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

N. Versione	Data di Approvazione	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	23/07/2024	-	

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.

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'adeguatezza e alla pertinenza dei dati rispetto alle finalità del trattamento.

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.

In particolare, nel caso in cui sia palese l'irrilevanza 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 aziendalmente 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 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.