei dati personali ha il compito di predisporre il "*Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici*" (di seguito "Manuale") nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

Come previsto dalle Linee Guida, il presente documento prevede quale parte integrante dello stesso, il "Piano per la sicurezza informatica (e la tutela dei dati personali)" (allegato A al presente Manuale).

Il Manuale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Esso contiene le informazioni obbligatorie previste dal paragrafo 3.5 delle Linee Guida.

1.4 Eliminazione dei protocolli diversi da quello generale

In coerenza con quanto previsto e disciplinato dal presente Manuale, tutti i documenti inviati e ricevuti dall'Azienda devono essere registrati all'interno del registro ufficiale di protocollo informatico (ad eccezione di quelli per i quali non è prevista la protocollazione o che sono soggetti a registrazione particolare, secondo quanto specificato, rispettivamente, nei paragrafi 5.5 e 5.6).

Pertanto, tutti gli eventuali registri di protocollo, interni all'Azienda, diversi dal registro ufficiale di protocollo informatico sono soppressi.

1.5 Repertori

Nell'ambito della gestione dei flussi documentali sono attivi i seguenti repertori:

- Delibere del Consiglio di Amministrazione
- Determinazioni Dirigenziali
- Lettere d'ordine/contratto
- Provvedimenti del Direttore
- Relate di notifica
- Repertorio Albo Pretorio
- Verbali degli accertamenti delle dichiarazioni sostitutive degli studenti

- Verbali del Collegio dei Revisori
- Verbali del Consiglio di Amministrazione
- Verbali della Conservazione Digitale

1.6 Informazioni sull'Amministrazione

L'Azienda ha individuato un'unica AOO denominata **AOODSUTOSCANA** (**A2D6EE0** nell'Indice delle Pubbliche Amministrazioni - di seguito "IPA"). *(figura 1).*

All'interno della AOO il sistema di protocollazione dei documenti in entrata, uscita ed interni avviene in un unico registro con un'unica sequenza numerica di protocollazione per tutte le UOP e rinnovata automaticamente ad ogni anno solare.

L'Azienda, nell'ambito degli adempimenti previsti, si è accreditata all'IPA, tenuto e reso pubblico dal medesimo fornendo le informazioni che individuano l'amministrazione e l'articolazione della sua AOO. Il codice IPA dell'Azienda è: **ardsu_to**.

L'IPA è accessibile tramite il relativo sito internet da parte di tutti i soggetti, pubblici o privati. L'Azienda comunica tempestivamente all'IPA ogni successiva modifica dei propri dati aziendali e della propria organizzazione ed effettua comunque, ogni mese, la verifica della correttezza dei dati inseriti a cura del referente IPA dell'Azienda attualmente coincidente con il RGD.

1.7 Caselle PEC e PEO

L' AOO dispone:

- di una casella di posta elettronica certificata istituzionale **dsutoscana@postacert.toscana.it** per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'IPA. Tale casella costituisce il domicilio digitale della AOO e di tutti i Servizi / Aree che ad essa fanno riferimento. La casella non è abilitata alla ricezione di messaggi provenienti da indirizzi non certificati. La casella è configurata nel PEC manager del software dei flussi documentali;
- di una casella di posta elettronica certificata **dsuprotocollo@postacert.toscana.it** alimentata dall'applicativo di gestione dei benefici agli studenti con le istanze presentate sul Portale dei servizi on line (soggette anch'esse a protocollazione). La casella è configurata nel PEC manager del software dei flussi documentali;
- di una casella di posta elettronica di tipo tradizionale **protocollo@dsu.toscana.it** adibita alla ricezione e all'invio di documenti per i quali è prevista la protocollazione; La casella è configurata nel PEO manager del software dei flussi documentali;
- di altre caselle di posta elettronica certificata in uso ad alcuni Servizi aziendali non adibite alla ricezione o alla trasmissione di documentazione per cui è prevista la protocollazione. Nel dettaglio:

Indirizzo PEC	Servizio gestore	Finalità
pec.dsucontratti@postacert.toscana.it	Servizio Approvvigionamenti e Contratti	Comunicazioni con fornitori
dsu.fatturazione@postacert.toscana.it	Servizio Gestione Risorse Economico-Finanziarie	Ricezione fatture dal Sistema di Interscambio (backup)
pec.dsuaccertamenti.fi@postacert.toscana.it	Servizio Gestione Interventi FSE e Accertamenti	Comunicazioni con soggetti esterni per accertamenti sulle autocertificazioni presentate dagli studenti per ottenere benefici
pec.dsuaccertamenti.pi@postacert.toscana.it	Servizio Gestione Interventi FSE e Accertamenti	Comunicazioni con soggetti esterni per accertamenti sulle autocertificazioni presentate dagli studenti per ottenere benefici
pec.dsuaccertamenti.si@postacert.toscana.it	Servizio Gestione Interventi FSE e Accertamenti	Comunicazioni con soggetti esterni per accertamenti sulle autocertificazioni presentate dagli studenti per ottenere benefici
stranieri.dsu@postacert.toscana.it	Servizio Benefici e Interventi Monetari	Ricezione copia documentazione da parte di studenti stranieri per l'ottenimento di benefici
dsu.voucher@postacert.toscana.it	Servizio Benefici e Interventi Monetari	Corrispondenza relativa all'erogazione di voucher nell'ambito del Progetto POR-FSE
dsu.tirocini@postacert.toscana.it	Servizio Gestione Interventi FSE e Accertamenti	Corrispondenza relativa ai tirocini extra-curriculari

1.8 Descrizione dell'AOODSUTOSCANA

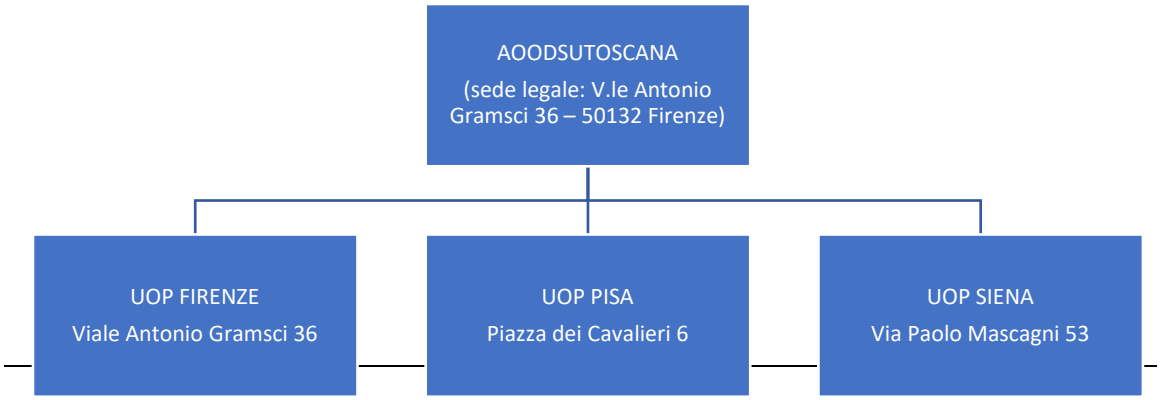


Figura 1 – Unità Operative di Protocollo dell'Articolazione Organizzativa Omogenea AOODSUTOSCANA

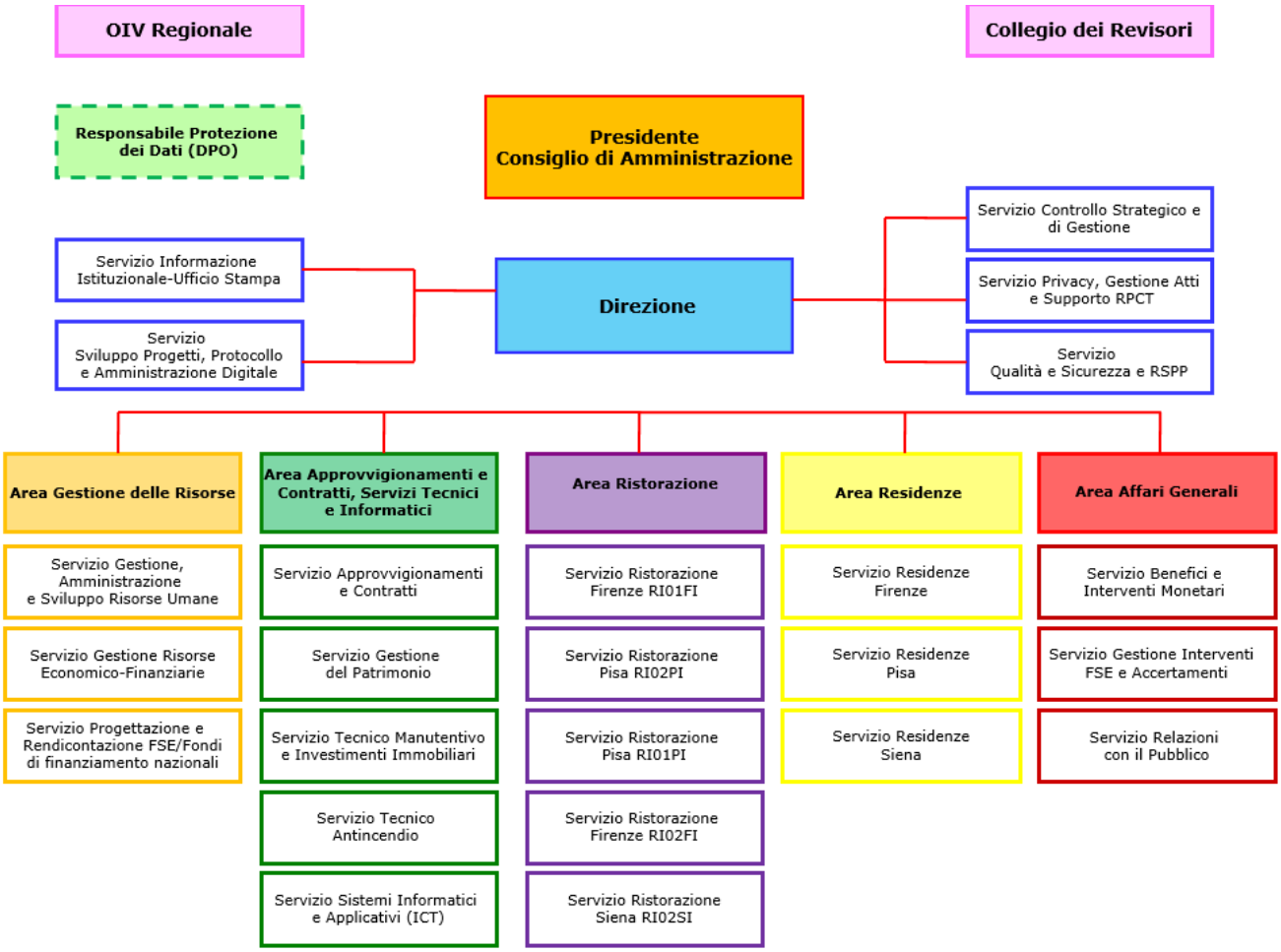


Figura 2 - Organigramma aziendale in vigore al 29/04/2023

Con Deliberazione del Consiglio di Amministrazione n. 8/23 del 21 febbraio 2023 è stata modificata la macrostruttura organizzativa dell'Azienda, dando mandato alla Direzione aziendale, con il supporto della Dirigenza aziendale anche in seno al Comitato di Direzione, di provvedere agli atti necessari e conseguenti che derivino dall'adozione della deliberazione citata.

La nuova macrostruttura, a regime, prevederà le seguenti Aree Dirigenziali:

- Area Residenze e Ristorazione
- Area Interventi Monetari e Relazioni con il Pubblico
- Area Gestione del patrimonio, dei Servizi Tecnici e Informatici
- Area Gestione delle Risorse
- Area Affari legali
- Area di Direzione

CAPITOLO 2 – ORGANIZZAZIONE DELL'AREA ORGANIZZATIVA OMOGENEA

2.1 Figure coinvolte nella gestione operativa e nella sicurezza dei flussi documentali

- Responsabile della gestione documentale (RGD) e un suo vicario, in caso di sua vacanza, assenza e impedimento;
- Responsabile della conservazione digitale (RCD);
- Responsabile per la protezione dei dati personali;
- Responsabile per la transizione al digitale;
- Responsabile dei sistemi Informativi
- Amministratore di sistema
- Addetti delle unità operative di protocollo (di seguito UOP);
- Utenti interni appartenenti ai Servizi aziendali (figura 2) abilitati all'utilizzo del sistema di gestione informatica dei documenti;

In sintesi:

Figura	Nominativo	Atto di nomina
Responsabile della gestione documentale (RGD)	Dott. Marco Aleksy Commisso	Provvedimento del Direttore n. 388/15 del 12/10/2015
Vicario Responsabile della gestione documentale	Dott. Mirko Carli	Provvedimento del Direttore n. 67/22 del 31/05/2022
Responsabile della conservazione digitale (RCD)	Dott. Marco Aleksy Commisso	Provvedimento del Direttore n. 406/15 del 26/10/2015
Responsabile per la protezione dei dati personali	Findata S.r.l.	Deliberazione del Consiglio di Amministrazione n. 49/22 del 29/09/2022
Responsabile per la transizione al digitale	Dott. Enrico Carpitelli	Deliberazione del Consiglio di Amministrazione n. 18/22 del 27/04/2022
Responsabile dei sistemi Informativi	Dott.ssa Sonia Chiantini	Provvedimento del Direttore n. 41/22 del 11/04/2022
Amministratore di sistema	Ing. Andrea Franci	Deliberazione del Consiglio di Amministrazione n. 5/23 del 21/02/2023

2.1.1 Responsabile della gestione documentale (RGD)

Al Servizio per la tenuta del protocollo informatico, della gestione documentale e degli archivi dell'Azienda, istituito presso l'AOO, è preposto il RGD che per l'Azienda coincide con il Responsabile del Servizio Sviluppo Progetti, Protocollo e Amministrazione Digitale.

Il vicario coincide con il Responsabile del Servizio Privacy, Gestione Atti e Supporto RPCT.

Per l'RGD e per il suo vicario è prevista una formazione obbligatoria e continua, a seguito di aggiornamenti normativi e di evoluzione tecnologica, ai sensi dell'art. 61 comma 2 del TUDA.

Non è prevista la figura del Coordinatore della Gestione documentale in quanto l'Azienda è dotata di un'unica AOO.

Il RGD, ai sensi del paragrafo 3.4 delle Linee Guida:

- d'intesa con il RCD, il Responsabile per la transizione digitale di cui all'art. 17 del CAD e acquisito il parere del responsabile della protezione dei dati personali predispone il "*Manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici*" nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;
- predispone con il supporto del Responsabile dei Sistemi Informativi il piano per la sicurezza informatica;
- verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Inoltre, l'Azienda, attribuisce al RGD e al suo vicario i seguenti compiti:

- assegna, sospende e disabilita le credenziali di accesso al sistema di gestione informatica dei documenti sia per gli utenti interni all'AOO che per eventuali utenti esterni;
- attribuisce il livello di autorizzazione per l'accesso al sistema di gestione informatica dei documenti distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del TUDA;
- definisce e assicura criteri uniformi di trattamento del documento informatico e, in particolare, di classificazione ed archiviazione;
- garantisce la corretta produzione e la conservazione del registro di protocollo giornaliero e annuale;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo e di gestione dei documenti e dei flussi documentali incluse le funzionalità di accesso di cui agli artt. 59 e 60 del TUDA e le attività di gestione degli archivi di cui agli artt. 67, 68 e 69 del TUDA;
- autorizza le operazioni di annullamento delle registrazioni di protocollo;
- verifica che le funzionalità del sistema in caso di guasti e anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e comunque nel più breve tempo possibile; in caso di permanenza del blocco delle attività è informato il Direttore circa la criticità della situazione autorizzando, se del caso, il prosieguo dell'utilizzo del registro di emergenza fino al ripristino dell'operatività;
- garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
- verifica che le copie di salvataggio delle informazioni del sistema di protocollo, del registro di emergenza nonché le copie di cui agli articoli 62 e 63 del TUDA siano conservate in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;

- autorizza l'apertura e chiusura del registro di emergenza;
- dispone periodicamente controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale e sull'utilizzo di un unico registro informatico, verificando anche, attraverso ispezioni mirate, la classificazione e la fascicolazione archivistica;
- vigila sull'osservanza delle disposizioni del TUDA da parte degli addetti delle UOP;
- su richiesta del Direttore o di un Dirigente di Area, può abilitare determinati utenti alla protocollazione di documenti informatici sul registro di protocollo generale – o su altri repertori - in aggiunta agli operatori delle UOP.

2.1.2 Responsabile della Conservazione Digitale (RCD)

Il RCD coincide, per l'Azienda, con la figura del RGD.

Il RCD definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il RCD, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione (al quale si rimanda per il dettaglio delle operazioni di conservazione), deve individuare le specifiche funzioni e competenze delegate.

In particolare, il RCD:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare, della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dalle Linee Guida;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- provvede per le amministrazioni statali centrali e periferiche a versare i documenti.

2.1.3 Responsabile per la protezione dei dati personali (DPO)

I compiti principali del DPO sono individuati dall'art. 39 paragrafo 1 del Regolamento UE del Parlamento e del Consiglio europeo 2016/679:

- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Servizio "Privacy, Gestione Atti e Supporto RPCT" collabora con il DPO nelle attività sopra elencate.

2.1.4 Responsabile per la transizione al digitale (RTD)

Ai sensi dell'art. 17 del Decreto Legislativo 82/2005 (Codice dell'Amministrazione Digitale) nonché della Circolare n. 3 del 1 ottobre 2018 del Ministro per la Pubblica Amministrazione, l'Azienda ha individuato nella figura del Direttore il RTD.

Il RTD è a capo dell'ufficio per la transizione digitale che ai sensi della Deliberazione del Consiglio di Amministrazione n. 18/2022 corrisponde al Servizio "Sviluppo Progetti, Protocollo e Amministrazione Digitale", supportato dai Servizi aziendali competenti in materie specifiche, al quale sono assegnati i seguenti compiti:

- coordinamento strategico dello sviluppo dei sistemi informativi di telecomunicazione e fonia;
- indirizzo e coordinamento dello sviluppo dei servizi, sia interni sia esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività;

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

2.1.5 Responsabile dei sistemi informativi

Il Responsabile dei sistemi informativi coincide con il Coordinatore del Servizio “Sistemi Informatici e Applicativi – ICT”.

I principali compiti riguardano la programmazione, gestione, manutenzione, implementazione, sviluppo e supervisione della rete informatica, dei server, della dotazione hardware e software dell’Azienda, da attuarsi mediante attività gestite direttamente o esternalizzate.

2.1.6 Amministratore di sistema

La figura di Amministratore di sistema, per l’Azienda, coincide con quella del Dirigente dell’Area “Approvvigionamenti e Contratti, Servizi Tecnici e Informatici”.

Con riferimento ad ogni applicativo installato sulle postazioni informatiche dell’Azienda ad esclusione di quelli elencati nel registro dei trattamenti nella sezione relativa alle attività per le quali l’Azienda ha attribuito incarico di Responsabile del trattamento esterno dei dati ai sensi del Regolamento UE 2016/679 del Parlamento e del Consiglio europeo, l’Amministratore di Sistema è tenuto:

- ad impostare ed aggiornare le proprie credenziali di utilizzo del sistema rispettando quanto previsto dal paragrafo “ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE” della Circolare AGID n. 2/2017 “Misure minime di sicurezza ICT per le Pubbliche Amministrazioni”, per quanto in proprio potere;

- a seguire le indicazioni riportate nel Disciplinare d'uso delle risorse informatiche e dell'accesso ai servizi di rete del Titolare per l'attivazione/aggiornamento degli account utenti sul sistema;
- a monitorare regolarmente e adeguatamente la funzionalità del sistema, servizio, apparato, database, relazionandosi adeguatamente con eventuali fornitori esterni dei sistemi e dei servizi di assistenza e manutenzione;
- a comunicare tempestivamente al Titolare o al delegato dello stesso eventuali rischi potenziali, problematiche, anomalie o criticità relative alla sicurezza dei dati occorse nelle attività di trattamento e di amministrazione di sistemi, relazionando sulle eventuali azioni correttive poste in atto (da lui o dal fornitore dei servizi di assistenza/manutenzione) e sugli esiti delle stesse;
- a fornire ogni assistenza al Titolare e al DPO del Titolare, soprattutto qualora sia necessario attivare le procedure per i Data Breach, ovvero garantire i diritti degli interessati.

Con riferimento all'infrastruttura informatica dell'Azienda, l'Amministratore di Sistema è tenuto ad applicare i controlli identificati al livello minimo del documento misure di sicurezza – Circolare AGID n. 2/2017 - per quanto in proprio potere e non delegato contrattualmente ai Responsabili esterni del trattamento, ed in particolare:

- monitorare la funzionalità del sistema, servizio, apparato, database di cui abbia la responsabilità;
- effettuare, in caso di necessità, gli interventi di assistenza e manutenzione consentiti dal profilo autorizzativo del proprio account amministrativo;
- attivare le credenziali di autenticazione univocamente correlate ai soggetti autorizzati del trattamento, con caratteristiche di robustezza adeguate a garantire una ragionevole sicurezza dei trattamenti e configurare il profilo di autorizzazione coerentemente alle specifiche mansioni affidate (basi dati accessibili e trattamenti consentiti);
- verificare la funzionalità degli strumenti per la protezione dei dati contro il rischio di intrusione (firewall) e dell'azione di programmi informatici malevoli (virus informatici etc.);
- aggiornare periodicamente i programmi allo scopo di prevenire la vulnerabilità degli strumenti elettronici e correggerne i difetti;
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e sovraintendere alle operazioni di backup periodico degli stessi con copie di sicurezza;
- assicurarsi della qualità delle copie di sicurezza dei dati ed applicare i criteri per la conservazione, il riutilizzo e/o la distruzione delle copie di sicurezza delle banche dati;
- segnalare tempestivamente al Titolare o al delegato dello stesso eventuali rischi o anomalie nella gestione delle misure di sicurezza relative ai dati personali;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento degli strumenti elettronici.

L'Amministratore di sistema è inoltre tenuto a proporre al Titolare l'adozione e occuparsi della conseguente gestione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono

comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Per l'espletamento dell'incarico, vengono assegnate all'Amministratore di sistema le credenziali di autenticazione che gli permettono l'accessibilità al sistema per lo svolgimento delle stesse funzioni assegnate.

L'Amministratore di sistema risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza. Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

Resta inteso che, per la tipologia di rapporti contrattuale che intercorre tra Titolare e Amministratore di sistema, è al Titolare che spetta il compito di creare le condizioni tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento). L'Amministratore di sistema, relativamente alla parte di log management, si atterrà a quanto verrà disposto dal Titolare del Trattamento.

Sono individuati quali sub-amministratori di sistema i dipendenti del Servizio "Sistemi Informatici e Applicativi – ICT", appositamente delegati con atto acquisito al protocollo aziendale.

2.1.7 Addetti delle Unità Operative di Protocollo

Ciascuna sede territoriale dell'Azienda ha una propria UOP afferente alla AOO unica. L'ubicazione delle sedi amministrative è la seguente:

- Firenze: Viale Antonio Gramsci 36 - Cap 50132 (sede legale)
- Pisa: Piazza dei Cavalieri 6 - Cap 56126
- Siena: Via Paolo Mascagni 53 - Cap 53100

L'orario di apertura al pubblico delle UOP è pubblicato sul sito istituzionale all'indirizzo: https://www.dsu.toscana.it/servizio-protocollo .

Gli addetti delle UOP:

- hanno l'abilitazione e l'autorizzazione ad eseguire le operazioni di acquisizione, registrazione, classificazione, segnatura, smistamento ed invio dei documenti sul registro di protocollo generale;
- hanno, altresì, l'abilitazione e l'autorizzazione ad eseguire le operazioni di acquisizione, registrazione, classificazione, segnatura, smistamento ed invio dei documenti sugli altri repertori presenti nel sistema di gestione informatica dei documenti;
- provvedono all'affrancatura della corrispondenza analogica in uscita e alla consegna al centro di smistamento postale attraverso apposito servizio di *pick-up* o attraverso apposito servizio telematico;
- verificano l'effettiva ricezione dei messaggi di posta elettronica certificata (inviati dall'indirizzo dsutoscana@postacert.toscana.it) ed in caso di mancato recapito provvedono ad avvisare il servizio aziendale competente;
- verificano l'eventuale presenza di messaggi di errore di consegna della posta elettronica convenzionale (inviati dalla casella protocollo@dsu.toscana.it) e provvedono ad avvisare il servizio aziendale

competente;

- procedono, a seguito dell'autorizzazione del RGD o del suo vicario, all'annullamento delle registrazioni di protocollo.

2.1.8 Utenti interni appartenenti ai Servizi aziendali

L'Azienda è suddivisa in Aree e ciascuna di esse è composta da una pluralità di Servizi.

L'elenco degli utenti interni abilitati all'accesso al sistema di gestione informatica dei documenti è riportato nella "Gestione Organigramma" dello stesso.

Tutti gli utenti interni sono tenuti a consultare giornalmente i documenti assegnati dagli addetti delle UOP e – se ricoprono posizioni apicali o di coordinamento - a curarne lo smistamento ai propri collaboratori ovvero ad altri soggetti aziendali cui i documenti siano di competenza (se non già avvenuto a cura delle UOP).

Per gli utenti presenti nell'organigramma vigente, gli addetti delle UOP provvedono a smistare con notifica i documenti ad essi indirizzati a meno che il mittente non abbia previsto modalità di invio alternative.

Qualora i destinatari delle missive siano le rappresentanze dei lavoratori, indipendentemente dalla modalità di spedizione indicata dal mittente, gli addetti delle UOP provvedono allo smistamento con notifica e all'invio tramite posta elettronica tradizionale dall'indirizzo protocollo@dsu.toscana.it.

Con Provvedimento del Direttore vengono individuati i Servizi responsabili della gestione della fascicolazione archivistica (Allegato F al presente Manuale).

CAPITOLO 3 – STRUMENTI PER LA FORMAZIONE DEI DOCUMENTI INFORMATICI, PER LO SCAMBIO E L'ACCESSO

(Il contenuto di questo capitolo riprende in parte quanto riportato nel paragrafo 3.5.1 lettera a – Linee Guida)

3.1 Il documento informatico

3.1.1 Formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle Linee Guida;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica;

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

L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.

L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti.

In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nelle Linee Guida[1].

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

[1] Linee Guida, allegato 6, tabella 1 del paragrafo 2.2.

Modalità di formazione del documento informatico	Criteri per garantire l'immodificabilità e l'integrità *(una o più delle operazioni sotto indicate)*
Lettera a)	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza ai sensi del paragrafo 3.9 delle Linee Guida; • trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale; • versamento ad un sistema di conservazione
Lettera b)	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza ai sensi del paragrafo 3.9 delle Linee Guida; • versamento ad un sistema di conservazione
Lettera c)	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema; • produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione
Lettera d)	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema; • produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione

La certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che ha sottoscritto il documento stesso.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati.

I metadati definiti per le diverse tipologie documentarie sono riportati nell'allegato D del presente Manuale.

L'evidenza informatica corrispondente al documento informatico immodificabile è prodotta in uno dei formati contenuti nell'Allegato 2 "Formati di file e riversamento" delle Linee Guida ove sono specificate, anche, le caratteristiche e i criteri di scelta del formato stesso.

3.1.2 Copie per immagine su supporto informatico 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 o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" delle Linee Guida.

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD nel caso in cui non vi sia l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1 bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

3.1.3 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; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto.

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti
- certificazione di processo

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" delle Linee Guida.

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23 bis comma 2 del CAD nel caso in cui non vi sia l'attestazione di un

pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

3.2 Il documento amministrativo informatico – Indicazioni operative interne

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 3.1.1 del presente Manuale, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, nonché i metadati relativi alla classificazione, ai sensi dell'articolo 56 del TUDA, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle Linee Guida.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel presente Manuale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter comma 5 bis del CAD, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

I Servizi aziendali utilizzano per la formazione dei documenti amministrativi informatici le applicazioni messe a disposizione dall'Azienda avendo cura di convertire – laddove possibile - qualsiasi documento, compresi gli allegati, in formato PDF/A. A tal fine, viene reso disponibile apposito software già configurato per la conversione in tale formato.

Sui documenti amministrativi informatici deve essere apposta la firma digitale avendo cura di verificare la validità della firma apposta attraverso una delle applicazioni messe a disposizione dall'Azienda.

Il formato di firma digitale consigliato dall'Azienda è il PADES che consente di mantenere l'estensione pdf.

In alternativa è comunque possibile utilizzare il formato CADES il quale, in ogni caso, deve essere utilizzato per la sottoscrizione di file con estensioni differenti dal pdf.

L'Azienda mette a disposizione dei servizi aziendali anche un pacchetto di marche temporali da utilizzare qualora si rendesse necessario un riferimento temporale certificato opponibile a terzi.

Ogni documento, formato per essere inoltrato all'esterno o all'interno in modo formale, deve essere redatto sui modelli ufficiali reperibili nella intranet aziendale.

È obbligatorio inoltre attenersi alle disposizioni inerenti:

- la corretta indicazione delle sigle che identificano le aree aziendali
- la corretta indicazione del servizio aziendale o dell'area che ha prodotto il documento

Oltre agli elementi presenti nei modelli di immagine coordinata dovranno essere inseriti i seguenti dati:

- numero degli allegati, se presenti
- oggetto del documento
- sottoscrizione
- modalità di spedizione (se l'invio avviene per posta elettronica tradizionale o PEC occorre indicare i relativi indirizzi)

In assenza delle informazioni sopraindicate le UOP non procedono alla protocollazione e restituiscono il documento al servizio che ha redatto il documento.

3.3 Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 3.1.2.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

3.4 Modalità di scambio dei documenti amministrativi informatici

3.4.1 Trasmissione dei documenti informatici all'interno dell'AOO

I documenti amministrativi informatici protocollati dalle UOP sono trasmessi all'interno dell'AOO:

- mediante il sistema di gestione informatica dei documenti (con o senza notifica)
- inviati tramite email (dalla casella di posta elettronica istituzionale protocollo@dsu.toscana.it)

3.4.2 Trasmissione dei documenti informatici verso l'esterno: AOO afferenti ad altri Enti

Lo scambio di documenti amministrativi protocollati tra l'AOODSUTOSCANA e AOO afferenti ad altre Pubbliche Amministrazioni avviene di norma tramite posta elettronica certificata in formato di interoperabilità.

3.4.3 Trasmissione dei documenti informatici verso l'esterno: altri soggetti

La trasmissione di documenti amministrativi informatici protocollati verso soggetti diversi dalle Pubbliche Amministrazioni avviene principalmente tramite posta elettronica certificata.

L'invio tramite posta elettronica ordinaria viene effettuato esclusivamente qualora il destinatario non sia provvisto di una casella di posta elettronica certificata.

3.5 Firma digitale

L'Azienda, attraverso il Registration Authority Officer (Dott. Marco Aleksy Commisso), rilascia – dopo adeguata verifica dell'identità personale - ai Dirigenti, alle Posizioni Organizzative, ai Responsabili Unici dei Procedimenti, ai Direttori dell'Esecuzione nonché ad ogni altro dipendente (su richiesta del Dirigente di riferimento) il dispositivo di firma digitale.
Il certificato di firma digitale ha una durata triennale.

3.6 Diritto di accesso civico

Il diritto a conoscere dati, documenti e informazioni formati o detenuti dall'Azienda può essere esercitato attraverso la visualizzazione degli stessi nel sito istituzionale o, quando questi non sono pubblicati, con la richiesta di accesso così come previsto dal Decreto Legislativo n. 33/2013 recante "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità e diffusione di informazioni da parte delle pubbliche amministrazioni*".

3.6.1 Accesso civico semplice

Nell'ipotesi di mancata pubblicazione di un atto, documento o altra informazione per il quale è previsto l'obbligo di pubblicazione ai sensi della normativa vigente, gli interessati possono esercitare il diritto di accesso civico ai sensi dell'art. 5, comma 1 del Decreto Legislativo n. 33/2013, per vedere esercitato il diritto attraverso la richiesta di pubblicazione dei documenti.

L'Azienda, entro trenta giorni, deve procedere alla pubblicazione nel proprio sito web istituzionale, del dato, documento o informazione richiesta e, contestualmente, trasmetterlo al richiedente. In alternativa, può comunicare al medesimo l'avvenuta pubblicazione e indicare il collegamento ipertestuale a quanto richiesto.

Se invece il documento, l'informazione o il dato richiesti sono già pubblicati, l'Azienda provvede a specificare al richiedente il relativo collegamento ipertestuale.

La richiesta di accesso civico è riconosciuta a chiunque e non deve essere motivata. Deve essere presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza - che si pronuncia sulla stessa – secondo le modalità indicate nel sito istituzionale dell'Azienda, sezione: Amministrazione Trasparente - Altri contenuti - Accesso civico.

In caso di ritardo o mancata risposta, entro trenta giorni dall'istanza presentata, il richiedente può ricorrere al titolare del potere sostitutivo.

A fronte dell'inerzia da parte del Responsabile della Prevenzione della Corruzione e della Trasparenza o del Titolare del potere sostitutivo, il richiedente, ai fini della tutela del proprio diritto, può proporre ricorso al Tribunale Amministrativo Regionale ai sensi dell'art. 116 del Decreto Legislativo n. 104/2010.

3.6.2 Accesso civico generalizzato

L'accesso civico generalizzato è la richiesta fatta da un soggetto all'Azienda per visionare o chiedere copia di dati e documenti detenuti dall'amministrazione stessa e per i quali non ci sono obblighi di pubblicazione. La richiesta non necessita di motivazione, in quanto nasce dal diritto all'informazione che ciascuno ha e la regola generale è rappresentata dalla trasparenza. Questa forma di accesso è stata riconosciuta allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

L'istanza può essere presentata secondo le modalità indicate nel sito istituzionale dell'Azienda, sezione: Amministrazione Trasparente - Altri contenuti - Accesso civico.

Per procedere nella richiesta avanzata è necessario che siano identificati i dati, le informazioni o i documenti che si desidera richiedere. Sono, infatti, inammissibili le richieste nelle quali l'oggetto sia talmente vago da non permettere di identificare la documentazione di interesse, oppure laddove la predetta richiesta risulti manifestamente irragionevole.

Il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali.

Ai sensi dell'art. 5 bis del Decreto Legislativo n. 33/2013, l'accesso civico generalizzato può essere rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di un interesse pubblico (sicurezza pubblica e l'ordine pubblico, la sicurezza nazionale, la difesa e le questioni militari, le relazioni internazionali, la politica e la stabilità finanziaria ed economica dello Stato, la conduzione di indagini sui reati e il loro perseguimento, il regolare svolgimento di attività ispettive) o per evitare un pregiudizio concreto alla tutela di un interesse privato (connesso alla protezione dei dati personali, alla libertà e segretezza della corrispondenza, agli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali).

Laddove l'istanza di accesso civico possa incidere su interessi di soggetti controinteressati legati alla protezione dei suddetti interessi privati, l'Azienda ha l'obbligo di interpellare i controinteressati. Il soggetto controinteressato può presentare, entro dieci giorni dalla ricezione di tale comunicazione, una eventuale e motivata opposizione all'istanza di accesso civico. Decorso tale termine l'Azienda, accertata la ricezione della comunicazione da parte del controinteressato, provvede sulla richiesta di accesso civico.

Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza con la comunicazione del relativo esito al richiedente e agli eventuali controinteressati.

Tali termini sono sospesi nel caso di comunicazione dell'istanza al controinteressato durante il tempo stabilito dalla norma per consentire allo stesso di presentare eventuale opposizione (10 giorni dalla ricezione della comunicazione).

In caso di accoglimento l'Azienda provvede a trasmettere tempestivamente al richiedente i dati o i documenti richiesti. Laddove vi sia stato, invece, l'accoglimento della richiesta di accesso civico nonostante l'opposizione del controinteressato, l'Azienda è tenuta a darne comunicazione a quest'ultimo.

La stessa Azienda, ai sensi dell'art. 5, comma 2, del Decreto Legislativo n. 33/2013 è tenuta a motivare l'eventuale rifiuto, differimento o la limitazione dell'accesso con riferimento ai soli casi e limiti stabiliti dall'art.

5 bis, e contestualmente, se ne ritiene opportuno, può chiedere un parere formale al Garante per la protezione dei dati personali.

L'istante, nel caso di diniego totale o parziale dell'accesso o di mancata risposta entro trenta giorni dalla presentazione della richiesta, ovvero i controinteressati, nei casi di accoglimento della richiesta di accesso nonostante la loro motiva opposizione, possono presentare domanda di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato entro il termine di venti giorni.

Il Garante per la protezione dei dati personali può essere interpellato dal Responsabile della Prevenzione della Corruzione e della Trasparenza nel caso di richiesta di riesame solo laddove l'accesso civico sia stato negato o differito per motivi attinenti la tutela della «*protezione dei dati personali, in conformità con la disciplina legislativa in materia*» (art. 5 bis, comma 2, lett. a, Decreto Legislativo n. 33/2013). In tali ipotesi, il Garante si pronuncia entro il termine di dieci giorni dalla richiesta, durante i quali il termine per l'adozione del provvedimento da parte del Responsabile della Prevenzione della Corruzione e della Trasparenza è sospeso.

La decisione dell'Azienda sulla richiesta e il provvedimento del Responsabile della Prevenzione della Corruzione e della Trasparenza possono essere impugnati davanti al Tribunale Amministrativo Regionale ai sensi dell'art. 116 del Decreto Legislativo n. 104/2010.

L'accesso civico generalizzato è rifiutato per evitare un pregiudizio concreto alla tutela di interessi pubblici (sicurezza e ordine pubblico, sicurezza nazionale, difesa e questioni militari, relazioni internazionali, politica e stabilità finanziaria ed economica dello Stato. indagini su reati e loro perseguimento, svolgimento attività ispettive) e alla tutela di interessi privati (protezione dati personali, libertà e segretezza della corrispondenza, interessi economici e commerciali di persone fisiche e giuridiche quali ad esempio: la proprietà intellettuale, il diritto d'autore e segreti commerciali). L'Autorità Nazionale Anticorruzione con la Deliberazione n. 1309 del 28 dicembre 2016 ha adottato le "*Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 c. 2 del D.Lgs. 33/2013*".

3.7 Accesso ai documenti amministrativi (legge 241/1990)

Possono richiedere l'accesso ad atti e documenti amministrativi tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiamo un interesse diretto, concreto e attuale collegato ad una situazione giuridicamente tutelata e connessa al documento oggetto di richiesta di accesso.
La richiesta può essere presentata dai diretti interessati o da persone delegate. La delega, con copia fotostatica del documento di identità del delegante, deve essere allegata alla richiesta.
La richiesta di accesso, qualora non sia sottoscritta dall'interessato in presenza di un dipendente addetto alla ricezione, deve essere sottoscritta e presentata, obbligatoriamente, unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La mancanza della copia del documento rende l'istanza improcedibile.
Nel caso di accesso formale l'ufficio deve concludere il procedimento entro 30 giorni dal ricevimento della richiesta, ad eccezione dei casi di sospensione o differimento.
Nell'istanza l'interessato deve:

- dimostrare la propria identità o i poteri di rappresentanza del soggetto interessato;

- indicare gli elementi che consentono di individuare i documenti amministrativi ai quali si chiede di accedere; nel caso di documenti composti da più allegati, è sempre onere del richiedente indicare in maniera specifica le parti e/o gli allegati di interesse;
- specificare il proprio interesse diretto, concreto ed attuale;
- specificare le modalità con cui intende esercitare il diritto di accesso;
- apporre data e sottoscrizione

Il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali, come indicato nel "Regolamento disciplinante i procedimenti relativi all'accesso civico, all'accesso civico generalizzato e all'accesso ai documenti amministrativi L. 241/1990" approvato con Deliberazione n. 61/22 del 16.11.2022. L'accesso ai documenti è escluso nei casi previsti dall'art. 24 della legge 241/1990 e ss.mm.ii e negli altri casi previsti dalla legge, in aggiunta a quanto stabilito dall'art. 26 del Regolamento sopra indicato.
In caso di diniego o differimento il richiedente può presentare ricorso al tribunale amministrativo regionale (TAR Toscana).

CAPITOLO 4 - SISTEMA DI GESTIONE, CLASSIFICAZIONE, FASCICOLAZIONE

4.1 Premessa

In questo capitolo verranno descritti il sistema di classificazione dei documenti, le modalità di formazione del fascicolo (fascicolazione archivistica) e di conservazione dell'archivio.

4.2 Classificazione dei documenti

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del Titolario di classificazione.

Il Titolario e il piano di conservazione (adottati con Provvedimento del Direttore) sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'Azienda.

La classificazione si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

La classificazione dei documenti soggetti a registrazione di protocollo viene effettuata dalle UOP.

Il RGD verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento.

Il Titolario di classificazione (Allegato B al presente Manuale) è un sistema logico che suddivide i documenti amministrativi secondo la funzione esercitata, in titoli, classi (ed eventualmente sottoclassi) permettendo di organizzare in maniera omogenea i documenti che si riferiscono a medesimi affari o a medesimi procedimenti amministrativi.

L'aggiornamento del Titolario compete esclusivamente al RGD.

La revisione periodica tiene conto delle disposizioni legislative, dell'evoluzione tecnologica e delle migliori pratiche in materia di formazione e conservazione degli archivi.

Ad ogni modifica del Titolario, il RGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo.

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.

4.3 Selezione e scarto

I documenti analogici ed informatici possono essere oggetto di selezione e scarto secondo quanto riportato nel relativo Piano.

Periodicamente (almeno 1 volta all'anno) il RGD propone alla Soprintendenza Archivistica e Bibliografica della

Regione Toscana una ipotesi di scarto della documentazione che ha superato i limiti temporali di conservazione. Solo una volta ricevuta l'autorizzazione allo scarto, il RGD procede con le attività necessarie per disporre la distruzione della documentazione.

A conclusione di tale attività il RGD provvede a trasmettere alla Soprintendenza il verbale di avvenuta distruzione.

Il piano di selezione e scarto è adottato con Provvedimento del Direttore ed è allegato al presente Manuale (Allegato E).

4.4 Archivio

L'archivio è il complesso dei documenti prodotti, acquisiti o utilizzati dall'Azienda nell'esercizio delle proprie funzioni e nello svolgimento della propria attività.

L'archivio generale è unico (anche se conservato in luoghi differenti). In relazione alla sua gestione, si suddivide in:

- archivio corrente
- archivio di deposito
- archivio storico

L'archivio corrente è il complesso di documenti relativi ad affari ed a procedimenti amministrativi:

- in corso di istruttoria o di trattazione;
- conclusi da breve periodo e pertanto aventi ancora un forte interesse ai fini dello svolgimento dell'attività corrente.

I servizi aziendali sono tenuti alla corretta custodia dei documenti relativi alle funzioni e alle attività esercitate e non ancora concluse.

L'archivio di deposito è il complesso di documenti relativi ad affari ed a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o verso i quali sussistono saltuarie esigenze di consultazione ai fini dell'attività corrente.

Periodicamente e secondo un apposito piano di versamento, ogni Servizio deve trasferire all'archivio generale i fascicoli relativi ad affari e a procedimenti conclusi.

L'archivio storico è il complesso di documenti relativi ad affari ed a procedimenti amministrativi conclusi e destinati, previa effettuazione delle operazioni di scarto, alla conservazione permanente.

4.5 Fascicolazione

4.5.1 Fascicolazione archivistica

Tutti i documenti registrati nel Sistema di gestione informatica dei documenti e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.

Ogni documento, dopo la classificazione, viene inserito nel fascicolo di riferimento.

I documenti sono archiviati all'interno di ciascun fascicolo, o, all'occorrenza, sotto-fascicolo o inserito, secondo l'ordine cronologico di registrazione.

4.5.2 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'AOO, i soggetti designati per la gestione dei fascicoli provvedono all'apertura di un nuovo fascicolo. La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni:

- tipologia del fascicolo
- oggetto del fascicolo
- descrizione
- codice del fascicolo
- ubicazione
- anni di conservazione nell'archivio corrente
- anni di conservazione nell'archivio di deposito
- soggetto
- note
- voci d'indice
- visibilità del fascicolo (indicazione degli utenti o dei servizi aziendali cui è consentita la visibilità)
- servizio aziendale responsabile del fascicolo
- utente responsabile del fascicolo

4.5.3 Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

4.5.4 Processo di assegnazione dei fascicoli

Il soggetto deputato all'operazione di fascicolazione, valuta se il documento stesso debba essere ricollegato ad un affare o procedimento in corso e pertanto debba essere inserito in un fascicolo già esistente oppure se il documento si riferisce a un nuovo affare, o procedimento, per cui è necessario aprire un nuovo fascicolo. A seconda delle ipotesi, si procede come segue:

- se il documento si ricollega ad un affare o procedimento in corso, l'addetto seleziona il relativo

fascicolo e collega la registrazione di protocollo del documento al fascicolo selezionato;

- se il documento da avvio ad un nuovo fascicolo, il soggetto preposto esegue le operazioni di apertura di cui al paragrafo 4.5.2.

4.5.5. Modifica dell'assegnazione dei fascicoli

Quando si verifica un errore nell'assegnazione di un fascicolo, l'utente abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico: Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua la modifica, con la data e l'ora dell'operazione.

4.5.6 Repertorio dei fascicoli

I fascicoli, sono annotati nel repertorio dei fascicoli.

Il repertorio dei fascicoli, ripartito per ciascun titolo del Titolario, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del Titolario e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il Titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

Il repertorio dei fascicoli è costantemente aggiornato.

4.6 Protezione e conservazione degli archivi

Gli archivi e i singoli documenti dello Stato, delle regioni e degli enti pubblici sono beni culturali inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, e deve essere conservato nella sua organicità.

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

La richiesta di consultazione, e di conseguenza di movimentazione dei fascicoli, può pervenire dall'interno dell'Azienda, oppure da utenti esterni per scopi giuridico- amministrativi o per scopi storici.

4.7 Consultazione da parte di personale esterno all'Azienda

La domanda di accesso ai documenti viene presentata alle UOP, direttamente presso ciascuna sede oppure

tramite PEC.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'Azienda.

4.8 Consultazione da parte di personale interno all'Azienda

I servizi aziendali, per motivi di consultazione, possono richiedere in ogni momento alle UOP i fascicoli conservati nella sezione archivistica di deposito o storica, comunicando tale necessità all'indirizzo protocollo@dsu.toscana.it.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito, o storico, avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Tale movimentazione viene registrata a cura del RGD in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, degli stessi rispettandone la sedimentazione archivistica e il vincolo.

In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

Il RGD verifica, per ogni richiesta, la possibilità di esaudire la medesima attraverso l'invio del fascicolo in forma elettronica.

CAPITOLO 5 – DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI E REGOLE DI SMISTAMENTO

5.1 Flusso di lavorazione dei documenti

La descrizione del flusso di lavorazione dei documenti all'interno dell'AOO è riportata nei successivi paragrafi. Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. Essi si riferiscono ai documenti:

- **ricevuti** dalla AOODSUTOSCANA, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale alle aree funzionali e/o ai servizi aziendali;
- **inviati** dalla AOODSUTOSCANA all'esterno o anche all'interno di essa, in modo formale.

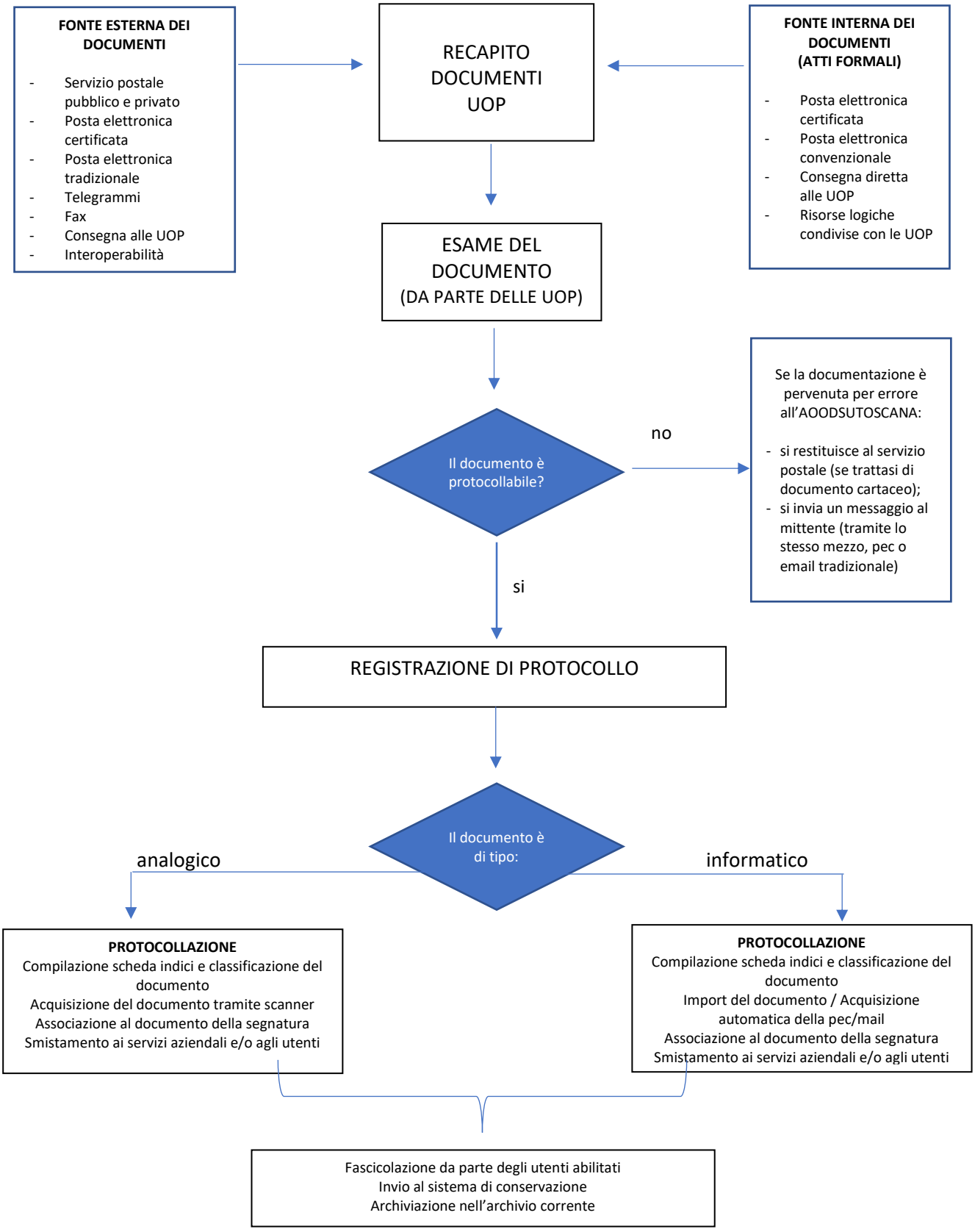
Le comunicazioni informali tra uffici avvengono tramite posta elettronica interna e non sono soggette a protocollazione.

Sono invece soggette a protocollazione le comunicazioni che vengono inviate dalla posta elettronica aziendale del dipendente alla casella istituzionale protocollo@dsu.toscana.it quando esse assumono rilevanza ai fini dei procedimenti amministrativi.

La documentazione che non è stata registrata presso una UOP viene considerata giuridicamente inesistente presso l'Azienda.

Non è consentita la protocollazione di un documento già protocollato. In caso di duplicazione di una registrazione di protocollo si procede ad annullare il protocollo più recente, dandone comunicazione al destinatario se trattasi di documento già trasmesso.

5.1.1 Flusso dei documenti in ingresso



5.1.1.1 Documenti analogici in arrivo

La corrispondenza pervenuta a mezzo posta convenzionale o corriere è consegnata alla UOP competente per sede che provvede ad una preliminare verifica del mittente e del destinatario.

Le buste sulle quali è riportata l'indicazione "Riservata", "Personale", "Confidenziale" (o simili) devono essere consegnate al destinatario che ne valuterà il contenuto e, nel caso in cui si rendesse necessaria la protocollazione, provvederà a inoltrarla alla UOP competente per sede per la registrazione.

La corrispondenza ricevuta via telegramma o via telefax è trattata come un documento cartaceo.

Le ricevute di ritorno della posta raccomandata non devono essere protocollate: esse vengono consegnate ai servizi aziendali competenti.

La busta delle missive (qualora esse pervengano tramite raccomandata, raccomandata a.r., corriere o altra modalità di spedizione tracciabile) viene scansionata e acquisita come allegato per la parte relativa al timbro postale e al codice a barre.

Eventuali planimetrie o documenti composti da numerose pagine che rendono non praticabile la scansione degli stessi e l'acquisizione nel sistema di gestione dei flussi documentali, vengono scansionati limitatamente al frontespizio dando evidenza nelle annotazioni della scheda di protocollo del servizio aziendale dove gli atti sono reperibili nella loro interezza.

Qualora la corrispondenza non rientrasse nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in arrivo è aperta di norma il giorno lavorativo in cui è pervenuta, e protocollata entro la fine della giornata successiva.

Qualora gli originali debbano essere consegnati al servizio competente se ne dà menzione nelle note della scheda di protocollo dell'applicativo di gestione dei flussi documentali.

Gli originali esclusi dalla protocollazione saranno consegnati al Servizio interessato.

I Servizi aziendali consegnano alla UOP competente per sede i documenti cartacei a loro pervenuti direttamente che necessitano di protocollazione (consegnati a mano da studenti, dipendenti, fornitori; ricevuti per telefax; ricevuti direttamente per posta presso le strutture aziendali).

I Servizi aziendali, in caso di allegati piuttosto voluminosi, sono invitati a trasmettere alla UOP competente per sede, gli stessi documenti su supporto ottico.

Per la corrispondenza recapitata a mano da utenti esterni gli operatori della UOP, su richiesta dell'interessato, rilasciano apposita ricevuta.

Qualora un utente si presenti presso una UOP per consegnare un documento riguardante un altro soggetto, è necessario che costui sia munito di delega con copia del documento di identità della persona delegante (oltre al proprio) che verranno acquisiti assieme alla documentazione presentata.

Le istanze e le dichiarazioni sostitutive di atto di notorietà presentate presso le UOP, sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo.

5.1.1.2 Errata ricezione di documenti analogici

Nel caso in cui pervengano erroneamente, tramite il servizio postale, buste indirizzate ad altri soggetti, le stesse non devono essere aperte, ma restituite tempestivamente all'addetto che consegna la posta.

Qualora una busta venga erroneamente aperta è compito degli operatori delle UOP:

- apporre all'esterno di essa la dicitura "aperta per errore"
- provvedere a inviarla al destinatario tramite apposita lettera di trasmissione protocollata in uscita

5.1.1.3 Documenti informatici in arrivo

La ricezione dei documenti informatici è assicurata di norma tramite:

- la casella di posta elettronica certificata: dsutoscana@postacert.toscana.it;
- la casella di posta elettronica certificata: dsuprotocollo@postacert.toscana.it (non adibita alla ricezione di documentazione dall'esterno ma utilizzata esclusivamente in interoperabilità con l'applicazione di gestione benefici);
- la casella di posta elettronica tradizionale: protocollo@dsu.toscana.it;
- strumenti di interoperabilità tra le PP.AA.;
- risorse logiche condivise con le UOP (solo all'interno dell'Azienda);
- la intranet aziendale (Portale dipendenti);
- acquisizione da risorse esterne (par. 5.1.1.4);
- acquisizione da supporto informatico (part. 5.1.1.5).

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.

I messaggi provenienti da una casella di posta elettronica certificata in arrivo sulla casella PEC istituzionale (abilitata alla ricezione di messaggi provenienti esclusivamente da caselle PEC) nonché i messaggi in arrivo sulla casella di posta elettronica tradizionale vengono protocollati, previa verifica:

- della necessità di procedere alla protocollazione;
- della validità di eventuali firme digitali apposte;
- della leggibilità del contenuto;
- della provenienza

Le comunicazioni in arrivo sulla casella dsutoscana@postacert.toscana.it o protocollo@dsu.toscana.it sono senz'altro protocollate in presenza di questi elementi:

- il messaggio in arrivo sulla casella protocollo@dsu.toscana.it proviene da una casella di posta elettronica univocamente assegnata dagli Atenei della Toscana agli studenti universitari;
- il messaggio in arrivo sulla casella protocollo@dsu.toscana.it proviene da una casella di posta elettronica rilasciata a ciascun dipendente dell'Azienda (fatto salvo quanto previsto dall'art. 38 comma 3 del TUDA);
- l'istanza allegata al messaggio è firmata digitalmente, con altro tipo di firma elettronica qualificata o

con firma elettronica avanzata o, comunque, formate previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 del Codice dell'amministrazione digitale – CAD con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore;

- l'istanza è presentata attraverso il Sistema pubblico di identità digitale - SPID, la Carta di identità elettronica - CIE o la carta nazionale dei servizi – CNS;
- l'istanza è presentata con allegato documento di identità del dichiarante;
- l'istanza è trasmessa dal proprio domicilio digitale iscritto all'interno degli elenchi IPA, INI-PEC e INAD o, in assenza di un domicilio digitale iscritto, da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS.

Nel caso in cui il messaggio venga ricevuto su una casella di posta elettronica non destinata al servizio di protocollazione o su una casella di PEC diversa da quella istituzionale esso deve essere trasmesso via email (o via PEC) alle relative caselle istituzionali.

È preferibile, tuttavia, chiedere ai mittenti di rinviare la mail (o il messaggio PEC) agli indirizzi di cui sopra.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente, il messaggio è comunque inserito nel sistema di gestione documentale con il formato di origine e successivamente protocollato, smistato, assegnato e gestito. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo.

5.1.1.4 Documenti informatici resi disponibili attraverso download da risorse esterne

Nel caso in cui pervengano messaggi di posta elettronica (certificata o tradizionale) contenenti link dal quale scaricare documenti informatici (generalmente per via delle dimensioni degli stessi) essi vengono protocollati (dopo aver scaricato e controllato i documenti ed averli allegati al messaggio stesso nella scheda "allegati esterni" del software di gestione dei flussi documentali) solo se provenienti:

- da una pubblica amministrazione ai sensi dell'art. 47, c. 1 del CAD;
- da operatori economici per le quali sono in essere procedure di approvvigionamento di beni e servizi.

5.1.1.5 Documenti informatici su supporto informatico

I documenti informatici resi disponibili su supporto informatico sono acquisiti nella scheda "allegati esterni" del software di gestione documentale qualora la dimensione complessiva sia < 100 MB.

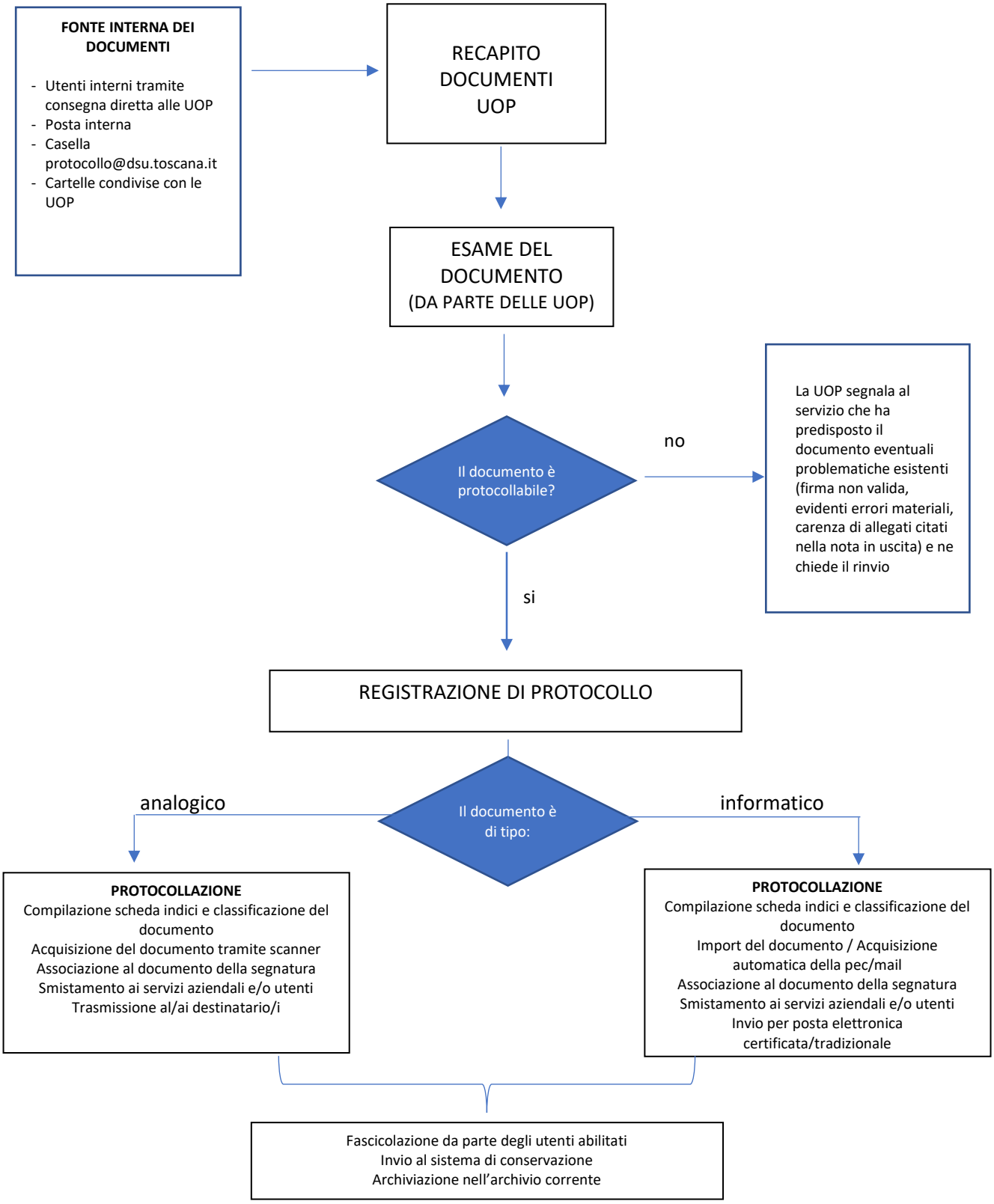
Qualora la dimensione superi i 100 MB il supporto viene conservato presso la UOP e copia di esso viene trasmessa ai destinatari indicati nel software di gestione dei flussi documentali. Di ciò ne viene data menzione nel campo "annotazioni" del software di gestione dei flussi documentali.

5.1.1.6 Errata ricezione di documenti informatici

Nel caso in cui pervengano erroneamente sulle caselle di posta istituzionali dell'AOO, documenti indirizzati ad altre amministrazioni, aziende, associazioni o privati, l'operatore rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore – non di competenza di questa AOO" e non procede alla protocollazione.

In caso di messaggi ricevuti in interoperabilità è possibile rifiutare il messaggio tramite l'applicazione di gestione dei flussi documentali indicando la medesima motivazione di cui sopra.

5.1.2 Flusso dei documenti in uscita



5.1.2.1 Documenti analogici in uscita

Gli operatori delle UOP eseguono le verifiche di conformità della documentazione cartacea ricevuta dai Servizi Aziendali (per essere spedita) agli standard formali, ovvero, verifica:

- che siano indicati correttamente il mittente e il destinatario
- che il documento sia sottoscritto
- la presenza di allegati se dichiarati
- che siano compilate le ricevute di ritorno (per le raccomandate A.R.)
- che sia allegata la busta personalizzata con logo aziendale, completa di indirizzo del destinatario
- che il layout del documento sottoscritto sia conforme all'immagine coordinata dell'Azienda.

In caso contrario il documento è rispedito al Servizio aziendale di provenienza con le osservazioni del caso.

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dalle UOP.

Qualora i destinatari siano più di uno può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari è allegato alla registrazione di protocollo.

La documentazione da inviare via fax deve essere necessariamente protocollata prima della trasmissione in quanto ad ogni trasmissione deve essere in qualsiasi momento abbinato un numero di protocollo generale.

Gli operatori delle UOP non possono protocollare, successivamente, una lettera che è già stata inviata per fax.

Gli operatori delle UOP non devono acquisire nella scheda di protocollo né l'eventuale copertina di trasmissione né la ricevuta di trasmissione di fax.

5.1.2.2 Documenti informatici in uscita

Tutti i documenti in uscita che devono essere trasmessi per posta elettronica certificata o per posta elettronica tradizionale sono inviati dalle UOP (attraverso le caselle di posta elettronica istituzionali protocollo@dsu.toscana.it o dsutoscana@postacert.toscana.it) a meno che il servizio mittente non chieda espressamente di procedere autonomamente all'invio. In questo caso l'operatore della UOP ne dà menzione nel campo "Annotazioni" della scheda di protocollo.

L'indirizzo di posta elettronica dei destinatari viene registrato automaticamente dall'applicativo una volta effettuato l'invio.

L'operatore della UOP provvede a verificare l'avvenuta consegna dei documenti spediti per posta elettronica certificata e per posta elettronica tradizionale e in caso di mancata consegna (ad esempio per indirizzo non corretto, ~~o~~ per dimensioni del messaggio che eccede il limite previsto dal gestore, per casella del destinatario "piena") ne dà notizia al Servizio interessato.

I Servizi aziendali hanno la possibilità di ricercare gli indirizzi corretti delle caselle di posta elettronica certificata sui siti:

https://www.indicepa.gov.it/ipa-portale/consultazione/domicilio-digitale/ricerca-domicili-digitali-ente

(per le amministrazioni pubbliche)

https://www.inipec.gov.it/cerca-pec

(per professionisti e imprese)

I documenti protocollati indirizzati ad Enti, Gestori di Pubblici Servizi, Imprese e Professionisti **devono essere obbligatoriamente trasmessi tramite PEC** (l'invio per email può essere al limite aggiuntivo ma non sostitutivo all'invio per PEC).

Le ricevute di avvenuta accettazione e consegna (nonché eventuali messaggi di errori di consegna) sono acquisite automaticamente nella scheda del relativo protocollo.

5.1.3 Registrazione di protocollo, segnatura e smistamento

5.1.3.1 Registrazione di protocollo

Per ogni documento ricevuto o spedito dall'Azienda è effettuata una registrazione con il sistema di gestione informatizzata del protocollo. La registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive (art. 53 del TUDA).

La registrazione di protocollo, per ogni documento ricevuto o spedito, è effettuata mediante la memorizzazione nel sistema delle seguenti informazioni:

- il numero di protocollo, assegnato in automatico dal sistema e registrato in forma non modificabile;
- la data di registrazione del protocollo, assegnata in automatico dal sistema e registrata in forma non modificabile;
- il mittente (o i mittenti) per i documenti ricevuti, o in alternativa, destinatario (o destinatari) per i documenti spediti, registrati in forma non modificabile;
- data e numero di protocollo del documento ricevuto, se disponibili;
- la classificazione;
- l'oggetto del documento, registrato in forma non modificabile;
- l'impronta (hash) del documento principale costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
- il numero e la descrizione sintetica degli allegati;
- l'eventuale riferimento della nota del mittente;
- l'indicazione dell'archivio corrente ove è conservato il documento.

5.1.3.2 Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente, non modificabile, delle informazioni riguardanti la registrazione di protocollo. Essa consente di individuare

ciascun documento in modo inequivocabile.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale avente entrambe la natura di atto pubblico. Non potranno, quindi, essere effettuate registrazioni di protocollo senza disporre del documento a cui la registrazione si riferisce.

Le informazioni apposte od associate al documento mediante l'operazione di segnatura sono quelle riportate all'art. 55 del TUDA:

- il progressivo di protocollo (composto da n. 7 cifre + anno es. 0000001/22);
- la data di protocollo
- l'identificazione in forma sintetica dell'Azienda (a tal fine viene riportato il codice IPA dell'Azienda).

Inoltre, sono riportate nella segnatura:

- il codice identificativo dell'AOO
- il codice identificativo del registro di protocollo
- il progressivo assoluto di registrazione
- la classificazione del documento

Nei messaggi indirizzati alle AOO afferenti ad altre Pubbliche Amministrazioni, vengono riportate ulteriori informazioni:

- l'oggetto del documento
- il mittente
- il destinatario
- il nome del documento principale costituito dal progressivo assoluto di registrazione + l'estensione del file
- il nome degli eventuali allegati al documento principale
- il domicilio digitale dell'AOODSUTOSCANA
- il domicilio digitale dell'Ente destinatario

5.1.3.3 Smistamento dei documenti

La UOP competente per sede provvede alle operazioni di registrazione, segnatura, classificazione, archiviazione e spedizione del documento.

Lo smistamento dei documenti segue di norma il criterio di "competenza" e di "gerarchia".

Occorre preliminarmente effettuare una precisazione in merito alla spedizione effettuata tramite l'applicativo di gestione dei flussi documentali.

Si distingue tra:

- spedizione con notifica
- spedizione senza notifica (comprendendo in essa anche la visibilità predefinita)

La spedizione con notifica consente al destinatario di visualizzare il documento in evidenza nella cassetta della posta dell'applicativo. Il documento apparirà in neretto. Effettuando il "click" sul medesimo, l'applicativo registrerà la "presa visione" nella storia della relativa scheda di protocollo.

La spedizione senza notifica comporta che la scheda di protocollo sarà visualizzabile solo tramite l'apposita funzionalità di ricerca e non ne sarà data evidenza nella cassetta della posta dell'applicativo.

Esistono soggetti che a seconda del ruolo occupato all'interno dell'Azienda hanno una visibilità più o meno ampia.

Tipologia archivio	**Visibilità completa**
Protocollo generale[2]	RGD, Direttore, UOP
Gestione Atti	RGD, Direttore, UOP, Operatori gestione atti
Verbali Collegio Revisori	RGD, Presidente, Direttore, Dirigenti, UOP, Operatori gestione atti
Verbali Consiglio di Amministrazione	RGD, Presidente, Direttore, UOP
Verbali Accertamenti Studenti	RGD, Direttore, Dirigente AA.GG., Servizio Interventi Monetari, Servizio Interventi FSE e Accertamenti, UOP
Lettere d'ordine/contratto	RGD, Direttore, Dirigenti, Servizio App. e Contratti, UOP
Relate di notifica	Tutti
Repertorio Albo Pretorio	Tutti

Gli operatori delle UOP dopo un attento esame del documento provvedono ad assegnare la visibilità della posta in arrivo, in uscita e interna. Come criterio generale, fermo restando la visibilità del documento assegnata di default come sopra riportato, i documenti in entrata vengono smistati con notifica al/ai destinatario/i, al Dirigente dell'Area di competenza, ai Coordinatori competenti per materia.
I documenti in uscita o interni, oltre agli stessi soggetti previsti per i documenti in entrata, vengono smistati con notifica al redattore del documento e al firmatario.
In caso di smistamento errato o incompleto, è a carico di uno dei destinatari provvedere tempestivamente a segnalare alla UOP la necessità di modificare/integrare lo smistamento (fermo restando la possibilità di provvedere autonomamente alla spedizione con notifica che risulterà nella storia delle attività nella relativa

[2] Il Collegio dei Revisori ha la visibilità completa del solo Titolo VI "Approvvigionamenti, Patrimonio e Sicurezza"

scheda di protocollo).

5.1.4 Acquisizione dei documenti cartacei nella scheda di protocollo

I documenti ricevuti su supporto cartaceo, di formato compatibile con lo scanner collegato alla postazione operatore, dopo le operazioni di registrazione e segnatura protocollo, devono essere acquisiti in formato PDF con l'ausilio dello scanner.

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei

A tal fine è compito dell'operatore della UOP assicurarsi che il documento venga acquisito correttamente, utilizzando le funzionalità presenti nell'applicativo per migliorarne la leggibilità (attraverso la modifica della luminosità/soglia/contrasto nelle opzioni di scansione). E' possibile inoltre adoperare la scansione a colori qualora sia strettamente necessario.

Qualora il documento sia difficilmente leggibile in origine e non vi sia possibilità di contattare il mittente per una nuova trasmissione, l'operatore della UOP è tenuto ad acquisirlo nel migliore dei modi possibili dandone evidenza nelle "annotazioni" della scheda di protocollo.

Qualora il documento sia composto anche da allegati, la scansione dovrà essere effettuata tenendo preferibilmente separati il documento principale (sul quale viene apposta la segnatura di protocollo) dagli allegati.

I documenti in formato elettronico possono essere importati tramite l'apposita funzionalità presente nel sistema di gestione informatica dei documenti. Stessa cosa dicasi per gli allegati.

E' possibile, che esistano registrazioni di protocollo ibride formate da documenti acquisiti tramite scanner e documenti in formato elettronico.

5.2 Tempistica di registrazione dei documenti ed eventuale differimento dei termini di protocollazione

La registrazione di protocollo deve essere effettuata di norma in giornata e, comunque, entro le 24 ore lavorative successive alla ricezione della corrispondenza.

Nei casi in cui per temporaneo ed eccezionale carico di lavoro le operazioni di protocollazione non possano oggettivamente essere effettuate nei termini di cui sopra e qualora dalla mancata registrazione a protocollo del documento nello stesso giorno di arrivo possa venire meno un diritto di terzi il differimento dei termini di registrazione a protocollo può essere autorizzato dal RGD.

Con tale autorizzazione debbono essere indicati:

- la tipologia di documenti da ammettere alla registrazione differita di protocollo;
- le cause che determinano la necessità di procedere al differimento dei termini di registrazione;

- la durata del periodo di differimento, entro il quale tutte le registrazioni di protocollo debbono essere effettuate (massimo 3 giorni lavorativi).

Successivamente, nel procedere alla registrazione di protocollo della documentazione precedentemente timbrata e siglata, l'addetto al protocollo inserisce nel sistema di gestione informatica dei documenti la data di effettivo arrivo del documento che, in tal caso, assume valore legale anche se precedente a quella di protocollo.

5.3 Annullamento di una registrazione di protocollo

È consentito l'annullamento di una registrazione di protocollo.

L'annullamento di una registrazione di protocollo può essere autorizzata unicamente dal RGD o, in caso di assenza o impedimento, dal suo vicario.

Le informazioni annullate rimangono memorizzate nella scheda di protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché gli estremi di autorizzazione all'annullamento del protocollo.

La procedura di annullamento riporta una dicitura in posizione sempre visibile, tale da consentire la lettura di tutte le informazioni originarie.

Nel record di protocollo devono apparire inoltre, in forma ben visibile, anche data e ora dell'annullamento, nonché il nominativo dell'operatore che ha proceduto allo stesso.

Si rammenta che comporta l'annullamento della registrazione di protocollo la presenza di errori nel mittente, nel destinatario e nell'oggetto.

5.4 Registro di emergenza

Qualora non fosse possibile fruire del sistema di gestione informatica dei documenti per una interruzione accidentale o programmata, il RGD autorizza l'apertura del registro di emergenza.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Qualora nel corso di un anno non venga utilizzato il RGD annota sullo stesso il mancato uso.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul protocollo generale.

Al termine dell'emergenza, ad ogni registrazione effettuata sul registro viene attribuito un nuovo numero di protocollo generale, continuando la numerazione raggiunta al momento dell'interruzione del servizio.

A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

Esempio:

Protocollo Generale 0014850/23 = Protocollo: EM0000001/23

Al termine dell'emergenza, le UOP effettueranno l'inserimento dei dati nel sistema di gestione informatica dei

documenti seguendo la numerazione progressiva raggiunta all'inizio dell'emergenza (quindi il primo protocollo avrà il numero successivo all'ultima registrazione effettuata).

Le operazioni da effettuare al ripristino consisteranno, inoltre, nella stampa dell'etichetta e nella scansione dei documenti (se trattasi di documenti cartacei) o nell'import del documento e apposizione della segnatura elettronica (se trattasi di documenti informatici).

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo

Sul registro sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il RGD autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Per ogni giornata di registrazione di emergenza è riportato sul relativo registro il numero totale di operazioni registrate manualmente.

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono gli stessi previsti dal protocollo generale.

Durante il periodo di interruzione del servizio di protocollo informatico generale, il Responsabile ICT provvede a tener informato il RGD sui tempi di ripristino del servizio.

5.5 Documenti esclusi dalla protocollazione

L'art. 53 comma 5 del TUDA stabilisce che *"sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione."*

A tal fine, essendo soggette a registrazione particolare sul sistema di gestione informatica dei documenti, non sono protocollate le seguenti tipologie documentali:

- Deliberazioni del Consiglio di Amministrazione
- Provvedimenti del Direttore

- Determinazioni dei Dirigenti di Area
- Verbali del Collegio dei Revisori
- Verbali di accertamento di veridicità delle autocertificazioni
- Verbali del Consiglio di Amministrazione
- Lettere d'ordine/contratto
- Relate di notifica
- Repertorio Albo Pretorio
- Verbali relativi alla conservazione digitale

Sono altresì esclusi dalla protocollazione:

- fatture attive e passive, mandati, reversali ed in generale tutti i documenti contabili per i quali è prevista la registrazione sul gestionale della contabilità;
- estratti conto bancari e postali ad eccezione degli estratti conto contrattuali relativi all'affrancatrice postale;
- bollettini di conto corrente postale;
- certificazioni e attestazioni esistenti nelle banche dati dell'Agenzia delle Entrate, dell'INPS, dei Comuni e di altre PP.AA. (in merito all'attività di accertamento di veridicità delle dichiarazioni sostitutive di certificazione presentate dai richiedenti i benefici erogati dal Diritto allo Studio Universitario).

5.6 Casistiche particolari

5.6.1 Lettere anonime o prive di firma

Le lettere anonime non vengono immediatamente protocollate ma inoltrate, se contengono informazioni o dati di interesse dell'Azienda, dal RGD al Direttore il quale valuta l'opportunità di dare seguito alle comunicazioni ed individua le eventuali procedure da sviluppare.

I documenti privi di firma o con firma illeggibile, ma riconducibili ad un mittente certo (ente, studio privato, fornitore, ecc..), vengono protocollati ed inoltrati ai Servizi competenti.

5.6.2 Documenti idonei a rivelare lo stato di salute dei dipendenti dell'Azienda

Devono essere osservate cautele particolari nel trattamento dei dati sensibili contenuti nei documenti pervenuti in qualsiasi forma alla UOP e, nello specifico, di quelli idonei a rivelarne lo stato di salute. Tra questi ultimi, può rientrare l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza della contestuale enunciazione della diagnosi.

Il lavoratore assente per malattia è tenuto a consegnare all'Azienda un certificato senza diagnosi, con la sola indicazione dell'inizio e della durata presunta dell'infermità

Qualora, tuttavia, dovessero essere presentati dai lavoratori (o da soggetti delegati) certificati medici, certificati di degenza e dimissioni dalle strutture ospedaliere pubbliche e private, nei quali i dati di prognosi e di diagnosi non siano separati, le UOP sono tenute, per conto del datore di lavoro, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione e l'acquisizione nel protocollo informatico.

Pertanto gli operatori della UOP dovranno oscurare

- l'indicazione del reparto
- l'indicazione della diagnosi
- timbri con evidenza della specializzazione del medico

e in generale tutti quei dati dai quali si possa risalire alla patologia del paziente.

Gli unici dati da lasciare in evidenza sono:

- la struttura sanitaria che rilascia il certificato
- il nominativo del lavoratore
- la prognosi (intendendo per essa il numero dei giorni di riposo prescritti)

5.6.3 Messaggi PEC/PEO incompleti

Qualora pervengano sulla casella di posta elettronica certificata o sulla casella di posta elettronica tradizionale messaggi carenti di allegati (è presente solo il testo del messaggio il quale cita uno o più allegati) le UOP sono tenute a:

- rispondere al mittente: "Il messaggio risulta privo di uno o più allegati, si prega di rinviare per consentire la regolare protocollazione";
- smistare al Servizio competente attraverso la funzione di condivisione della scheda senza procedere alla protocollazione, informando contestualmente il Dirigente di Area e il Coordinatore del Servizio della richiesta di integrazione i quali possono chiedere alle UOP di procedere ugualmente alla protocollazione.

5.6.4 Ricezione di PEC/PEO di messaggi frazionati in più invii

Qualora pervengano sulla casella di posta elettronica certificata o sulla casella di posta elettronica tradizionale messaggi frazionati in più invii (generalmente denominati "invio x di y" le UOP procedono alla creazione di una sola scheda di protocollo allegando al primo messaggio i file .eml corrispondenti agli invii successivi.
Di ciò se ne dà menzione nel campo "annotazioni".

5.6.5 Trasmissione di messaggi di grandi dimensioni

Qualora gli allegati di una scheda di protocollo abbiano una dimensione complessiva superiore al limite massimo definito dal gestore di posta elettronica, le UOP procedono all'invio di più messaggi frazionati, inserendo nel campo "oggetto" del messaggio di posta elettronica "Invio 1 di x", "invio 2 di x" e così via.

5.6.6 Ricezione del medesimo documento tramite differenti canali

In caso di ricezione del medesimo documento tramite canali differenti (es: per PEC e successivamente per

Raccomandata A.R.) fermo restando l'obbligo di procedere ad una sola registrazione di protocollo le UOP, qualora siano a conoscenza della ricezione duplicata, sono tenute a seguire le seguenti indicazioni:

a) se viene registrato prima il documento informatico, il successivo documento analogico verrà comunque archiviato apponendo ad esso la stampa della scheda indici del software di gestione documentale;
b) se viene registrato prima il documento analogico, il successivo documento informatico verrà smistato ai destinatari comunicando ad essi che trattasi del medesimo documento di cui al protocollo "x";
c) se viene registrato un documento tramite PEC, la successiva (o contestuale) eventuale ricezione di un documento tramite PEO seguirà il medesimo trattamento di cui al punto b) ;
d) se viene registrato un documento tramite PEO, la successiva (o contestuale) eventuale ricezione di un documento tramite PEC seguirà il medesimo trattamento di cui al punto c).

Qualora avvenga la protocollazione del medesimo documento pervenuto da canali differenti si procede con l'annullamento del protocollo più recente dandone menzione nel campo "Annotazioni" del software di gestione dei flussi documentali.

5.7 Disposizioni sulle copie analogiche di documenti informatici: il timbro digitale

L'Azienda adotta il "timbro digitale" in tutti quei casi in cui occorra stampare un documento firmato digitalmente e protocollato.

Il timbro digitale consente di mantenere inalterata, anche nel processo di stampa, la validità legale di un documento informatico firmato digitalmente: la versione stampata può essere letta e decodificata tramite uno scanner o con un lettore di codici a barre bidimensionali ed un apposito software di visualizzazione.

Una volta stampato, il documento includerà un codice grafico (QR code) che contiene le informazioni relative al documento informatico e alla firma digitale.

5.8 Registro giornaliero ed annuale di protocollo

L'Azienda ha istituito, ad oggi, un unico registro di protocollo nel quale la numerazione si chiude automaticamente al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

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

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

Alle ore 21:00 di ogni giorno, l'applicativo genera automaticamente un file in formato pdf/a del registro giornaliero di protocollo che viene inviato al sistema di conservazione entro la fine della giornata successiva.

Entro il 31 gennaio dell'anno successivo a quello di riferimento, il RGD esegue la stampa del registro annuale di protocollo (in formato PDF/A), lo sottoscrive digitalmente e appone la marca temporale.

CAPITOLO 6 – DISPOSIZIONI FINALI

6.1 Qualità delle informazioni memorizzate

La gestione informatizzata dei flussi documentali dell'Azienda necessita di particolare attenzione alla qualità delle informazioni associate, in fase di protocollazione, ai documenti interessati al fine di evitare che questi risultino non reperibili o difficilmente rintracciabili.

A tal fine le UOP sono tenute a seguire le indicazioni contenute nel testo "Raccomandazioni di Aurora" predisposte dal Gruppo di lavoro interistituzionale Aurora. Nell'allegato G al presente Manuale se ne riporta una sintesi.

6.2 Entrata in vigore

La revisione 11 del Manuale entra in vigore il 1° giugno 2023 e sostituisce integralmente la revisione 10.

COMMISSO MARCO ALEKSY
2023.04.29 15:24:25
CN=COMMISSO MARCO ALEKSY
C=IT
2.5.4.4=COMMISSO
2.5.4.42=MARCO ALEKSY
RSA/2048 bits