

Linea Guida Sistema di Segnalazione delle Violazioni (Whistleblowing) di Poste Assicura

Emesso da:	Poste Italiane	18/06/2026
Recepito da:	<i>Insurance Operations e Business Support di Poste Vita</i>	25/06/2026
Verificato da:		
Verifica Operativa	<i>Resp. Insurance Operations e Business Support</i>	06/07/2026
Verifica specialistica	<i>Compliance (ambito 231, Sistema di Gestione della Qualità e Anticorruzione) Sicurezza e Governo Outsourcing (ambito Privacy e Sicurezza delle Informazioni) Risorse Umane e Organizzazione</i>	06/07/2026
Verifica specialistica di conformità normativa (*)	<i>Compliance</i>	06/07/2026
Verifica sistemica:	<i>Insurance Operations e Business Support</i>	06/07/2026
Approvato da:	<i>Consiglio di Amministrazione</i>	21/07/2026

(*) Così come rappresentato all'interno del Compliance Risk Model riportato nella Linea Guida Il modello di governo del Rischio di non conformità adottata dalla Compagnia.

VERSIONE	DATA	MODIFICHE
1	23/03/2021	Prima emissione
2	22/11/2021	Aggiornamento non sostanziale al <i>disclaimer</i> di recepimento della Linea Guida di Poste Italiane, al fine di chiarire come sia il Presidente del Comitato Whistleblowing delle singole Società del Gruppo a compiere il previsto reporting verso gli Organi sociali delle società del Gruppo Poste Vita.
3	21/06/2024	Recepimento Linea Guida di Poste Italiane riportante modifiche normative, aggiornamenti organizzativi e di processo anche con riferimento ai ruoli privacy.
4	21/07/2026	Recepimento della Linea Guida di Poste Italiane, aggiornata in adeguamento al nuovo quadro normativo in materia di <i>whistleblowing</i> , con evoluzione dei processi e della <i>governance</i>

1. OBIETTIVO DEL DOCUMENTO

Il presente documento ha l'obiettivo di recepire nelle Società Poste Assicura la “**Linea Guida Sistema di Segnalazione delle Violazioni (Whistleblowing)**” emanata dalla Capogruppo Poste Italiane disciplinando un sistema che consente al personale e/o a soggetti terzi di segnalare fenomeni illeciti, comportamenti sospetti, irregolarità nella conduzione aziendale, fatti o atti che possano costituire violazioni delle norme, interne ed esterne che disciplinano l'attività di Poste Italiane e delle Società del Gruppo, nonché dei principi e delle regole di comportamento contenuti nel Codice Etico del Gruppo Poste Italiane, nella Politica Integrata e nelle previsioni contenute nel Modello 231 di Poste Italiane e delle Società del Gruppo.

In merito a presidi, ruoli e responsabilità identificati nella Linea Guida di Poste Italiane anche con riferimento alle singole Società controllate, si precisa che non sussiste per Poste Assicura l'esigenza di nominare un Responsabile del Sistema di Segnalazione delle Violazioni, in relazione alla normativa applicabile alle stesse. Pertanto, non si prevede di implementare questo ruolo per Poste Assicura.

Con riferimento a quanto previsto al paragrafo 4.5 sulla *Reportistica*, il Presidente del Comitato Whistleblowing di Poste Assicura assicurerà in via diretta i necessari flussi informativi periodici e/o ad evento agli Organi sociali e alle funzioni interessate con riferimento alle segnalazioni ricevute, alle verifiche eventualmente svolte e ai relativi esiti.

2. SISTEMI DI GESTIONE E/O MODELLI ORGANIZZATIVI/NORMATIVE DI RIFERIMENTO

Modello ai sensi del Decreto Legislativo n. 231/2001	X
Modello 262	
Modello Privacy	X
Sistema di Gestione della Qualità (SGQ)	X
Sistema di Gestione Anticorruzione (SGA)	X
Sistema di Gestione per la sicurezza e la tutela della salute sui luoghi di lavoro e Ambiente	
Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)	X
Antitrust	
Normativa di Settore \ Disposizioni da Organi di Vigilanza (es. IVASS)	
Data Quality	
Cooperative Compliance	
Controllo Rete	

3. LINEA GUIDA SISTEMA DI SEGNALAZIONE DELLE VIOLAZIONI (WHISTLEBLOWING) DI POSTE ITALIANE

Linea Guida Sistema di Segnalazione delle Violazioni (Whistleblowing)

Poste Italiane

Redazione	Raffaele Panico	RCG
Verifica	Giuseppe Lasco Paolo Casati Andrea Novelli	Direttore Generale CI BP
Approvazione	Consiglio di Amministrazione	CdA

Il presente documento è stato approvato dal Consiglio di Amministrazione di Poste Italiane S.p.A. in data 18 giugno 2026, su proposta dell'Amministratore Delegato e previo parere del Comitato Controllo e Rischi.

N. Versione	Data di Approvazione	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	04/03/2015	-	-
2.0	22/12/2015	3, 4, 6, 7	Modifica del ruolo del coordinatore (da Resp. RUO a Resp. CI)
3.0	11/10/2016	tutti	Aggiornamento a seguito della introduzione di disposizioni nella Circolare n. 285 del 17 dicembre 2013 e nel Codice di Autodisciplina
4.0	19/04/2018	tutti	Aggiornamento a seguito dell'introduzione del portale whistleblowing e della Legge 179/2017
5.0	5/11/2019	tutti	Aggiornamento a seguito delle modifiche nella composizione del Comitato Whistleblowing
6.0	27/01/2021	tutti	Aggiornamenti organizzativi e di processo

7.0	18/04/2024	tutti	Modifiche normative, aggiornamenti organizzativi e di processo
8.0	18/06/2026	1, 4, 5, 7	Modifiche normative ed aggiornamenti organizzativi

Sommario

Introduzione	6
1 Obiettivi, ambito di applicazione e modalità di recepimento	8
2 Definizioni, abbreviazioni e acronimi	10
3 Principi di riferimento	15
4 Sistema di Segnalazione delle Violazioni	16
4.1 Soggetti Coinvolti	16
4.2 Fattispecie oggetto di segnalazione Whistleblowing e suo contenuto	16
4.2.1 Fattispecie oggetto di segnalazione ordinaria	17
4.3 Processo di Gestione delle Segnalazioni	17
4.3.1 Segnalazione	17
4.3.2 Analisi Preliminare	19
4.3.3 Esame e Valutazione delle Segnalazioni	19
4.3.4 Provvedimenti decisionali collegati alla Segnalazione	22
4.3.5 Archiviazione, conservazione e tracciabilità delle Segnalazioni	23
4.4 Tutele del Segnalante e del Segnalato	24
4.4.1 Tutele del Segnalante	24
4.4.2 Tutele del Segnalato e delle altre persone coinvolte o menzionate nella segnalazione	26
4.5 La reportistica	26
4.6 La formazione aziendale	27
5 Ruoli e Responsabilità	28
5.1 Consiglio di Amministrazione	28
5.2 Responsabile del sistema di Segnalazione delle violazioni	28
5.3 Organo preposto alla ricezione, esame e valutazione delle Segnalazioni	29
5.4 Collegio Sindacale	30
5.5 Organismo di Vigilanza	31
5.6 Funzione di Conformità della Prevenzione della Corruzione	31
5.7 Responsabile del Programma di Trade Compliance	31
6 Responsabilità di aggiornamento	32
7 Riferimenti	33
8 Sistemi di gestione e/o modelli organizzativi/normative di riferimento	36
9 Allegati	37

Documento ad uso interno

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate dal personale aziendale con ordinaria diligenza per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti “ad uso interno” possono circolare liberamente nell’ambito di Poste Italiane ma non sono destinati alla diffusione.

L’eventuale divulgazione esterna può risultare inopportuna rispetto agli interessi aziendali. Pertanto, a tal fine è necessario richiedere un’autorizzazione al responsabile della classificazione.

Introduzione

Poste Italiane S.p.A. si conforma agli interventi legislativi in materia di segnalazione di irregolarità o violazioni della normativa, al fine di consentire la diffusione di comportamenti etici in ambito lavorativo, rafforzare il rispetto delle norme ed il governo societario, nonché tutelare gli investitori e le categorie di soggetti fruitori dei servizi offerti, tramite l'adozione di un sistema di segnalazione delle violazioni (c.d. "Whistleblowing") e di disciplinarne i relativi aspetti di natura organizzativa e procedurale.

In particolare, con il decreto legislativo 10 marzo 2023, n. 24, è stata recepita nell'ordinamento italiano la direttiva UE 2019/1937 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione" (cd. disciplina Whistleblowing).

L'obiettivo della direttiva europea è stabilire norme minime comuni per garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri, sia all'interno di un'organizzazione, sia all'esterno. In casi specifici, è prevista la possibilità di effettuare la segnalazione mediante la divulgazione pubblica¹ attraverso i media.

Il Decreto abroga e modifica la disciplina nazionale previgente², racchiudendo in un unico testo normativo - per il settore pubblico e per il settore privato - il regime di protezione dei soggetti che segnalano condotte illecite poste in essere in violazione non solo di disposizioni europee, ma anche nazionali, purché basate su fondati motivi e lesive dell'interesse pubblico o dell'integrità dell'ente, al fine di garantire il recepimento della direttiva senza arretrare nelle tutele già riconosciute nel nostro ordinamento.

Il quadro regolatorio di riferimento è stato infine completato con le Linee Guida ANAC, adottate con delibera del 12 luglio 2023, recanti procedure per la presentazione e gestione delle segnalazioni esterne, nonché indicazioni e principi di cui enti pubblici e privati possono tener conto per i canali interni.

Il decreto legislativo n. 24/2023, nel recepire le indicazioni della Direttiva europea, ha previsto un sistema diversificato di presentazione delle segnalazioni. I canali di segnalazione possono infatti essere:

- canale interno;
- canale esterno presso ANAC;
- divulgazione pubblica;
- denuncia all'Autorità Giudiziaria.

¹ La divulgazione pubblica costituisce un canale residuale di segnalazione che consente di rendere di dominio pubblico informazioni su violazioni tramite stampa o altri mezzi di diffusione (anche elettronici), attivabile esclusivamente al ricorrere delle condizioni previste dal legislatore ai sensi dell'art. 15 del D.Lgs. 24/2023. In questi casi occorre richiedere alla persona segnalante appositi chiarimenti in merito alle circostanze che hanno condotto alla diffusione delle informazioni per accertare se ricorra o meno una delle condizioni previste dall'art. 15 del menzionato decreto.

² Per effetto delle disposizioni del Decreto sono abrogati: l'art. 54 bis del Decreto legislativo 30 marzo 2001 n. 165, l'art. 6, commi 2 ter e 2 quater, del D. Lgs n. 231/2001, l'art. 3 del D. Lgs. 179/2017. È stato invece modificato l'art. 6 comma 2 bis del D. Lgs n. 231/2001.

Il D. Lgs. n. 24/2023 prevede anche la possibilità di effettuare una segnalazione esterna all'Autorità Nazionale Anticorruzione ("canale esterno"). L'accesso al canale esterno di segnalazione è consentito solo al ricorrere di determinate condizioni espressamente previste dal citato Decreto, di seguito indicate:

- canale interno non attivato o, anche se attivato, non conforme a quanto richiesto dalla legge;
- segnalazione interna che non ha avuto seguito;
- fondati motivi di ritenere che a un'eventuale segnalazione interna non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- in caso di atti o comportamenti ritorsivi, anche solo tentati o minacciati, in conseguenza della segnalazione presentata.

In tale prospettiva, le indicazioni sopra richiamate debbono altresì considerare l'aggiornamento delle Linee Guida adottato dall'ANAC nel 2025, che ne ha ulteriormente chiarito i profili applicativi. In particolare, con la Delibera ANAC n. 478 del 26 novembre 2025³ sono state approvate le nuove Linee Guida in materia di Whistleblowing sui canali interni di segnalazione, che integrano e aggiornano il quadro di indirizzo precedente, recependo gli sviluppi applicativi della disciplina Whistleblowing e fornendo indicazioni operative sulle modalità di gestione dei canali interni.

³ A tal proposito, tale aggiornamento ha previsto anche la pubblicazione della Delibera ANAC n. 479 del 26 novembre 2025 che modifica e integra la Delibera n. 311 del 12 luglio 2023, aggiornando le Linee Guida sulle segnalazioni esterne e armonizzandole con le nuove indicazioni sui canali interni introdotte dalla Delibera n. 478/2025.

1 Obiettivi, ambito di applicazione e modalità di recepimento

Il presente Documento ha l'obiettivo di disciplinare un sistema volto a permettere la segnalazione da parte del personale e/o di soggetti terzi di fenomeni illeciti e comportamenti sospetti, di irregolarità nella conduzione aziendale, di atti o fatti che possano costituire una violazione delle norme, interne ed esterne, che disciplinano l'attività di Poste Italiane S.p.A. e delle Società del Gruppo dei principi e delle regole di comportamento contenuti nel Codice Etico del Gruppo Poste Italiane e nella Politica Integrata nonché delle previsioni contenute nel Modello 231 di Poste Italiane e delle Società del Gruppo. In particolare, il documento ha l'obiettivo di descrivere:

- i ruoli e le responsabilità degli organi e delle funzioni coinvolte nella gestione delle segnalazioni;
- i canali messi a disposizione del segnalante per la denuncia di presunte anomalie o violazioni effettuate da dipendenti, dirigenti, membri degli organi sociali o terzi;
- il perimetro oggettivo e il contenuto della segnalazione;
- i soggetti segnalanti e le forme di tutela nei confronti degli stessi;
- le modalità di gestione della segnalazione e il procedimento che si instaura nel momento in cui viene effettuata una segnalazione;
- le modalità di informazione del segnalante e del segnalato circa gli sviluppi del procedimento.

Inoltre, la presente Linea Guida è tesa a⁴:

- garantire la riservatezza dei dati personali del segnalante, del presunto responsabile della violazione e delle altre persone coinvolte o menzionate nella segnalazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione;
- tutelare adeguatamente il soggetto segnalante contro condotte ritorsive e/o, discriminatorie dirette o indirette per motivi collegati "direttamente o indirettamente" alla segnalazione;
- assicurare per la segnalazione un canale specifico, indipendente da altri canali di segnalazione, autonomo e protetto.

Il Documento si applica

- a Poste Italiane S.p.A., compreso il Patrimonio Bancoposta, e, previo processo di recepimento, a tutte le società sottoposte alla sua attività di direzione e coordinamento (SdG)⁵, coerentemente con gli accordi di servizio in essere. Le SdG ricevono il presente documento e lo recepiscono tempestivamente secondo quanto indicato nella richiesta di recepimento inviata alle stesse.

Il documento è approvato con delibera del Consiglio di Amministrazione di Poste Italiane S.p.A., sentito il CCR, e, al fine di garantirne la massima diffusione, viene inviato ai membri del Consiglio di Amministrazione, ai Responsabili di primo livello organizzativo di Poste Italiane S.p.A. e agli Amministratori Delegati delle Società del Gruppo e viene pubblicato sul sito intranet e Internet aziendale. Poste Italiane S.p.A., inoltre, intende promuovere opportune attività di formazione del

⁴ Anche in conformità a quanto previsto dagli artt. 52-bis e 52 ter del D.lgs. 385/1993 (TUB), dagli artt. 2 undecies e 2 duodocies del D.Lgs. 196/2003 e dal General Data Protection Regulation- Regolamento UE 2016/679.

⁵ Le Società Controllate sono quelle incluse nell'ultimo bilancio consolidato approvato.

proprio personale dipendente in materia di normativa “Whistleblowing” e “Privacy” per assicurare la consapevolezza e la corretta interpretazione del procedimento di segnalazione adottato.

Infine, è prevista un’interlocuzione preventiva⁶, di carattere meramente informativo, con le Organizzazioni Sindacali competenti, interne e/o territoriali, in occasione di aggiornamenti significativi della presente Linea Guida⁷.

⁶ A cura della funzione Risorse Umane e Organizzazione.

⁷ Nello specifico, si tratta di una interlocuzione preventiva che consente di acquisire eventuali osservazioni di parte sindacale sul documento in esame; il parere espresso dai sindacati nell’interlocuzione preventiva, come previsto dalle Linee Guida dell’ANAC, non ha comunque natura vincolante.

Le predette Linee Guida prevedono inoltre che le specifiche modalità di interlocuzione con i rappresentanti sindacali siano rimesse alla discrezionalità dei singoli enti.

2 Definizioni, abbreviazioni e acronimi

Acronimi

Acronimo/abbreviazione	Descrizione
AD	Amministratore Delegato
DG	Direttore Generale
CdA	Consiglio di Amministrazione
PI	Poste Italiane S.p.A.
BP	BancoPosta
BP/RI	BancoPosta/Revisione Interna
BP/RI/PADR	BancoPosta/Revisione Interna/Pianificazione, Analisi a Distanza e Reporting
CI	Controllo Interno
CI/AM	Controllo Interno/Audit Mirati
RUO	Risorse Umane e Organizzazione
AL	Affari Legali
RCG	Risk e Compliance di Gruppo
RCG/FMSI	Risk e Compliance di Gruppo/Fraud Management e Security Intelligence
RCG/P231	Risk e Compliance di Gruppo/Presidio 231
RCG/PSG	Risk e Compliance di Gruppo/Presidio Sistemi di Gestione
RCG/CIG	Risk e Compliance di Gruppo/Compliance Integrata di Gruppo
CCNL	Contratto Collettivo Nazionale di Lavoro personale non dirigente
CCR	Comitato Controllo e Rischi
CS	Collegio Sindacale
CW	Comitato Whistleblowing di Poste Italiane e delle Società del Gruppo
OdV	Organismo di Vigilanza ex D.Lgs. n. 231/01

Modello 231	Modello Organizzativo 231 ai sensi del Decreto Legislativo 8 giugno 2001, n.231 adottato da Poste Italiane e dalle Società del Gruppo
SdG	Società del Gruppo
ST/CW	Segreteria Tecnica Comitato Whistleblowing
Responsabile del Programma Antitrust	Affari Regolamentari e Rapporti con le Authority

Definizioni

Termine	Definizione
Comitato Whistleblowing	Il Comitato Whistleblowing è un comitato interfunzionale costituito da: ▪ un Presidente esterno a Poste Italiane S.p.A., scelto tra personalità di comprovata esperienza e competenza; ▪ i responsabili delle funzioni aziendali CI/AM, RCG/FMSI, RCG/P231 e i responsabili di strutture operanti nell'ambito delle funzioni AL, RUO (membri permanenti); ▪ il responsabile della funzione BP/RI/PADR (membro a chiamata) che interviene solo per le segnalazioni di propria competenza. Il Comitato Whistleblowing assolve anche le funzioni del Comitato Etico
Responsabile del Sistema di segnalazione delle violazioni di Poste Italiane	Il Responsabile del Sistema di segnalazione delle violazioni è il Responsabile della Funzione CI che riferisce al CdA e al CS, mentre per le segnalazioni inerenti al Patrimonio BP, tale informativa è resa dal Responsabile BP/RI.
Responsabile del Sistema di segnalazione delle violazioni delle Società del Gruppo	Il Responsabile del Sistema di segnalazione delle violazioni delle Società del Gruppo nominato dai CdA delle Società del Gruppo ove applicabile
Comitato Whistleblowing SdG	Il Comitato Whistleblowing di ogni singola Società del Gruppo è costituito da:

	▪ un Presidente esterno alla Società del Gruppo, scelto tra personalità di comprovata esperienza e competenza; ▪ il responsabile della funzione di Poste Italiane RCG/P231; ▪ un rappresentante della Società del Gruppo individuato, compatibilmente con la struttura organizzativa di quest'ultima, tra le funzioni non operative. Il Comitato Whistleblowing delle SdG assolve anche le funzioni del Comitato Etico
Segreteria Tecnica CW	La Segreteria Tecnica dei Comitati WB (di PI e delle SdG) è gestita dalla funzione Controllo Interno/Audit Mirati di PI.
Segnalazione/i Whistleblowing	Per la definizione delle segnalazioni considerate come "whistleblowing", si fa riferimento a quanto riportato nel D. Lgs n. 24/2023, all'art. 2, comma 1, lett a) e b). Ai sensi del D. Lgs. 24 del 10 marzo 2023 (art. 1, comma 2), le disposizioni non si applicano: ▪ alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante; ▪ alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali; ▪ alle segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale.
Segnalazione/i ordinaria/e	Le segnalazioni legate a un interesse personale della persona segnalante sono trattate come segnalazioni ordinarie, in quanto, seppur non rientranti nel campo di applicazione della disciplina whistleblowing, possono risultare rilevanti in relazione ai principi del Codice Etico.
Segnalante/i whistleblowing (che godono della protezione in caso di segnalazione)	Soggetto che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo. Il soggetto può appartenere, ad una delle seguenti categorie di seguito riportate:

	▪ lavoratori dipendenti, o persone il cui rapporto di lavoro o collaborazione è cessato (qualunque tipologia contrattuale) di Poste Italiane S.p.A. o di altra Società del Gruppo e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato (es. volontari e tirocinanti retribuiti e non retribuiti); ▪ azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, di Poste Italiane S.p.A. e/o di altre società del Gruppo, anche qualora tali funzioni siano esercitate in via di mero fatto; ▪ soggetti terzi aventi rapporti e relazioni d'affari con Poste Italiane e Società del Gruppo (ad esempio, clienti fornitori, liberi professionisti e consulenti).
Soggetto/i che godono della protezione diverso/i da chi segnala	▪ Facilitatore, persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata. ▪ Persone del medesimo contesto lavorativo del segnalante, che comunque sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado (esistenza di un legame qualificato). ▪ Colleghi di lavoro del segnalante, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente ▪ Enti di proprietà - in via esclusiva o in compartecipazione maggioritaria di terzi - del segnalante. ▪ Enti presso i quali il segnalante, denunciante lavorano. ▪ Enti che operano nel medesimo contesto lavorativo del segnalante.
Segnalato/i	Soggetto/i cui si riferiscono le violazioni oggetto di Segnalazione.
Patrimonio BancoPosta	Il Patrimonio destinato esclusivamente all'esercizio dell'attività di BancoPosta, costituito da Poste Italiane

	S.p.A. ai sensi dell'art. 2, commi 17-octies e ss. del Decreto Legge 29 dicembre 2010 n. 225, convertito con modificazioni dalla Legge 26 febbraio 2011, n. 10.
--	---

3 Principi di riferimento

Le attività disciplinate dal presente documento devono essere svolte nel rispetto delle vigenti disposizioni di legge nonché dei principi e delle regole di comportamento contenuti nel Codice Etico e Politica Integrata del Gruppo Poste Italiane e negli altri strumenti normativi aziendali⁸.

Il presente documento si ispira ai principi generali riportati nella Linea Guida Sistema di Controllo Interno e Gestione Rischi (SCIGR), cui si rimanda per il relativo dettaglio.

Le persone coinvolte nel Sistema di Segnalazione delle Violazioni operano nel rispetto del sistema normativo, organizzativo e dei poteri e delle deleghe interne e sono tenute ad operare in conformità con le normative di legge ed i regolamenti vigenti e nel rispetto dei principi di seguito riportati.

Inoltre, rispetto all'ambito del presente documento, rilevano anche i seguenti principi generali:

GARANZIA DELLA RISERVATEZZA DEI DATI PERSONALI E TUTELA DEL SOGGETTO SEGNALANTE E DEL SEGNALATO – Tutti i soggetti che ricevono, esaminano e valutano le segnalazioni, il responsabile del sistema di segnalazione e ogni altro soggetto coinvolto nel processo di gestione delle segnalazioni, sono tenuti a garantire la dovuta riservatezza sui fatti segnalati, sull'identità del segnalato e del segnalante che in ogni caso è opportunamente tutelato da condotte ritorsive, discriminatorie o comunque sleali.

La tutela si applica anche quando il rapporto giuridico con il Segnalante non è ancora iniziato, se le informazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali, durante il periodo di prova e successivamente allo scioglimento del rapporto giuridico, se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

PROTEZIONE DEL SOGGETTO SEGNALATO DALLE SEGNALAZIONI EFFETTUATE CON DOLO O COLPA GRAVE – Tutti i soggetti, dipendenti di Poste Italiane S.p.A. e delle società del Gruppo sono tenuti al rispetto della dignità, dell'onore e della reputazione di ciascuno. A tal fine, è fatto obbligo al soggetto segnalante dichiarare se ha un interesse privato collegato alla segnalazione. Più in generale, Poste Italiane S.p.A. e le società del Gruppo garantiscono adeguata protezione dalle segnalazioni effettuate con dolo o colpa grave rivelatesi infondate, censurando simili condotte ed informando che le segnalazioni inviate allo scopo di danneggiare o altrimenti recare pregiudizio nonché ogni altra forma di abuso del presente documento sono fonte di responsabilità, in sede disciplinare e nelle altre sedi competenti.

IMPARZIALITÀ, AUTONOMIA E INDIPENDENZA DI GIUDIZIO – Tutti i soggetti che ricevono, esaminano e valutano le segnalazioni sono in possesso di requisiti morali e professionali e assicurano il mantenimento delle necessarie condizioni di indipendenza e la dovuta obiettività, competenza e diligenza nello svolgimento delle loro attività.

⁸ L'inosservanza dei principi contenuti nel presente documento normativo potrà comportare l'applicazione delle misure sanzionatorie contenute nel sistema disciplinare del CCNL.

4 Sistema di Segnalazione delle Violazioni

Con la presente Linea Guida, Poste Italiane definisce un sistema di segnalazione delle violazioni e i relativi aspetti di natura organizzativa e procedurale, in particolare: i soggetti che possono attivare tale sistema, le violazioni oggetto di Segnalazione, i canali per le Segnalazioni, le attività per la gestione, le tutele per il Segnalante ed il Segnalato, la reportistica.

4.1 Soggetti Coinvolti

Ai sensi del quadro normativo e regolatorio vigente e in linea con le best practice, il sistema di segnalazione può essere attivato da tutti i soggetti tutelati dalla normativa whistleblowing, inclusi coloro che abbiano acquisito le informazioni sulle violazioni in fase precontrattuale, durante il periodo di prova o successivamente alla cessazione del rapporto, purché nel contesto lavorativo o ad esso connesso:

In particolare, è Segnalante il soggetto che appartiene ad una delle seguenti categorie:

- lavoratori dipendenti, o persone il cui rapporto di lavoro o di collaborazione è cessato, (qualunque tipologia contrattuale) di Poste Italiane S.p.A. e/o di altre Società del Gruppo compresi i dirigenti o responsabili di Poste Italiane S.p.A. e/o di altre Società del Gruppo, e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato (es. volontari e tirocinanti retribuiti e non retribuiti);
- azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, di Poste Italiane S.p.A. e/o di altre società del Gruppo, anche qualora tali funzioni siano esercitate in via di mero fatto;
- soggetti terzi aventi rapporti e relazioni d'affari con Poste Italiane e con le Società del Gruppo (es. clienti, fornitori, liberi professionisti e consulenti).

Le Segnalazioni possono riguardare i seguenti soggetti:

- dipendenti e/o dirigenti di Poste Italiane S.p.A. e/o di altre Società del Gruppo;
- membri degli organi sociali;
- terzi (ad esempio fornitori, clienti consulenti, collaboratori), che possono determinare in modo diretto o indiretto, un danno economico-patrimoniale e/o di immagine all'Azienda.

4.2 Fattispecie oggetto di segnalazione Whistleblowing e suo contenuto

Fatta salva la definizione normativa di segnalazione considerate come "whistleblowing", di cui all'art. 2, comma 1, lett. a) e b) del D. Lgs. 24/2023, queste ultime, a titolo esemplificativo e non esaustivo, possono riguardare atti o fatti riferibili a:

- violazioni di norme, interne ed esterne⁹, che disciplinano l'attività di Poste Italiane S.p.A. compreso il Patrimonio Bancoposta, e delle Società del Gruppo e/o dei principi e delle

⁹ Si precisa che tra le violazioni di norme esterne devono intendersi ricomprese anche quelle afferenti alle misure restrittive, incluse le sanzioni economiche e finanziarie, adottate dall'Unione europea, nonché agli eventuali provvedimenti nazionali di attuazione o esecuzione delle stesse, come previsto dal D.Lgs. 30 dicembre 2025, n. 211

regole di comportamento contenuti nel Codice Etico e nella Politica integrata del Gruppo Poste Italiane, nonché delle previsioni contenute nel Modello 231 di Poste Italiane e delle Società del Gruppo;

- comportamenti illeciti o fraudolenti, compiuti da dipendenti, dirigenti o responsabili, membri degli organi sociali, o terzi (fornitori, consulenti, collaboratori e società del gruppo), che possano determinare in modo diretto o indiretto, un danno economico-patrimoniale e/o di immagine per l'Azienda;
- violazioni relative alla normativa antitrust e/o comportamenti illeciti con riferimento alla normativa a tutela della concorrenza e del mercato e delle norme a tutela dei consumatori nonché violazioni di quanto previsto negli strumenti normativi aziendali in materia. La violazione segnalabile non può consistere in una mera irregolarità; tuttavia, le irregolarità possono costituire quegli "elementi concreti" (indici sintomatici) tali da far ritenere ragionevolmente al whistleblower che potrebbe essere commessa una delle violazioni previste dal decreto.

Inoltre, le violazioni sopra indicate sono segnalabili tramite il canale informatico dedicato di segnalazione adottato da Poste Italiane S.p.A. e dalle Società del Gruppo. Il canale costituisce, unitamente alla segnalazione orale mediante incontro diretto, l'unico strumento aziendale deputato alla presentazione e gestione di tutte le tipologie di segnalazioni Whistleblowing.

Le informazioni sulle violazioni devono riguardare comportamenti, atti od omissioni di cui il segnalante o il denunciante sia venuto a conoscenza nel contesto lavorativo.

4.2.1 Fattispecie oggetto di segnalazione ordinaria

Le segnalazioni che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse o dell'integrità aziendale), essendo escluse dall'ambito di applicazione del D.Lgs n. 24/2023, non sono considerate segnalazioni whistleblowing; ad ogni modo, le stesse sono trattate come segnalazioni ordinarie, in quanto possono risultare rilevanti in relazione ai principi del Codice Etico.

Quanto sopra, in considerazione del fatto che il Comitato Whistleblowing assolve anche le funzioni di Comitato Etico.

4.3 Processo di Gestione delle Segnalazioni

4.3.1 Segnalazione

Un soggetto Segnalante, qualora abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni indicate al precedente paragrafo 4.2 ha la possibilità di effettuare una Segnalazione al CW di PI o delle SdG utilizzando il canale istituzionale:

(pubblicato in G.U. n. 6 del 9.1.2026), che estende la tutela Whistleblowing alle violazioni delle misure restrittive dell'UE di cui al Capo I-bis del Codice penale.

- “Portale Segnalazioni - Whistleblowing”, accessibile dal sito internet aziendale istituzionale www.posteitaliane.it; o direttamente dal sito istituzionale delle SdG, fornendo in modo chiaro e completo tutti gli elementi utili per effettuare le verifiche e gli accertamenti necessari a valutarne la fondatezza e l’oggettività, indicando, a titolo esemplificativo e non esaustivo:
 - la descrizione dei fatti e riferimenti sul loro svolgimento (es. data, luogo) ogni informazione e/o prova che possa fornire un valido riscontro circa la sussistenza di quanto segnalato;
 - generalità o altri elementi, ove possibile, che consentano di identificare chi ha commesso quanto dichiarato;
 - generalità di eventuali altri soggetti che possano riferire sui fatti oggetto di Segnalazione;
 - eventuali interessi privati collegati alla Segnalazione.

Il segnalante ha la possibilità di allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione.

Ove quanto segnalato non sia adeguatamente circostanziato, si potranno richiedere elementi integrativi al segnalante tramite il canale dedicato.

Le segnalazioni devono essere rese in buona fede e non in forma anonima. Tuttavia, qualora pervengano segnalazioni anonime, al fine di garantirne la rintracciabilità in caso di successiva comunicazione di presunte ritorsioni e attivazione della tutela che il decreto garantisce a fronte di eventuali misure ritorsive, ne è comunque assicurata la registrazione, la tracciabilità e la conservazione della relativa documentazione nei limiti temporali previsti dalla normativa applicabile e nel rispetto dei principi di riservatezza e minimizzazione, sebbene ciò non comporta l’attivazione dell’iter ordinario di valutazione né la trattazione da parte del Comitato Whistleblowing. Ciascuna Società del Gruppo Poste Italiane garantisce la riservatezza dell’identità del segnalante e del contenuto della segnalazione, attraverso l’utilizzo di protocolli sicuri e adotta le più idonee misure di protezione a tutela del Segnalante, del Segnalato e delle altre persone coinvolte o menzionate nella segnalazione, secondo quanto previsto nei paragrafi 4.4.1 e 4.4.2.

In coerenza con quanto sopra indicato, e in linea con il D.Lgs. 24/2023 e le Linee Guida ANAC, che privilegiano l’adozione di una piattaforma dedicata, non vengono trattate segnalazioni rese, con altre modalità (in formato cartaceo) e/o in forma anonima¹⁰. Si evidenzia che, mediante l’utilizzo del Portale - interfaccia unica di Gruppo, il segnalante può selezionare la società del Gruppo Poste Italiane per la quale intende effettuare la segnalazione (il Portale consente inoltre l’“anonimizzazione” del segnalante); tale sistema consente infatti “partizioni” separate e segregate per singola società del Gruppo.

In aggiunta al predetto Portale informatico che resta il canale da privilegiare per l’invio di segnalazioni - è prevista la possibilità di effettuare una segnalazione in forma orale, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. L’incontro diretto è gestito mediante registrazione della sessione¹¹ ovvero, in alternativa, tramite

¹⁰ In ogni caso, il segnalante o il denunciante anonimo, successivamente identificato, che ha comunicato ad ANAC di aver subito ritorsioni può beneficiare della tutela che il decreto garantisce a fronte di misure ritorsive

¹¹ Previo consenso da parte del segnalante.

redazione di apposito verbale. In caso di verbalizzazione, il relativo documento è messo a disposizione della persona segnalante ai fini della verifica del contenuto e dell'eventuale formulazione di osservazioni o rettifiche; successivamente, esso è sottoscritto dalla medesima a conferma di quanto riportato. I canali di segnalazione interna garantiscono la riservatezza, anche tramite il ricorso a strumenti di crittografia, con riferimento all'utilizzo del Portale informatico, assicurando che i dati trattati siano cifrati e che lo strumento consenta un'interlocuzione riservata con la persona segnalante, anche mediante l'utilizzo di un codice identificativo o meccanismi equivalenti. I canali di segnalazione adottati garantiscono la conformità alla normativa in materia di protezione dei dati personali, con particolare riferimento alla tutela della riservatezza

- della persona segnalante;
- del facilitatore;
- della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- del contenuto della segnalazione e della relativa documentazione.

Il sistema di gestione delle segnalazioni è progettato, implementato e aggiornato secondo i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e privacy by default).

4.3.2 Analisi Preliminare

La ST/CW, o il rappresentante della Società del Gruppo per gli ambiti di competenza, analizza in via preliminare le segnalazioni ricevute, effettuando laddove possibile alcune verifiche sui sistemi aziendali per facilitare lo svolgimento delle istruttorie da parte del CW. In presenza di:

- reclami e denunce di disservizi per problematiche operative;
- segnalazioni disguidate¹²;
- phishing;
- esposti generici e inconsistenti;
- frodi esterne evidentemente agite senza il coinvolgimento di personale aziendale.

La ST CW o il rappresentante della Società del Gruppo può proporre al CW l'archiviazione delle segnalazioni qualora queste ultime risultino non rientrare nell'ambito di applicazione del Whistleblowing.

4.3.3 Esame e Valutazione delle Segnalazioni

Il CW, mediante il supporto della ST/CW, ricevute le Segnalazioni attraverso i canali dedicati, effettua le seguenti attività:

- fornisce evidenza alla persona segnalante, tramite il Portale informatico, del ricevimento della segnalazione entro sette giorni dalla data di ricezione;

¹² Tali segnalazioni devono quindi essere reindirizzate a cura del segnalante mediante nuova registrazione a portale sul dominio della società competente, previa specifica comunicazione tramite portale a cura della ST o rappresentante della Società del Gruppo alla società di interesse, che procede pertanto all'archiviazione della stessa.

- analizza la documentazione ricevuta dal Segnalante e la esamina in via preliminare per valutare la sussistenza dei presupposti necessari ad avviare gli ulteriori approfondimenti. In particolare, la valutazione iniziale tiene conto della presenza di un ragionevole presupposto di fondatezza/attendibilità, quanto meno rispetto alla possibilità di poter pervenire a concrete verifiche circa i fatti segnalati, con esclusione di tutti i casi in cui la completa genericità delle Segnalazioni non consente neppure di avviare una verifica indirizzandola verso prospettive concrete, nel qual caso si determinano, implicitamente, i presupposti per l'archiviazione;
- re-indirizza le Segnalazioni gestite in via preliminare e non rientranti nel perimetro definito nella presente Linea Guida, alle Funzioni competenti (es. Uffici Reclami nel caso di reclami dei clienti);
- invia per informativa, tempestivamente la segnalazione alle Funzioni competenti in materia di Compliance e Antiriciclaggio, in caso di segnalazione afferente tematiche di market abuse o violazioni, potenziali o effettive, delle disposizioni in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, omettendo, nel rispetto della privacy, gli altri aspetti non di pertinenza;
- invia per informativa, tempestivamente la segnalazione al Responsabile del Programma Antitrust, in caso di segnalazione afferente violazioni, potenziali o effettive, delle disposizioni in materia di antitrust e di tutela dei consumatori, omettendo, nel rispetto della privacy, gli altri aspetti non di pertinenza;
- nei casi di segnalazioni riguardanti presunte violazioni del Modello 231 e/o del Codice Etico, informa tempestivamente l'OdV, affinché quest'ultimo possa procedere alla valutazione dei fatti e disporre gli accertamenti ritenuti necessari, avvalendosi anche del supporto delle funzioni aziendali di controllo. L'OdV dà comunicazione delle decisioni assunte al Comitato Whistleblowing. L'OdV riceve, inoltre, da parte del Comitato Whistleblowing un flusso informativo periodico sulle complessive segnalazioni gestite, con evidenza delle decisioni assunte.
- analizza i casi di presunte violazioni del Codice Etico e, in qualità di Comitato Etico, preposto alla sensibilizzazione ed osservanza dello stesso Codice, valuta le successive azioni;
- informa direttamente e senza indugio il Responsabile del sistema di segnalazione dei fatti oggetto di Segnalazione, ove rilevanti¹³;
- identifica le funzioni competenti, definite caso per caso in relazione all'oggetto della Segnalazione, da coinvolgere per lo svolgimento delle ulteriori verifiche e conseguenti relative decisioni (cfr. par. 4.3.4);
- valuta le ulteriori opportune azioni da compiere, coerentemente con gli strumenti normativi aziendali vigenti, al fine di stabilire la fondatezza o meno delle Segnalazioni (es. richiedere approfondimenti gestionali, avviare un intervento di audit o di fraud investigation, procedere con l'archiviazione della Segnalazione in caso di evidente e manifesta infondatezza, ecc.) o

¹³. Per segnalazione rilevante/urgente si intende una comunicazione avente ad oggetto eventi incombenti capaci di generare impatti/danni diretti e immediati, perdite o rischi potenziali compresi quelli di compliance e reputazionali derivanti da comportamenti con coinvolgimento anche di soggetti con rilevanti responsabilità organizzative.

richiedere, quando ne sia il caso, l'intervento di Autorità esterne preposte alle indagini e accertamenti che non possono essere svolti in ambito aziendale;

- fornisce evidenza al Segnalante degli sviluppi del procedimento tramite il “Portale Segnalazioni Whistleblowing” con invio automatico di opportune comunicazioni che tengono conto dell'obbligo della confidenzialità delle informazioni ricevute, anche in ottemperanza ad obblighi di legge, che impediscano la divulgazione delle risultanze in ambiti esterni; l'anonimato del segnalante è garantito, in coerenza con quanto descritto nel paragrafo 4.4.1;
- fornisce, all'esito dell'istruttoria, un riscontro alla persona segnalante tramite il “Portale Segnalazioni Whistleblowing”¹⁴;
- informa, nei casi di segnalazioni di presunti atti corruttivi e violazioni delle Politiche Integrate, tempestivamente la Funzione di Conformità alla Prevenzione della Corruzione di Poste Italiane e delle Società del Gruppo (ove designata);
- informa, nei casi di segnalazione di presunte violazioni delle misure restrittive, tempestivamente il Responsabile del Programma di Trade Compliance.

In aggiunta a quanto sopra, Poste Italiane S.p.A. e le Società del Gruppo promuovono l'utilizzo esclusivo dei canali interni ufficialmente predisposti per l'invio delle segnalazioni, sia in forma scritta sia in forma orale, al fine di garantirne una gestione uniforme, tracciabile e conforme alla disciplina in materia di whistleblowing.

Tuttavia, qualora una segnalazione pervenga, anche per errore, tramite canali diversi da quello dedicato, a soggetti interni a Poste Italiane S.p.A. o alle Società del Gruppo non competenti alla gestione del canale informativo – laddove la persona segnalante dichiara espressamente di voler beneficiare delle tutele in materia *whistleblowing* o tale volontà sia desumibile dalla segnalazione - il destinatario provvede a inoltrarla al soggetto competente entro sette giorni dal ricevimento, informandone contestualmente la persona segnalante – ove identificabile - e assicurando, in ogni caso, il rispetto degli obblighi di riservatezza e di tutela dell'identità del segnalante.

L'iter ordinario di gestione e valutazione è attivato esclusivamente con riferimento alle segnalazioni ove il soggetto segnalante è chiaramente identificato¹⁵.

Si fa presente che, ai fini dello svolgimento dell'istruttoria, il CW, mediante il supporto della ST/CW, può avviare un dialogo con il whistleblower, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, sempre tramite il canale a ciò dedicato nelle piattaforme informatiche o anche di persona.

Qualora, nell'ambito dell'attività istruttoria, il CW abbia la necessità di condurre approfondimenti o richiedere documentazione, coinvolgendo anche altre funzioni aziendali, è prevista l'adozione

¹⁴ Con riferimento al “riscontro” da effettuare entro il termine di tre mesi, si evidenzia che lo stesso può consistere nella comunicazione dell'archiviazione, nell'avvio di un'inchiesta interna ed eventualmente nelle relative risultanze, nei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'autorità competente per ulteriori indagini. Tuttavia, occorre precisare che il medesimo riscontro, da rendersi nel termine di tre mesi, può anche essere meramente interlocutorio, giacché possono essere comunicate le informazioni relative a tutte le attività sopra descritte che si intende intraprendere e lo stato di avanzamento dell'istruttoria. In tale ultimo caso, terminata l'istruttoria, gli esiti dovranno comunque essere comunicati alla persona segnalante.

¹⁵ La funzione competente per la gestione della segnalazione whistleblowing – laddove il segnalante è chiaramente identificato – potrà, altresì, fornire allo stesso le indicazioni necessarie per procedere con il corretto utilizzo del canale interno (piattaforma informatica dedicata) per effettuare la segnalazione.

di apposite cautele volte a non rivelare l'identità del segnalante, non solo rispetto al nominativo di quest'ultimo, ma anche rispetto a qualsiasi altra informazione o elemento della segnalazione - ivi inclusa la documentazione - dal cui disvelamento si possa direttamente o indirettamente dedurre l'identità del segnalante

Le Segnalazioni inviate allo scopo di danneggiare o altrimenti recare pregiudizio al Segnalato nonché ogni altra forma di abuso del presente documento sono fonte di responsabilità del Segnalante, in sede disciplinare e nelle altre sedi competenti, in particolar modo se venga accertata la infondatezza di quanto segnalato e la strumentale/ volontaria falsità di accuse, rilievi, censure, ecc.

A tal fine, qualora nel corso delle verifiche la Segnalazione ricevuta si riveli intenzionalmente diffamatoria nonché la Segnalazione si riveli infondata ed effettuata con dolo o colpa grave, in coerenza con quanto sopra descritto, Poste Italiane e le SdG possono applicare opportuni provvedimenti disciplinari.

Al fine di garantire l'indipendenza gerarchico-funzionale e l'imparzialità di giudizio dell'organo deputato alla ricezione, esame e valutazione, nonché la piena collegialità del CW, si prevede che qualora, la segnalazione riguardi uno dei membri del CW o uno dei responsabili delle funzioni facenti parte del CW o un dipendente delle funzioni facenti parte dello stesso, dovranno essere previsti meccanismi di astensione del membro interessato o di sostituzione dello stesso anche mediante la nomina di un soggetto esterno all'azienda¹⁶. Eventuali situazioni di cumulo di incarichi non determinano incompatibilità automatica, ma, qualora con riferimento alla singola segnalazione emergano concreti profili di conflitto di interessi o di possibili compromissione dell'autonomia e imparzialità della valutazione, si attivano meccanismi di astensione e sostituzione previamente disciplinati, idonei ad assicurare la piena terzietà del gestore del canale di segnalazione. Per i dettagli operativi si rinvia ai regolamenti di funzionamento di Poste Italiane e delle singole SdG.

4.3.4 Provvedimenti decisionali collegati alla Segnalazione

I provvedimenti decisionali sono rimessi alle funzioni o agli organi aziendali competenti, di volta in volta sulla base delle responsabilità organizzative attribuite (cfr. par.4.3.3). Le funzioni coinvolte per la definizione dei provvedimenti decisionali saranno diverse dalle funzioni facenti parte del CW.

Per le casistiche che coinvolgono soggetti apicali, il CW ne dà evidenza agli Organi aziendali/sociali competenti¹⁷ assicurando informativa e aggiornamento sugli sviluppi delle iniziative attivate.

¹⁶ Si fa riferimento all'aggiornamento delle Linee Guida ANAC in materia di Whistleblowing, che prevedono l'individuazione di un sostituto idoneo a garantire la continuità della gestione dell'attività in caso di impedimento, assenza o potenziale conflitto del responsabile.

¹⁷ CdA, anche attraverso il CCR, CS e OdV (quest'ultimo per le casistiche rilevanti ai fini "231").

Qualora il Segnalante sia corresponsabile delle violazioni da egli stesso denunciate, il sistema di segnalazione di Poste Italiane e delle Società del Gruppo prevede un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile¹⁸.

4.3.5 Archiviazione, conservazione e tracciabilità delle Segnalazioni

Al fine di garantire la ricostruzione delle diverse fasi del processo, è cura del CW, anche per il tramite della ST, assicurare:

- la tracciabilità delle Segnalazioni e delle relative attività di ricezione, istruttoria e valutazione;
- la conservazione di eventuale documentazione cartacea inerente alle Segnalazioni e le relative attività di verifica gli eventuali provvedimenti decisionali adottati dalle funzioni competenti, nonché i verbali del CW nel Portale Whistleblowing e/o in appositi armadi blindati per la documentazione cartacea;
- la conservazione della documentazione e delle Segnalazioni per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti o successivamente trattati e comunque nel rispetto della vigente normativa in tema di protezione dei dati personali, con termine massimo pari a 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione; concluse le attività di gestione, la documentazione Whistleblowing è cancellata senza ritardo e, comunque, entro il predetto termine massimo;
- che i dati personali manifestamente non utili al trattamento di una specifica segnalazione non siano raccolti o, se raccolti accidentalmente, siano cancellati senza ingiustificato ritardo.

Qualora la documentazione e gli atti relativi alla Segnalazione abbiano dato avvio a procedimenti, tale documentazione deve essere conservata, nei limiti di quanto pertinente e secondo le regole ordinarie applicabili al relativo procedimento, al fine di garantirne la tracciabilità e la gestione. Resta fermo che, ove possibile, essa non deve riportare riferimenti puntuali alla persona segnalante; inoltre, qualora la contestazione disciplinare si fondi in tutto o in parte sulla Segnalazione e l'identità del segnalante sia indispensabile per la difesa dell'incolpato, la Segnalazione è utilizzabile solo con il consenso espresso del segnalante alla rivelazione della propria identità, ai sensi dell'art. 12, comma 5, d.lgs. 24/2023.

Decorso il termine di conservazione previsto dalla normativa whistleblowing, Poste Italiane S.p.A. e le Società del Gruppo provvedono alla cancellazione effettiva delle segnalazioni e della relativa documentazione, non essendo sufficiente la mera anonimizzazione dei dati.

Resta ferma la possibilità di conservare, separatamente, gli atti e i documenti relativi a procedimenti avviati in conseguenza della segnalazione, nei limiti in cui tali atti non contengano riferimenti puntuali all'identità del segnalante, salvo quanto strettamente necessario per legge.

Le funzioni coinvolte nelle attività di riscontro della fondatezza della Segnalazione previste dal presente documento assicurano, ciascuna per quanto di competenza, la tracciabilità dei dati e delle informazioni e provvedono alla conservazione e archiviazione della documentazione prodotta, cartacea e/o elettronica, in modo da consentire la ricostruzione delle diverse fasi del

¹⁸ L'inserimento di tale previsione discende da valutazioni discrezionali, quanto a organizzazione e regolamentazione dei processi aziendali, rientranti nei poteri e nelle prerogative datoriali; mentre, avuto riguardo alle attività afferenti il Patrimonio BancoPosta, essa costituisce recepimento delle indicazioni di Banca d'Italia in materia.

processo stesso sempre nel rispetto della vigente normativa in tema di protezione dei dati personali.

4.4 Tutele del Segnalante e del Segnalato

4.4.1 Tutele del Segnalante

Poste Italiane e le Società del Gruppo, in ottemperanza alla normativa di riferimento ed al fine di favorire la diffusione di una cultura della legalità e di incoraggiare la Segnalazione degli illeciti, assicurano la riservatezza dell'identità e dei dati personali del Segnalante e la confidenzialità delle informazioni contenute nella Segnalazione e ricevute da parte di tutti i soggetti coinvolti nel procedimento (rif. soggetti indicati al par. 2) e inoltre garantiscono che la segnalazione non costituisca di per sé violazione degli obblighi derivanti dal rapporto di lavoro.

In particolare, Poste Italiane e le Società del Gruppo garantiscono che l'identità del Segnalante e qualsiasi altra informazione o documentazione da cui può evincersi, direttamente o indirettamente, tale identità, non possa essere rivelata senza il suo espresso consenso e tutti coloro che sono coinvolti nella gestione della Segnalazione sono tenuti a tutelarne la riservatezza.

L'identità del segnalante non può essere rivelata senza il suo consenso, ad eccezione dei casi previsti dalla normativa vigente.

Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. In tali casi, è dato preventivo avviso alla persona segnalante mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati.

Qualora il soggetto segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione. Resta ferma in ogni caso, sussistendone i presupposti, la facoltà della Società di procedere con la denuncia all'Autorità giudiziaria.

Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale.

Nell'ambito del procedimento dinanzi alla Corte dei Conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge.

Inoltre, il Modello 231 prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi previste, ai sensi dell'art. 6, comma 2, lett. e), del d.lgs. n. 231/2001. Costituisce fonte di responsabilità disciplinare la commissione di condotte che possano compromettere l'efficacia del sistema di Whistleblowing, quali, a titolo esemplificativo, ritorsioni nei confronti della persona segnalante, l'ostacolo, anche solo tentato, alla segnalazione, le violazioni dell'obbligo di riservatezza, la mancata istituzione del canale, la mancata adozione (o l'adozione difforme rispetto alla normativa applicabile) delle procedure, nonché la mancata verifica e analisi delle segnalazioni.

In riferimento al divieto di ritorsioni, è fatto divieto assoluto di porre in essere, anche solo tentare o minacciare, atti o comportamenti ritorsivi nei confronti della persona segnalante e degli altri soggetti tutelati dalla normativa whistleblowing, fermo restando la nullità degli effetti derivanti dagli atti ritorsivi adottati in violazione della disciplina vigente.

Poste Italiane e le Società del Gruppo assicurano la tutela del segnalante contro qualsiasi forma di ritorsione, intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini – in via diretta o indiretta – un danno ingiusto ai soggetti tutelati. La stessa tutela si applica anche nei confronti dei facilitatori e degli altri soggetti assimilati al segnalante (es. colleghi di lavoro). Eventuali comunicazioni su presunte ritorsioni subite potranno essere indirizzate all'ANAC in qualità di Autorità preposta a ricevere dal segnalante e gestire tali segnalazioni.

Poste Italiane e le Società del Gruppo, inoltre, mettono in atto dei meccanismi di follow-up, adottando tutti gli accorgimenti necessari ad evitare che si possa risalire direttamente o indirettamente all'identità del Segnalante e quindi estendendo gli approfondimenti ad una numerosità maggiore di dipendenti applicati in diverse funzioni/strutture, finalizzati a conoscere le evoluzioni delle situazioni lavorative vissute dal Segnalante al fine di dimostrare l'efficacia del sistema di segnalazione delle violazioni, incoraggiarne l'utilizzo e provare l'assenza di azioni discriminatorie o altre forme di ritorsione sul dipendente Segnalante.

Fatte salve le specifiche limitazioni di responsabilità previste dal legislatore, la protezione prevista in caso di ritorsioni non trova applicazione in caso di accertamento con sentenza, anche non definitiva di primo grado nei confronti del segnalante, della responsabilità penale per i reati di calunnia o diffamazione o comunque per i medesimi reati commessi con la denuncia, ovvero della responsabilità civile, per aver riferito informazioni false riportate intenzionalmente con dolo o colpa grave.

Nei casi di accertamento delle dette responsabilità, al soggetto segnalante e denunciante è inoltre applicata una sanzione disciplinare proporzionata alla gravità della condotta posta in essere.

Poste Italiane e le Società del Gruppo, in qualità di Titolari del trattamento, forniscono alle persone segnalanti e alle persone coinvolte nella segnalazione l'Informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016.

4.4.2 Tutele del Segnalato e delle altre persone coinvolte o menzionate nella segnalazione

In conformità con la normativa vigente, Poste Italiane e le Società del Gruppo adottano forme di tutela a garanzia della riservatezza del Segnalante anche per il presunto responsabile della violazione, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge che imponga l'obbligo di comunicare il nominativo del Segnalato (es. richieste dell'Autorità giudiziaria, ecc.).

Poste Italiane e le Società del Gruppo, in qualità di Titolari del trattamento, informano il Segnalato e le altre persone coinvolte e/o comunque menzionate nella segnalazione circa il trattamento dei propri dati personali e della facoltà di esercitare i diritti di cui agli artt. da 15 a 22 del Regolamento (UE) n. 2016/679, nei limiti di quanto previsto dall'art. 2-undecies del D. Lgs. n. 196/2003 e ss.mm.ii. (Codice privacy). A tal fine Poste Italiane e le SdG forniscono agli interessati informativa specifica ai sensi degli artt. 13 e 14 del GDPR. Detti limiti operano qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente che segnala ai sensi dell'istituto del whistleblowing, fermo restando quanto stabilito dal comma 3 del predetto art. 2-undecies, che l'esercizio di tali diritti può essere ritardato, limitato o escluso con comunicazione motivata e resa all'interessato (a meno che la comunicazione possa compromettere la finalità della limitazione). In tali casi, i diritti possono essere esercitati per il tramite del Garante Privacy con le modalità di cui all'art. 160 del Codice privacy medesimo.

Il presente documento lascia impregiudicata la responsabilità penale e disciplinare del Segnalante nell'ipotesi di calunnia o diffamazione ai sensi delle vigenti previsioni di legge, e sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente Linea Guida, quali le Segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente Linea Guida.

4.5 La reportistica

Il CW predispone specifica reportistica periodica e in forma aggregata relativa alla totalità delle Segnalazioni ricevute, alle verifiche eventualmente svolte ed ai relativi esiti.

Le Società del Gruppo inviano, per il reporting annuale, alla ST del CW di Poste Italiane un quadro aggregato delle Segnalazioni ricevute da integrare nella reportistica di PI.

La reportistica prodotta dal CW con riferimento a PI e alle altre Società del Gruppo viene trasmessa al CCR, al CdA per informativa, e, successivamente, ai responsabili delle funzioni facenti parte del CW.

Ai sensi delle disposizioni vigenti, il Responsabile del sistema di segnalazione delle violazioni redige una relazione annuale sul corretto svolgimento del sistema interno di segnalazione che dovrà contenere le seguenti informazioni aggregate:

- esiti della verifica del regolare svolgimento del processo di Segnalazione e del rispetto dei principi generali (riservatezza, tutela dei dati del Segnalante e Segnalato, indipendenza e imparzialità di giudizio) su cui si fonda il sistema di segnalazione;
- executive summary relativo alle Segnalazioni ricevute nell'anno.

Tale relazione annuale, che costituisce parte integrante della reportistica sulla valutazione di idoneità del SCIGR, è presentata al Collegio Sindacale nonché al Consiglio di Amministrazione e sarà resa disponibile in abstract mediante pubblicazione sulla intranet aziendale e sul sito internet.

4.6 La formazione aziendale

Al fine di garantire l'effettiva operatività e solidità del sistema di Whistleblowing, Poste Italiane e le Società del Gruppo promuovono attività strutturate di informazione e formazione rivolte ai diversi stakeholder aziendali. La formazione rappresenta un presidio essenziale per consolidare la cultura della compliance, favorire la conoscenza dei canali disponibili e assicurare una gestione corretta, responsabile e conforme delle segnalazioni.

È previsto lo svolgimento di iniziative di informazione e formazione periodica con contenuti riconducibili anche alla materia Whistleblowing, finalizzate a garantire un utilizzo consapevole del canale e una gestione corretta delle segnalazioni, a tutela della persona segnalante e dell'organizzazione. Le attività formative sono impostate in modo trasversale e rivolte all'insieme degli stakeholder di Poste Italiane, ivi inclusi i dipendenti e i soggetti coinvolti nella gestione del canale, assicurando la diffusione delle regole di utilizzo, dei presidi di riservatezza e protezione e delle principali responsabilità operative connesse alla trattazione delle segnalazioni.

5 Ruoli e Responsabilità

I ruoli e le responsabilità attribuibili ai diversi soggetti coinvolti nel processo di gestione delle Segnalazioni delle violazioni sono nel seguito identificati.

5.1 Consiglio di Amministrazione

Il Consiglio di Amministrazione, nell'ambito del processo di gestione delle Segnalazioni delle violazioni:

- approva la Linea Guida - Sistema di segnalazione delle violazioni (Whistleblowing) e le successive modifiche necessarie per eventuali adeguamenti normativi, su proposta dell'AD e previo parere del CCR (nelle società ove presente);
- nomina il Responsabile del Sistema di segnalazione;
- è informato direttamente e senza indugio dal Responsabile del Sistema di segnalazione dei fatti oggetto di Segnalazione, ove rilevanti¹⁹ ;
- riceve e approva la relazione annuale sul corretto funzionamento del Sistema di segnalazione redatta dal Responsabile del Sistema di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle Segnalazioni ricevute.

5.2 Responsabile del sistema di Segnalazione delle violazioni

Il Responsabile della Funzione Controllo Interno di Poste Italiane o il Responsabile della funzione designata all'interno delle Società del Gruppo (ove applicabile), in virtù delle responsabilità e dei compiti che già presidia all'interno del complessivo sistema dei controlli interni, ricopre il ruolo di Responsabile del Sistema di segnalazione e come tale:

- assicura il corretto svolgimento del processo di Segnalazione delle violazioni;
- riferisce, direttamente e senza indugio, al Collegio Sindacale e al Consiglio di Amministrazione le informazioni oggetto di Segnalazione, ove rilevanti²⁰. Qualora le segnalazioni riguardino attività afferenti il Patrimonio BP, tale informativa sarà resa dal Responsabile di Revisione Interna BP;
- predispone, per Poste Italiane, una relazione annuale sul corretto funzionamento del Sistema interno di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle Segnalazioni ricevute per PI e per il Gruppo; predispone, nel caso delle Società del Gruppo, una relazione annuale sul corretto funzionamento del Sistema interno di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle Segnalazioni ricevute;
- ha l'obbligo di garantire la confidenzialità delle informazioni ricevute, anche in merito all'identità del Segnalante e del Segnalato.

¹⁹ Per segnalazione rilevante si intende una Segnalazione avente ad oggetto eventi incombenti capaci di generare impatti/danni diretti e immediati sul sistema di controllo interno o rischi potenziali, anche reputazionali, per l'Azienda.

²⁰ Cfr. nota nr. 11.

5.3 Organo preposto alla ricezione, esame e valutazione delle Segnalazioni

Il Comitato Whistleblowing di Poste Italiane è l'organo deputato alla ricezione, esame e valutazione delle Segnalazioni. Il CW si compone di:

- un Presidente esterno a Poste Italiane S.p.A., scelto tra personalità di comprovata esperienza e competenza;
- i responsabili delle funzioni aziendali CI/AM, RCG/FMSI, RCG/P231 e i responsabili di strutture operanti nell'ambito delle funzioni AL, RUO (membri permanenti);
- il responsabile della funzione BP/RI/PADR che interviene nei soli casi afferenti alle attività del Patrimonio BP, previste dal Regolamento del Patrimonio BancoPosta, svolte direttamente o per il tramite dell'esercizio dei disciplinari esecutivi stipulati con PI (membro "a chiamata").

L'atto di nomina dei componenti del predetto CW è adottato, in coerenza con i criteri della presente Linea Guida, a cura del Direttore Generale di PI o di un Responsabile di una struttura, incaricato da parte dello stesso Direttore Generale.

Il Comitato delle Società del Gruppo è l'organo deputato alla ricezione, all'esame, alla valutazione e all'esito finale delle Segnalazioni. Il CW si compone di:

- un Presidente esterno alla Società del Gruppo, scelto tra personalità di comprovata esperienza e competenza;
- il responsabile della funzione di Poste Italiane RCG/P231;
- un rappresentante della Società del Gruppo individuato, compatibilmente con la struttura organizzativa di quest'ultima, tra le funzioni non operative.

L'atto di nomina dei componenti del CW delle SdG è adottato, in coerenza con i criteri della presente Linea Guida, a cura dell'Amministratore Delegato della Società interessata.

Nell'ambito del CW, il Presidente ha funzioni di coordinamento del CW stesso. Per tale attività, il Presidente è supportato dalla Funzione CI che svolge il ruolo di Segreteria Tecnica del CW.

Il CW si dota inoltre di un Regolamento al fine di disciplinare le modalità di funzionamento.

Il CW con il supporto della ST/CW o del rappresentante della Società del Gruppo è incaricato di gestire le Segnalazioni oggetto della presente Linea Guida e nello specifico:

- esegue tutte le attività istruttorie compresa la verifica dell'esistenza dei presupposti e/o il re-indirizzamento di Segnalazioni non di pertinenza, non gestite in via preliminare;
- valuta le verifiche da compiere, le funzioni da coinvolgere nelle analisi o l'eventuale archiviazione ed effettua i necessari approfondimenti;
- garantisce la confidenzialità delle informazioni ricevute, anche in merito all'identità del Segnalante;
- predispone reportistica periodica riguardante le Segnalazioni ricevute.

Per il dettaglio delle attività svolte dal CW si rinvia al paragrafo 4.3.2.

Al fine di rispettare il dettato normativo-regolatorio circa l'indipendenza gerarchico-funzionale, intesa come capacità di gestire la segnalazione senza interferenze e in autonomia operativa e valutativa e l'imparzialità di giudizio, intesa come conduzione neutrale ed equidistante rispetto

alle parti coinvolte e scevra da condizionamenti o favoritismi, dell'organo deputato alla ricezione, esame e valutazione, Poste Italiane si è dotata di canali alternativi in modo da assicurare che tale soggetto non sia gerarchicamente e funzionalmente subordinato al Segnalato, non sia esso stesso il presunto responsabile della violazione e non abbia un potenziale interesse correlato alla Segnalazione (per il relativo dettaglio si rinvia al paragrafo 4.3.2). In tale ambito, il gestore opera in piena autonomia operativa e valutativa e gli organi di indirizzo non esercitano alcun potere di supervisione, influenza o condizionamento sulla gestione delle segnalazioni.

I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati da Poste Italiane S.p.A. e da ciascuna SdG in qualità di Titolari del trattamento rispetto alle segnalazioni di propria competenza, e, in quanto tali, ciascun Titolare è tenuto al rispetto della normativa in materia di protezione dei dati personali.

In considerazione delle attività svolte dalla Segreteria Tecnica dei Comitati WB (di PI e delle SdG) operante nell'ambito della funzione Controllo Interno di Poste Italiane S.p.A., quest'ultima assume il ruolo di Responsabile del trattamento per conto di ciascuna SdG e tale ruolo è regolato con atto separato, da parte di ciascuna di esse, ai sensi dell'art. 28 Regolamento UE 679/2016²¹.

Le Istruzioni relative ai trattamenti dei dati personali, da parte di ciascun Titolare del trattamento, dedicate ai componenti del CW e al personale operante nell'ambito della ST sono allegate alla presente LG; con la presa visione e sottoscrizione della presente LG e del relativo allegato "Atto di autorizzazione al trattamento dei dati personali ai sensi del regolamento UE 2016/679 ("Regolamento") e del decreto legislativo n. 196 del 30 giugno 2003 e successive integrazioni e modifiche ("Codice Privacy)", tali soggetti dichiarano di prendere atto delle istruzioni impartite dal Titolare del trattamento²².

5.4 Collegio Sindacale

L'organo con funzione di controllo vigila sull'osservanza delle norme di legge, regolamentari e statutarie, sulla corretta amministrazione, sull'adeguatezza degli assetti organizzativi e contabili di PI/SdG e sul sistema di controllo interno.

L'organo con funzione di controllo è informato direttamente e senza indugio dal Responsabile del Sistema di segnalazione²³ dei fatti oggetto di Segnalazione, ove rilevanti²⁴; qualora tali fatti riguardino attività afferenti il Patrimonio BP tale informativa sarà resa dal Responsabile di Revisione Interna BP.

L'organo con funzione di controllo, ove ne ricorrano i presupposti, deve informare senza indugio la Banca d'Italia, nei soli casi afferenti le attività del Patrimonio BP, e - ove previsto - altre

²¹ Le SdG utilizzano il "Contratto per il trattamento dei dati personali a norma dell'art. 28 del 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 (General Data Protection Regulation – "GDPR" messo a disposizione da Capogruppo.

²² Ciascuna Società controllata da Poste Italiane, nel recepire la presente Linea Guida, avrà cura di inserire nell'allegato in argomento i propri riferimenti in luogo di quelli di Poste Italiane.

²³ Ove il Responsabile del sistema di segnalazioni non è designato, l'organo con funzione di controllo è informato direttamente dal CW

²⁴ Cfr. nota nr. 12.

Autorità di Vigilanza in merito ad atti o fatti di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una irregolarità nella gestione ovvero una violazione della normativa.

L'organo con funzione di controllo delle Società del Gruppo, ove ne ricorrano i presupposti, deve informare senza indugio le Autorità di Vigilanza di riferimento in merito ad atti o fatti di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una irregolarità nella gestione ovvero una violazione della normativa.

5.5 Organismo di Vigilanza

L'Organismo di Vigilanza vigila sul funzionamento e sull'osservanza del Modello 231 aziendale.

Nei casi di segnalazioni riguardanti presunte violazioni del Modello 231 e/o del Codice Etico, il Comitato Whistleblowing informa tempestivamente l'OdV, affinché quest'ultimo possa procedere alla valutazione dei fatti e disporre gli accertamenti ritenuti necessari, avvalendosi anche del supporto delle funzioni aziendali di controllo di Poste Italiane e delle singole SdG. L'OdV dà comunicazione delle decisioni assunte al Comitato Whistleblowing di riferimento.

L'OdV riceve, inoltre, da parte del Comitato Whistleblowing un flusso informativo periodico sulle complessive segnalazioni gestite, con evidenza delle decisioni assunte.

5.6 Funzione di Conformità della Prevenzione della Corruzione

Il Responsabile della Funzione di Conformità della Prevenzione della Corruzione (ove individuata) viene informato tempestivamente dal Comitato Whistleblowing di segnalazioni e fatti riconducibili a potenziali eventi corruttivi e di violazioni della Politica Integrata, ricevendo aggiornamenti sulle decisioni assunte e/o sui successivi sviluppi.

5.7 Responsabile del Programma di Trade Compliance

Il Responsabile del Programma di Trade Compliance²⁵, individuato nella Funzione RCG, che si avvale al proprio interno della Funzione Compliance Integrata di Gruppo, viene informato tempestivamente dal Comitato Whistleblowing di segnalazioni e fatti riconducibili a presunte e/o accertate violazioni della normativa in materia di Trade Compliance (incluse le violazioni in materia di misure restrittive), ricevendo aggiornamenti sulle decisioni assunte e/o sui successivi sviluppi.

²⁵ Sistema di disposizioni e responsabilità finalizzato alla realizzazione di un adeguato controllo delle attività a rischio in materia di Trade Compliance e volto ad assicurare, mediante l'attuazione dei comportamenti e delle attività ivi previsti, il rispetto della normativa applicabile.

6 Responsabilità di aggiornamento

La Funzione responsabile del documento, che ne assicura la redazione, l'aggiornamento e la divulgazione è la funzione RCG.

Le Funzioni coinvolte nelle attività disciplinate dal presente documento sono responsabili della rilevazione e della segnalazione alla Funzione RCG degli accadimenti aziendali di carattere operativo che possono comportare la necessità di aggiornamento.

A fronte di modifiche di carattere non sostanziale, quali ad esempio la variazione di denominazione delle funzioni aziendali, aggiornamenti normativi o degli strumenti informatici senza impatti rilevanti sui processi disciplinati, il responsabile della funzione owner del documento aggiorna il documento, non attivando il processo di verifica e approvazione, ma garantendo l'informativa ai responsabili di queste ultime due fasi e ai destinatari del documento stesso.

7 Riferimenti

Il presente documento è definito in coerenza con gli strumenti normativi interni e i riferimenti normativi esterni vigenti applicabili al Gruppo Poste Italiane. In particolare:

Esterni

- R.D. 19 ottobre 1930, n. 1938 – Codice Penale
- D.P.R. 22 settembre 1998, n. 447 – Codice di procedura penale
- D.Lgs. n. 165/01 Norme Generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche
- D.Lgs. n. 231/01 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art.11 della legge 29 settembre 2000, n. 300" del 08/06/2011 e successive modifiche e integrazioni
- D.Lgs. n. 196/2003 Codice in materia di protezione dei dati personali e s.m.i.
- General Data Protection Regulation- Regolamento UE 2016/679 adottato con D.Lgs. n. 101 del 10/08/2018
- D.Lgs. n. 231 del 21 novembre 2007 e s.m.i. - Prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo
- Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo agli abusi di mercato
- D. Lgs. n. 90/2017, recante attuazione della Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminosi e di finanziamento del terrorismo ("IV Direttiva Antiriciclaggio")
- Segnalazione del Garante per la Protezione dei Dati Personali al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale - 10 dicembre 2009 v. doc. Web n.1693019
- Direttiva 2013/36/UE del 26 giugno 2013 (Capital Requirements Directive– CRD IV)
- D.Lgs n.24/2023 riguardante "la protezione delle persone che segnalano violazioni del diritto dell'Unione" (cd. disciplina whistleblowing).
- D.Lgs n.72/2015 Accesso alle attività degli enti creditizi e sulle imprese di investimento e vigilanza prudenziale
- D.Lgs. n. 385/1993 Testo Unico Bancario
- D.Lgs. n. 58/1998 Testo Unico Finanza

- Circolare Banca d'Italia n. 285/2013 – “Disposizioni di Vigilanza per le banche”, con riferimento alle attività afferenti il Patrimonio BancoPosta
- D.Lgs. n. 68 del 21 maggio 2018 “Codice delle Assicurazioni Private”
- D. Lgs. 30 dicembre 2025, n. 211 - “Attuazione della direttiva 2024/1226/UE del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673”
- Codice di Corporate Governance (ultimo aggiornamento del 2020)
- Legge 9 gennaio 2019 n. 3, G.U 16/01/2019 “Misure per il contrasto dei reati contro la pubblica amministrazione, nonché' in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici”.
- Trattato sul Funzionamento dell'Unione Europea - Parte terza: politiche dell'unione e azioni interne – Titolo VII, Capo 1, Sezione 1, Articoli 101 e 102
- Regolamento (CE) n. 139/2004 del Consiglio, del 20 gennaio 2004, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni")
- Legge 10 ottobre 1990, n. 287 - Norme per la tutela della concorrenza e del mercato
- Decreto Legislativo 6 settembre 2005, n. 206 - Codice del consumo
- Delibera AGCM 22 ottobre 2014, n.25152 - Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della legge n. 287/90
- Delibera n. 301 del 12 luglio 2023 dell'ANAC di emanazione del Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio in materia di whistleblowing.
- Delibera n. 311 del 12 luglio 2023 dell'ANAC - Linee Guida in materia di protezione delle persone che segnalano violazioni e procedure per la presentazione e gestione delle segnalazioni esterne
- Delibera n. 478 del 26 novembre 2025 dell'ANAC - Linee Guida n. 1/2025 in materia di Whistleblowing sui canali interni di segnalazione
- Delibera n. 479 del 26 novembre 2025 dell'ANAC - Modifica e integrazione della Delibera n. 311/2023 sulle Linee Guida in materia di segnalazioni esterne
- Provvedimento AGCM 25 settembre 2018, n. 27356 - Linee Guida sulla Compliance Antitrust
- CCNL per i Dirigenti di Aziende produttrici di Beni e Servizi.

Interni

- Politiche di Sostenibilità citate nella Relazione Finanziaria Annuale vigente

- Codice Etico del Gruppo Poste Italiane
- Modello Organizzativo, Gestione e Controllo di Poste Italiane S.p.A. ai sensi del D.Lgs. n. 231/2001 - "Responsabilità Amministrativa della Società"
- Politica integrata del Gruppo Poste Italiane
- Linea Guida Sistema Normativo Aziendale
- Procedura Gestione Documenti
- Compendio dei poteri di Poste Italiane
- CCNL per il personale non dirigente di Poste Italiane
- Accordi con OO.SS relativi ai temi in argomento
- Linea Guida - Sistema di Controllo Interno e Gestione Rischi (SCI GR)
- Regolamento del Patrimonio BancoPosta
- Linea Guida per la definizione del Risk Appetite Framework e la valutazione delle Operazioni di Maggior Rilievo per il patrimonio BancoPosta
- Linea Guida per la definizione ed il monitoraggio del "Risk Appetite Framework" del Gruppo Poste Italiane
- Linee Guida Prevenzione e Gestione degli eventi illeciti
- Linea Guida "Flussi informativi 231 all'Organismo di Vigilanza di Poste Italiane"
- Linea Guida di compliance per la tutela della concorrenza e del consumatore
- Linea Guida per la Gestione dei Diritti dell'Interessato
- Istruzione Operativa 'Istruttoria della documentazione in autorizzazione al Direttore Generale'
- Linea Guida Disciplina di Gruppo in materia di import-export, programmi di sanzioni e misure restrittive
- Linea Guida Privacy by design and by default

8 Sistemi di gestione e/o modelli organizzativi/normative di riferimento

Modello ai sensi del Decreto Legislativo n. 231/2001	☒
Modello 262	☐
Sistema di Gestione e Controllo del Rischio Fiscale (SGCRF)	☐
Modello Organizzativo Sistema di Controllo Interno sull'Informativa di Sostenibilità (SCIIS)	☐
Modello Privacy	☒
Sistema di Gestione per la Qualità (SGQ)	☒
Sistema di Gestione per la sicurezza delle informazioni (SGSI)	☒
Sistema di Gestione Ambientale (EMS)	☐
Sistema di Gestione per la sicurezza e la tutela della salute sui luoghi di lavoro (SGSL)	☐
Sistema di Gestione Anticorruzione (SGA)	☒
Sistema di Gestione dell'energia consumata per usi propri (EnMS)	☐
Gestione dei Servizi Informatici (ITSM)	☐
Sistema di Gestione della Compliance (CMS)	☒
Normativa di Settore/Disposizioni da Organi di Vigilanza (es: normative bancarie, finanziarie, assicurative, postale...)	☐
Patrimonio BancoPosta	☒

9 Allegati

Codice Documento	Nome
AL_GOV_WHISL_01	Allegato Autorizzazione al Trattamento dei Dati Personali

**** QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO ****

Allegato

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI (AI SENSI DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. N. 196 DEL 30 GIUGNO 2003 E S.M.I.)

Poste Assicura

Uso Interno

N. Versione	Data di Approvazione	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	23/07/2024	-	
2.0	21/07/2026	-	Aggiornamento dell'allegato conseguente alla revisione della Linea Guida di riferimento, senza modifiche al relativo contenuto

Documento ad uso interno

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate dal personale aziendale con ordinaria diligenza per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti "ad uso interno" possono circolare liberamente nell'ambito di Poste Assicura ma non sono destinati alla diffusione.

L'eventuale divulgazione esterna può risultare inopportuna rispetto agli interessi aziendali. Pertanto, a tal fine è necessario richiedere un'autorizzazione al responsabile della classificazione.

Uso Interno

Atto di autorizzazione al trattamento dei dati personali ai sensi del regolamento UE 2016/679 ("Regolamento") e del decreto legislativo n. 196 del 30 giugno 2003 e successive integrazioni e modifiche ("Codice Privacy")

Con il presente atto, i componenti del Comitato Whistleblowing (CW), nell'ambito dei compiti svolti per la Società Poste Assicura S.p.A., con sede legale in Roma, Viale Europa 190, (di seguito la "Società"), considerato che:

- ai sensi degli artt. 29 e 32, par. 4 GDPR, chiunque *"abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento"*, salvo che lo richieda il diritto dell'Unione o degli stati membri.
- l'art. 2-quaterdecies del Decreto Legislativo 30 giugno 2003, n. 196 stabilisce che *"il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità"*;

sono autorizzati al trattamento dati (Incaricati) da parte della stessa Società, in qualità di Titolare del trattamento, ai sensi e per gli effetti dell'art. 29 del Regolamento UE 2016/679 e dell'art. 2-quaterdecies del D.lgs. n. 196/2003, come modificato dal D.Lgs. 101/2018.

Si ricorda che il GDPR prevede le seguenti categorie di dati personali:

Dati Particolari: riguardanti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Nella categoria sopra citata sono ricompresi:

- **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **Dati biometrici:** i dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **Dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative allo stato di salute.

Dati relativi a condanne penali e reati o a connesse misure di sicurezza:

per il trattamento di tali dati, oltre ai presupposti dell'articolo 6, paragrafo 1 GDPR, occorre tenere conto di quanto stabilito dall'art. 10 GDPR, secondo il quale il trattamento deve avvenire esclusivamente sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Il Regolamento si applica sia ad operazioni di trattamento svolte con l'ausilio di mezzi elettronici o comunque automatizzati, sia a quelle svolte su supporto cartaceo.

Nel trattamento dei dati oggetto della presente autorizzazione, ci si dovrà attenere alle istruzioni allegate che, in conformità all'art. 5 del Regolamento UE 2016/679, sono finalizzate a garantire l'attuazione dei principi applicabili al trattamento dei dati personali, con particolare riguardo all'adequatezza e alla pertinenza dei dati rispetto alle finalità del trattamento.

Uso Interno

Il presente atto viene sottoposto alla sottoscrizione da parte delle persone autorizzate per presa visione e conoscenza delle istruzioni impartite. Si informa, infine, che il Regolamento (UE) 2016/679 in materia di protezione dei dati personali è consultabile sulla intranet aziendale della Società – ove è disponibile tutta la documentazione attuativa - e sul sito Internet www.garanteprivacy.it.

Per presa visione

(Nome e Cognome)

Firma

Data

ISTRUZIONI PER IL TRATTAMENTO DI DATI PERSONALI

Ciascun Incaricato è tenuto ad attenersi alle seguenti istruzioni:

1. il Trattamento dei dati personali deve essere effettuato esclusivamente per le finalità indicate dall'Azienda, nell'ambito del ruolo assegnato, in modo lecito e secondo correttezza, in modo da garantire, in ogni operazione di trattamento, la massima riservatezza;
2. effettuare la raccolta, l'elaborazione, la registrazione ed in generale il trattamento di dati personali esclusivamente per lo svolgimento del proprio mandato, avendo cura, ove possibile, di verificarne l'esattezza ed effettuare l'eventuale aggiornamento;
3. è fatto obbligo, inoltre, di verificare che i dati utilizzati mediante strumenti elettronici, siano pertinenti, completi, non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati e necessari al raggiungimento dello scopo per cui sono stati raccolti e trattati; in caso contrario, si dovrà provvedere a renderli irreversibilmente anonimi secondo le modalità indicate dalle policy aziendali in materia;
4. è fatto assoluto divieto di conservare le informazioni e i dati personali in archivi e banche dati al di fuori di quelli espressamente autorizzati;
5. è fatto divieto di comunicare o diffondere dati personali di cui gli Incaricati vengano a conoscenza nello svolgimento delle loro mansioni, a soggetti non espressamente autorizzati.

È fatto obbligo, per quanto sopra, di osservare le procedure di sicurezza di seguito indicate, in modo da ridurre al minimo i rischi di distruzione e perdita, anche accidentale, dei dati di accesso non autorizzato o di trattamento non consentito, nonché garantire l'adozione di misure per la custodia ed il controllo dei dati affidati, in ragione delle mansioni assegnate.

Le informazioni che confluiscono nei report periodici e nella contabilità, sia generale sia analitica, si attengono ai principi di trasparenza, correttezza, completezza e accuratezza.

Gli Incaricati che venissero a conoscenza di omissioni, improprie o errate rappresentazioni delle informazioni e della documentazione a supporto del trattamento di dati personali, riferiscono tali situazioni agli organi preposti alla verifica.

Le informazioni, i dati ed i documenti sono acquisiti, usati o comunicati solo dalle persone autorizzate, in via generale per ruolo aziendale, ovvero specificamente incaricate.

Disposizioni e regole tecniche ed organizzative da osservare nel trattamento in materia di whistleblowing

Il personale autorizzato alla gestione delle segnalazioni deve osservare tutte le disposizioni previste dalla regolamentazione aziendale, con particolare riferimento alle Linee Guida "Sistema di Segnalazione delle Violazioni (Whistleblowing)".

Nello specifico, ciascun incaricato del trattamento accede esclusivamente alle segnalazioni ed ai dati personali necessari ad effettuare il trattamento istruttorio. La segnalazione può avvenire mediante l'utilizzo della piattaforma informatica, che, in conformità a quanto previsto dall' art. 7, co. 1, del d.lgs. n. 24/2023, impiega misure tecniche (crittografia ed accesso con autenticazione informatica a più fattori) a garanzia della riservatezza dei dati personali trattati sia in fase di segnalazione che nelle successive fasi di istruttoria e trasmissione interna dei dati ricevuti nonché ai fini della conservazione degli stessi nella piattaforma.

A tal fine, l'incaricato del trattamento accede alla piattaforma esclusivamente per lo svolgimento delle attività necessarie agli approfondimenti relativi alla segnalazione. Accedendo all'area dedicata, visualizza il modulo di segnalazione privo dell'apposita sezione "Identità" che il segnalante avrà compilato per sottoscrivere la segnalazione. I dati inseriti in questa sezione, utili alla sua identificazione univoca, sono oggetto di oscuramento e quindi non accessibili ai componenti dell'ufficio che si occuperà dell'istruttoria salvo esplicita autorizzazione all'accesso concessa dal supervisore, garante del processo, previa motivata richiesta.

L'incaricato del trattamento procede all'esame e all'assegnazione al personale autorizzato delle segnalazioni acquisite per la successiva trattazione.

Uso Interno

In particolare, nel caso in cui sia palese l'irrelevanza rispetto alla vicenda segnalata di parti della segnalazione, che contengono dati personali, ai sensi dell'art. 13, co. 2, tali parti saranno oggetto di "oscuramento" (manuale ovvero cancellazione logica) e non utilizzati per le successive attività di istruttoria. Nell'eventualità di trasmissione a terzi, la segnalazione dovrà essere epurata da elementi ritenuti non significativi o utili.

Nel trattamento dei dati personali in ambito Whistleblowing, l'incaricato deve osservare i seguenti principi generali:

- Trattare i dati in modo lecito, corretto e trasparente nei confronti dei soggetti interessati («liceità, correttezza e trasparenza»);
- Raccogliere i dati solo al fine di gestire e dare seguito alle segnalazioni, divulgazioni pubbliche o denunce effettuate da parte dei soggetti tutelati dal d.lgs. 24/2023 («limitazione della finalità»);
- Garantire che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). A tal riguardo, il decreto precisa, infatti, che i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati senza indugio;
- Assicurare che i dati siano esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti relativi alla specifica segnalazione, divulgazione pubblica o denuncia che viene gestita («esattezza»);
- Conservare i dati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della specifica segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione («limitazione della conservazione»). Tale termine decorre dalla chiusura del fascicolo sulla segnalazione da parte dell'ufficio aziendalimente competente;
- Effettuare il trattamento in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità, disponibilità e riservatezza»).

Le seguenti misure devono essere garantite in sede di definizione e aggiornamento del sistema di gestione delle segnalazioni, al fine di garantire il corretto trattamento dei dati personali sin dalla progettazione e per impostazione definita (by design e by default):

- Definire un modello di gestione delle segnalazioni in conformità ai principi di protezione dei dati personali. In particolare, tali misure devono fare in modo che non siano resi accessibili, in via automatica senza il tramite del titolare del trattamento o soggetto autorizzato, dati personali a un numero indefinito di soggetti;
- Il ricorso a strumenti di crittografia nell'ambito dei canali interni e del canale esterno di segnalazione è da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al predetto principio di integrità e riservatezza. Le misure di sicurezza adottate devono, comunque, essere periodicamente riesaminate e aggiornate;
- Effettuare, nella fase di progettazione del canale di segnalazione e dunque prima dell'inizio del trattamento:
 - a. la registrazione del trattamento nel Registro dei trattamenti tenuto dall'Azienda ai sensi dell'art. 30 del GDPR, assicurandone l'aggiornamento ed integrando, ove necessario, le informazioni connesse a quelle di acquisizione e gestione delle segnalazioni;
 - b. una valutazione d'impatto sulla protezione dei dati al fine di individuare ed applicare le necessarie misure tecniche per evitare tale rischio;
- Rendere ex ante agli interessati (ad es. segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) un'informativa sul trattamento dei dati personali mediante la pubblicazione di informative privacy (ad esempio tramite sito web, piattaforma, informative brevi in occasione dell'utilizzo degli altri canali previsti dal decreto);
- Garantire il divieto di tracciamento dei canali di segnalazione. Nel caso in cui l'accesso ai canali interni e al canale esterno di segnalazione avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità – sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del segnalante nel momento in cui viene stabilita la connessione a tali canali;

- Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione. Deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante.

Nel caso di trattamenti senza l'ausilio di strumenti elettronici (documenti cartacei)

Gli atti ed i documenti che contengono i dati di natura comune, necessari per lo svolgimento del ruolo degli Incaricati, non devono essere lasciati incustoditi.

In particolare:

- gli atti ed i documenti contenenti dati personali devono essere accuratamente controllati e custoditi per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento;
- i documenti affidati agli incaricati, contenenti eventuali dati particolari o giudiziari relativi ai sinistri, sono controllati e custoditi dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni. I citati documenti devono essere custoditi in luoghi o armadi muniti di apposita serratura;
- l'accesso agli archivi contenenti eventuali dati particolari o relativi a condanne penali o reati è limitato e sottoposto ad accesso controllato a cura della Struttura che svolge tale trattamento. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. In caso di archivi non dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate dal Delegato al Trattamento;
- ciascun Incaricato dovrà accertarsi che non vi sia possibilità da parte di terzi non autorizzati, anche se dipendenti, di accedere a dati personali per i quali è in corso un qualunque trattamento. A tal fine, l'incaricato che abbia accesso ai sistemi informativi, in caso di allontanamento dalla postazione o di temporanea sospensione dell'attività, si accerta di osservare le previste misure di blocco della postazione stessa;
- ogni Incaricato dovrà accertarsi di procedere con la distruzione sicura (es. mediante un tritacarte) di documenti cartacei contenenti dati personali non più necessari;
- è vietato agli Incaricati l'uso di carta che sia stato oggetto di precedenti stampe, potendo detto uso implicare un'impropria diffusione di dati personali.

Nel caso di affidamento a ditte esterne del servizio di distruzione di informazioni cartacee contenenti dati personali, l'Incaricato deve presidiare la corretta esecuzione delle attività (ad es. operazioni di carico e scarico, trasporto, deposito in aree dedicate e protette) al fine di garantire l'osservanza delle misure di sicurezza e verificare la corretta chiusura del processo.

Nel caso di trattamenti con l'ausilio di strumenti elettronici

Nel caso in cui i dati personali siano trattati e conservati con mezzi automatizzati, ciascun Incaricato dovrà:

- rispettare le procedure per l'autenticazione informatica in uso in azienda (password e user id, etc.), effettuando l'accesso alle applicazioni informatiche ed alle banche dati aziendali necessarie allo svolgimento del proprio ruolo;
- in caso di allontanamento dalla postazione di lavoro, adottare le misure in atto a sua disposizione, secondo le istruzioni ricevute, per evitare l'accesso da parte di terzi, anche se dipendenti, ai dati personali trattati sia con l'ausilio di strumenti elettronici che in formato cartaceo;
- osservare le politiche e Linee Guida aziendali in materia di protezione dei dati personali, compresa l'eventuale revisione dell'ambito di trattamento affidato a ciascun Incaricato;
- seguire le "Istruzioni al Personale – Norme per il Corretto Utilizzo delle Risorse Informative Aziendali";
- per il trattamento di dati particolari (dati sensibili) e relativi a condanne penali e reati, l'autorizzazione all'accesso è limitata ai soli dati la cui conoscenza è strettamente necessaria per lo svolgimento delle operazioni di trattamento;
- in particolare, gli eventuali dati particolari e quelli relativi a condanne penali e reati possono essere memorizzati su supporti rimovibili solo in casi eccezionali; in tal caso, i supporti rimovibili devono essere accuratamente custoditi ed utilizzati, al fine di garantire che non vi siano accessi non autorizzati e trattamenti non consentiti (ipotesi di violazione dei dati personali prevista dall'articolo 33, GDPR – Data Breach); inoltre, i medesimi supporti, ~~se non~~ ^{se non} utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati esclusivamente da altri incaricati autorizzati al trattamento degli stessi dati;

- i dati particolari, contenuti in elenchi, registri o banche di dati tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, devono essere, ove possibile, trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi, che permettano di identificare gli interessati solo in caso di necessità;
- accertarsi, in caso di dismissione o di sostituzione del personal computer in uso all'incaricato (ovvero anche solo dell'hard disk ivi contenuto) della distruzione dei dati in formato elettronico;
- rispettare le procedure di custodia delle copie di sicurezza (back-up), nonché le procedure di ripristino della disponibilità dei dati e dei sistemi;
- garantire che l'accesso e l'utilizzo dei sistemi (es. Service Delivery Platform) sia lecito e legittimo e avvenga limitatamente allo svolgimento delle attività strettamente connesse alla mansione dell'Incaricato e nel rispetto dei diritti dell'Interessato.

Sarà cura di ciascun Incaricato:

- mantenere segreta la parola chiave di accesso al sistema informatico, che dovrà essere composta di almeno 8 caratteri alfanumerici, ove il sistema lo consenta;
- non adottare, nella scelta della chiave di accesso, riferimenti personali agevolmente riconducibili a ciascun Incaricato (ad es. nome e data di nascita personali o dei propri familiari ecc.);
- provvedere alla sostituzione della parola chiave con frequenza almeno mensile (nei casi in cui le caratteristiche dell'elaboratore permettano la sostituzione della parola chiave).

È dovere di ciascun incaricato:

- garantire il rispetto di quanto indicato con la lettera di designazione e relative istruzioni e dalla normativa applicabile;
- essere a conoscenza degli obblighi di legge in materia di trattamento di dati personali, confermando altresì di aver compreso integralmente le istruzioni impartite, nonché di conformarsi ad eventuali istruzioni operative che saranno successivamente fornite;
- impegnarsi a mantenere l'obbligo di riservatezza sui dati dei quali verrà a conoscenza nello svolgimento delle mansioni per le quali è stato autorizzato;
- impegnarsi a partecipare alle attività di formazione in materia di trattamento dei dati alle quali sarà invitato.