SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

Revisione 0

Indice

Documenti citati

P01	Modello Organizzativo Privacy
	Codice Etico del Gruppo Poste Italiane

Moduli citati

km.001.00	Informativa per il trattamento dei dati personali
Km.002.00	Informativa Privacy dipendenti Kipoint

1 SCOPO E CAMPO DI APPLICAZIONE

1.1 Premessa

La nuova normativa europea sulla protezione dei dati personali (Regolamento (UE) 2016/679, "General Data Protection Regulation" - GDPR), è direttamente applicabile in tutti gli Stati membri dell'Unione Europea, a far data dal 25 maggio 2018. Uno dei principi cardine del GDPR è la responsabilizzazione *("accountability")* di ciascun Titolare del trattamento, il cui compito, tra gli altri, è quello di provvedere a garantire e dimostrare l'attuazione degli opportuni interventi organizzativi e tecnologici, conformemente agli adempimenti previsti dal GDPR ed adottando un approccio risk based.

In particolare, al fine di rispondere adeguatamente ai requisiti prescritti ed evitare il rischio di trattamenti illeciti e delle conseguenti sanzioni, ogni trattamento di dati personali effettuato dal Titolare o per conto del Titolare da parte dei Responsabili delegati al trattamento deve conformarsi alla sopra citata normativa.

I principali requisiti che caratterizzano il contesto normativo descritto riguardano i seguenti principi ed obblighi:

- L'applicazione dei principi di Privacy by Design e Privacy by Default per garantire il presidio del rischio di non conformità alla normativa privacy, con il coinvolgimento del Titolare nelle fasi precedenti alla realizzazione, implementazione o modifica sostanziale di prodotti/servizi che comportano il trattamento di dati personali;
- La predisposizione ed il continuo aggiornamento del Registro delle attività di trattamento;
- L'espletamento di un Data Protection Impact Assessment (DPIA) prima di procedere ad uno o più trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nonché nelle ulteriori casistiche previste dal Regolamento e declinate nella Linea Guida "Metodologia, per la valutazione d'impatto sulla protezione dei dati (DPIA)";
- La nomina del Data Protection Officer, del Responsabile del trattamento, qualora presente, nonché l'incarico delle persone autorizzate al trattamento;
- La definizione e la manutenzione di un catalogo di controlli in materia privacy e del Registro delle attività di trattamento;
- L'applicazione delle misure atte a garantire l'effettivo esercizio, da parte degli Interessati, dei diritti riconosciuti dal Regolamento;
- L'attuazione delle misure tecniche e organizzative opportune, per garantire un livello di sicurezza adeguato al rischio dei trattamenti effettuati, prima dell'avvio degli stessi;
- La garanzia del principio di accountability (responsabilizzazione), che prevede che il Titolare debba essere in grado di dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento;
- La notifica delle violazioni di dati personali all'Autorità di controllo e comunicazione agli Interessati (Data Breach);
- La formazione e la diffusione della cultura privacy

1.2 Obiettivo del documento

La presente Linea Guida è volta a garantire un sistema di gestione dei dati personali per Kipoint che sia uniforme a quello di Capo Gruppo e conforme alle disposizioni del Regolamento Europeo sulla Protezione dei Dati (Regolamento UE 2016/679, "General Data Protection Regulation" — GDPR) e alla normativa italiana vigente.

In particolare, la Linea Guida illustra il modello privacy aziendale, i principi di Privacy by Design e by Default, nonché i principali processi adottati da Kipoint e le relative responsabilità ai fini dell'efficace gestione dei rischi in materia di protezione dei dati personali.

1.3 Ambito di applicazione e modalità di recepimento

La presente Linea Guida si applica a Kipoint. Il presente documento rappresenta la ricezione del documento “Gruppo Poste Italiane - Linea Guida Sistema di gestione della protezione dei dati personali”, adattato ove necessario alle esigenze e peculiarità di business di Kipoint.

1.4 Principi Trasversali

Le persone coinvolte nei macro-processi illustrati nella presente Linea Guida devono operare 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 trasversali di seguito riportati:

TRACCIABILITÀ — deve essere garantita la tracciabilità delle attività e dei documenti inerenti ai processi operativi, e l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati a supporto delle

attività. Tale conservazione della documentazione deve essere assicurata, nel rispetto dei termini di legge, utilizzando, laddove disponibili, i sistemi informativi dedicati.

SEGREGAZIONE DI COMPITI E ATTIVITÀ — deve essere prevista la segregazione di compiti e responsabilità, tra unità organizzative distinte o all'interno delle stesse, al fine di evitare che attività incompatibili risultino concentrate sotto responsabilità comuni. In particolare, deve essere assicurata la segregazione tra le attività operative e quelle di controllo al fine di prevenire e/o attenuare i conflitti di interesse.

CONFORMITÀ ALLE LEGGI E COERENZA CON IL QUADRO NORMATIVO DI RIFERIMENTO GENERALE — deve essere garantito il rispetto delle normative applicabili, in coerenza al quadro di riferimento generale composto a titolo esemplificativo da: Statuto, Codice Etico, sistema organizzativo, sistema di poteri e deleghe, etc.

POTERI AUTORIZZATIVI — gli strumenti normativi devono assicurare specifici livelli autorizzativi e/o di supervisione commisurati alle caratteristiche o alla tipologia delle transazioni.

RISERVATEZZA — fermi restando la trasparenza delle attività poste in essere e gli obblighi di informazione imposti dalle disposizioni vigenti, deve essere assicurata altresì la riservatezza richiesta dalle circostanze per ciascuna notizia/informazione appresa nell'ambito delle funzioni lavorative previste nei processi.

CONFLITTO DI INTERESSI - nei confronti delle controparti devono essere assicurati rapporti improntati ai più alti livelli dell'etica di comportamento e nel rispetto del Codice Etico del Gruppo Poste Italiane, evitando di assumere decisioni e di svolgere attività, in conflitto, anche se solo potenziale con gli interessi dell'Azienda o comunque in contrasto con i propri doveri d'ufficio.

AUTONOMIA SOCIETARIA DELLE CONTROLLATE - è garantita l'autonomia societaria delle controllate per quanto attiene l'istituzione e il mantenimento di un adeguato e funzionante modello Privacy, nel rispetto degli indirizzi di direzione e coordinamento definiti da Capo Gruppo e da KIPOINT.

RESPONSABILIZZAZIONE MANAGEMENT — il Management, nell'ambito delle funzioni ricoperte e nel conseguimento dei correlati obiettivi, garantisce l'applicazione della Linea Guida per le attività di competenza, partecipando attivamente al suo funzionamento.

COERENZA CON OBIETTIVI AZIENDALI — il Modello Privacy contribuisce a una conduzione dell'impresa volta allo sviluppo sostenibile, alla massimizzazione del valore dell'Azienda e coerente con gli obiettivi aziendali.

1.5 Principi Normativi

La normativa di riferimento, alla data di emissione della presente Linea Guida, è il Regolamento (UE) 2016/679 sulla protezione dei dati personali (GDPR) e la normativa italiana vigente.

A tali riferimenti normativi si affiancano i provvedimenti adottati dal Garante per la protezione dei dati personali, per propria diretta iniziativa o in riferimento a istanze, ricorsi, reclami, segnalazioni, richieste di pareri, presentate dai vari stakeholder (es. cittadini, aziende, associazioni) ed ai pareri e raccomandazioni del Gruppo di Lavoro Articolo 29 per la protezione dei dati («WP29»). Quest'ultimo è un organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata, istituito in virtù dell'articolo 29 della Direttiva 95/46/EC e tuttora attivo a seguito dell'entrata in vigore del GDPR e dell'abrogazione della precedente direttiva.

In particolare, il GDPR introduce e specifica i seguenti Principi e Diritti:

ACCOUNTABILITY (RESPONSABILIZZAZIONE): *(articolo 5, paragrafo 2, GDPR)* Il Regolamento Europeo offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di Accountability. Tale principio riguarda il dovere del Titolare del trattamento di adottare misure organizzative e tecniche adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al GDPR.

TRATTAMENTO: *(articolo 5, paragrafo 1, lett. a), GDPR)* Secondo il Regolamento Europeo è necessario che i dati siano trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato.

MINIMIZZAZIONE DEI DATI: *(articolo 5, paragrafo 1, lett. c), GDPR)* I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

ESATTEZZA: *(articolo 5, paragrafo 1, lett. d), GDPR)* Il Regolamento prevede il principio di esattezza, secondo il quale i dati trattati devono essere esatti e, se necessario, aggiornati; inoltre devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

LIMITAZIONE DELLA CONSERVAZIONE: *(articolo 5, paragrafo 1, lett. e), GDPR)* I dati devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione

che siano trattati esclusivamente ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o ai fini statistici.

INTEGRITÀ E RISERVATEZZA: *(articolo 5, paragrafo 1, lett. f), GDPR)* I dati devono essere trattati 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 accidentale.

APPROCCIO RISK BASED: *(articolo 35, GDPR) È* necessario effettuare una valutazione dei rischi inerenti ai trattamenti di dati personali e una valutazione degli impatti per i trattamenti *a* rischio elevato.

PRIVACY BY DESIGN E BY DEFAULT: *(articolo 25, GDPR)* Il trattamento deve essere configurato, sin dalla fase di progettazione, prevedendo le garanzie indispensabili, al fine di tutelare i diritti degli Interessati e i requisiti del Regolamento.

CONSENSO DELL'INTERESSATO: *(articoli 6, 7 e 8, GDPR)* L'Interessato deve manifestare il proprio consenso al trattamento attraverso atto positivo ed inequivocabile, tale da dimostrare l'intenzione libera, specifica e informata.

DIRITTO ALLA PORTABILITÀ: *(articolo 20, GDPR)* Il Titolare deve garantire la trasmissione diretta dei dati ad un altro Titolare, se tecnicamente possibile, senza impedimenti.

INDIPENDENZA DEL DPO (**CONFLITTO DI INTERESSI**): *(articoli 37 e ss., GDPR)* Il DPO, nell'esecuzione dei compiti attribuitigli, è tenuto ad adempiere alle proprie funzioni in maniera indipendente, senza ricevere istruzioni su metodologie, accertamenti e consultazioni. A tal fine, pur potendo rivestire altri ruoli all'interno dell'Organizzazione, tali compiti e funzioni non devono dare adito a conflitti di interesse (ad esempio, ruoli che comportano la definizione di finalità del trattamento di dati personali).

Il presente documento si pone l'obiettivo di definire le linee guida e le regole per la nomina e la gestione dei Responsabili Esterni del Trattamento, con riferimento all'operatività della Kipoint.

Tali linee guida sono dettate allo scopo di garantire una gestione conforme alle disposizioni del Regolamento Europeo sulla Protezione dei Dati (Regolamento UE 2016/679, "General Data Protection Regulation" – GDPR) e della normativa italiana vigente.

1.6 Riferimenti esterni

Le principali fonti normative di riferimento sono rappresentate da:

a. Normativa Italiana vigente;
b. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
c. Codice in materia di protezione dei dati personali – Decreto legislativo 30 giugno 2003, n. 196, "Testo unico sulla privacy" e successive modifiche ed integrazioni;
d. Provvedimenti collegati al Codice Privacy, emessi dall'Autorità Garante in materia di Protezione dei Dati Personali;
e. Linea Guida "Sistema di gestione della protezione dei dati personali" di Poste Italiane
f. Codice Etico di Poste Italiane
g. Procedure, disposizioni di legge e contrattuali relative al processo di risoluzione del Contratto e del relativo atto di nomina del Responsabile del Trattamento

1.7 Abbreviazioni e acronimi

Acronimo	Descrizione
CdA	Consiglio d'Amministrazione
CA	Corporate Affairs in ambito Poste Italiane
TA	Tutela Aziendale in ambito Poste Italiane
DPIA	Data Protection Impact Assessment (Valutazione di impatto sulla protezione dei dati)
DPO	Data Protection Officer (Responsabile Protezione Dati)
GDPR	General Data Protection Regulation
WP29	Working Party 29

1.8 Definizioni

Termine	Definizione
Autorità di controllo	Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR (es. Garante per la Protezione dei Dati Personali per l'Italia).
Autorità di controllo interessata	Autorità di controllo interessata in riferimento alle attività di trattamento di dati personali, in quanto: **a)** il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale Autorità di controllo; **b)** gli Interessati che risiedono nello Stato membro dell'Autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; **c)** un reclamo è stato proposto a tale Autorità di controllo.
Cliente actual	È un cliente che ha già servizi in essere con Kipoint.
Cliente prospect	È un potenziale cliente: un Interessato che non ha servizi in essere con Kipoint
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Data Breach	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Data Protection Officer	Responsabile per la protezione dei dati.
Dato Personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Delegato al trattamento	La persona fisica che tratta dati personali per conto del Titolare del trattamento.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
Gruppo di Lavoro Privacy di SDA	La struttura di coordinamento individuata all'interno del Modello Organizzativo Privacy Kipoint, quale centro di competenza e funzione di supporto al Data Protection Officer di Gruppo per Kipoint nelle attività di gestione della Privacy, supporto alle Funzioni aziendali deputate alla gestione di segnalazioni e nella gestione delle Banche Dati contenenti dati personali e dei relativi trattamenti
Incaricato	Personale autorizzato al trattamento dei dati personali.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Addetto Governance IT	A diretto riporto dell'Amministratore Delegato Kipoint è stata individuata una risorsa, , nell'ambito della struttura Pianificazione Strategica, Segreteria e Assistenza Rete Franchisee, che, con il supporto delle equivalenti funzioni in ambito Capogruppo, ha il compito di gestire e svolgere le seguenti attività: • raccolta e gestione delle istanze relative ai diritti dell'interessato secondo il Capo III del GDPR; • smistamento delle istanze relative ai diritti dell'interessato alle funzioni competenti e follow up; • invio di un riscontro alle istanze avanzate dagli interessati ex articolo 19 GDPR, entro un mese dal ricevimento della richiesta; • reporting dei consensi/variazioni acquisiti/e; • gestione reclami circostanziati, ricorsi, ove l'Interessato intenda far valere gli specifici diritti di cui agli articoli 15 e seguenti GDPR; • monitoraggio e reporting delle istanze avanzate dagli interessati.
Responsabile esterno del Trattamento	Terza parte che effettua il trattamento dei dati personali per conto del Titolare del Trattamento.
Richiedente	Qualsiasi soggetto che avanza un'istanza.
Titolare	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente, o insieme ad altri, determina le finalità e i mezzi del trattamento.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicati a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Trattamento transfrontaliero	Consiste: • nel trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti ubicati in più di uno Stato membro dell'UE, ed effettuato da un Titolare del trattamento o Responsabile del trattamento nell'Unione stabiliti in uno o più Stati membri; • ovvero, nel trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento ed effettuato da un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide, o potrebbe incidere in modo sostanziale, su interessati in più di uno Stato membro.
Working Party 29	Organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'UE, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione UE.

2 LINEE GUIDA

2.1 Governo di Gruppo

Al fine di garantire una gestione della Privacy conforme alle disposizioni del Regolamento Europeo sulla Protezione dei Dati (Regolamento UE 2016/679, "General Data Protection Regulation" — GDPR) e alla normativa italiana vigente, Kipoint si è dotata di un'organizzazione uniforme a livello di Gruppo, declinata nel dettaglio nel Modello Organizzativo Privacy Kipoint.

Di seguito, vengono riportati alcuni aspetti rilevanti previsti nel suddetto documento:

- Definizione di figure aventi ruoli, compiti e responsabilità declinate dettagliatamente nel Modello; in particolare i Delegati al trattamento, devono assicurare:
  - una efficace attuazione delle istruzioni impartite dal Titolare;
  - la verifica e, se dovuta, la valutazione dell'impatto privacy, con il supporto delle funzioni specialistiche e sotto la supervisione del DPO;

- La piena e proattiva collaborazione del personale aziendale, ai fini del rispetto dei principi del GDPR;
- Una efficace pianificazione e gestione del sistema di formazione, che assicuri una elevata consapevolezza anche attraverso la partecipazione programmata agli appositi corsi;

Kipoint attua un sistema di monitoraggio, adeguato e aggiornato in funzione delle esigenze di business, assicurando il miglioramento continuo della gestione della privacy, che include la pianificazione pluriennale e la supervisione delle misure tecniche ed organizzative.

2.2 Privacy by Design and by Default

I principi trasversali di Privacy by Design e Privacy by Default hanno l'obiettivo di definire le logiche di protezione dei dati personali, attraverso l'individuazione dei potenziali rischi di non conformità in materia di privacy e delle conseguenti misure tecnico-organizzative per la riduzione degli stessi sin dalla fase di progettazione e lungo tutto il ciclo di vita del trattamento dei dati, dalla raccolta fino alla cancellazione.

Al fine di garantire un approccio proattivo e di evitare l'insorgenza di lesioni dei diritti e delle libertà degli Interessati, sono previsti i seguenti principi volti ad assicurare l'adozione di adeguate politiche di protezione dei dati:

- Privacy by Design: si sostanzia nell'obbligo, in capo al Titolare del trattamento, anche attraverso i suoi Delegati e Sub Delegati al trattamento, di adottare le misure tecniche e organizzative adeguate per la tutela dei dati personali sin dalla fase di progettazione e lungo tutto il ciclo di vita del trattamento previsto nell'ambito di prodotti e/o servizi di Kipoint e del Gruppo Poste Italiane;
- Privacy by Default: prevede l'impostazione standard e predefinita, dei massimi livelli di protezione dei dati personali, consentendo di default l'accesso alle persone/figure aziendali specificatamente autorizzate al trattamento e il trattamento stesso dei soli dati necessari alla relativa finalità e per un periodo limitato ed opportunamente stabilito (principio di minimizzazione).

2.2.1 Privacy by Design

La Privacy by Design si sostanzia nell'obbligo, in capo al Titolare del trattamento, di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli Interessati, tenendo conto del contesto complessivo, ove il trattamento si colloca e dei rischi per i diritti e le libertà degli Interessati.

Tale attività deve avvenire a monte, prima di procedere al trattamento dei dati, sia in corrispondenza della determinazione dei mezzi del trattamento sia all'atto del trattamento stesso, secondo quanto indicato dall'articolo 25 paragrafo 1 del Regolamento. Pertanto, è richiesta un'analisi preventiva e un impegno applicativo da parte del Titolare, attraverso i suoi Delegati e Sub Delegati, che devono sostanziarsi in una serie di attività specifiche e dimostrabili, quali la valutazione d'impatto privacy.

2.2.2 Privacy by Default

La *Privacy by Default* si sostanzia nell'obbligo in capo al Titolare/Delegato del trattamento di adottare misure tecniche e organizzative adeguate per garantire l'applicazione dei principi di protezione dei dati come impostazione di default. Tale attività ha l'obiettivo di definire le azioni da intraprendere al fine di assicurare che siano trattati solo i dati personali necessari al perseguimento delle specifiche finalità del trattamento.

2.3 Processi di gestione e protezione dei dati personali

In merito alla protezione dei dati personali, sono messi in atto una serie di macro-processi appositamente regolamentati e previsti dal GDPR, meglio descritti di seguito.

2.3.1 Gestione del Registro delle attività di trattamento

Kipoint in qualità di Titolare del trattamento ha l'obbligo di mantenere, mediante il supporto del DPO, un Registro delle attività di trattamento svolte sotto la propria responsabilità, in ottemperanza a quanto previsto dall'articolo 30 GDPR. Si tratta di uno strumento fondamentale, non soltanto ai fini dell'eventuale supervisione da parte dell'Autorità Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno della Società, indispensabile per ogni valutazione e analisi del rischio privacy.

La tenuta del Registro delle attività di trattamento è parte integrante di un sistema di corretta gestione dei dati personali. In particolare, in merito alla protezione dei dati personali, Kipoint attribuisce una elevata rilevanza alla declaratoria circa le finalità di protezione dei dati personali.

Tale Registro contiene le seguenti informazioni minime:

- Il nome e i dati di contatto del Titolare del trattamento;

- Le finalità del trattamento;
- Una descrizione delle categorie di Interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;
- La base giuridica del trattamento;
- I termini di conservazione e quelli previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

KIPOINT definisce, nella procedura "Gestione Registro Trattamento dati" (di prossima emissione) un processo di gestione del Registro in base al quale i Delegali al trattamento, anche per il tramite dei loro Sub Delegati:

- Assicurano la compilazione e l'aggiornamento del Registro, curando la correttezza e la completezza delle informazioni relative all'area di trattamento di competenza;
- Segnalano tempestivamente al Tavolo Permanente Coordinamento Privacy ogni nuovo trattamento o modifica rilevante ai trattamenti svolti;
- Consultano il Registro per la corretta gestione dei dati personali di competenza.

Al fine di assicurare la completezza di tale Registro, è obbligo dei Delegati al trattamento contribuire al costante aggiornamento dello stesso. In particolare, i Delegati al trattamento hanno l'obbligo di verificare e garantire la presenza della base giuridica del trattamento prima di procedere con l'avvio dello stesso.

Il Gruppo di Lavoro Privacy assicura la complessiva coerenza delle informazioni censite, consulta e gestisce il Registro nell'ambito delle attività di competenza.

I Registri delle attività di trattamento possono essere tenuti o in forma scritta o in formato elettronico e devono essere messi a disposizione dell'Autorità di controllo, in caso di richiesta.

2.3.2 Informative e Consensi

Kipoint, in ottemperanza agli articoli 12, 13, 14, 15 del GDPR, adotta e tiene costantemente aggiornate le informazioni contenute nelle Informative Privacy e garantisce la revisione del processo di gestione dei consensi.

L'obiettivo di tale processo è garantire la comunicazione agli Interessati di tutte le informazioni necessarie per assicurare un trattamento corretto e trasparente, tramite un'Informativa che deve essere redatta in forma concisa, trasparente, intellegibile, facilmente accessibile e con un linguaggio semplice e chiaro.

L'Informativa contiene i principi generali richiesti dal Regolamento e rinvia a sezioni dedicate del sito istituzionale per la specifica di informazioni di dettaglio, quali ad esempio quelle relative alle finalità del trattamento, ai destinatari dei dati e ai tempi di conservazione.

La struttura dell'Informativa standard è organizzata tenuto conto dei seguenti requisiti stabiliti dal GDPR:

- Definizioni principali;
- Dati di contatto del Titolare del trattamento e del Responsabile della Protezione dati;
- Soggetti autorizzati al trattamento e destinatari dei dati;
- Origine e categoria dei dati trattati;
- Base giuridica del trattamento;
- Elenco dei diritti dell'Interessato, con l'integrazione, ove necessario, degli elementi di novità introdotti dal GDPR, quali ad esempio la portabilità dei dati;
- Trasferimento dati verso Paesi Terzi;
- Trattamento dei dati personali di soggetti minori, con annessa gestione dei consensi, contemplando le ipotesi in cui il consenso deve essere espresso da un rappresentante della Responsabilità genitoriale, alternativamente per i casi previsti dalla legge applicabile dallo stesso minore;
- Tempi di conservazione dei dati;
- Consensi.

La gestione dei Consensi si fonda su un modello di processo *data subject-centric* che prevede per ciascuna società del Gruppo Poste Italiane:

- La raccolta dei Consensi privacy (es. a fini marketing), per cliente e non per servizio/prodotto;
- La riconducibilità dei Consensi ad un determinato cliente; l'adozione di un criterio cronologico, in base al quale si terrà conto, per ciascuna società del Gruppo Poste Italiane, esclusivamente dell'ultimo tra i Consensi (o dissensi) acquisiti con riferimento ad un determinato indipendentemente dalla tipologia di servizio erogato. In particolare, sarà mantenuto lo storico dei consensi, con timestamp (data e ora) e matricola dell'operatore che

avrà acquisito i Consensi (per i canali di acquisizione tramite operatore) e/o la fonte di acquisizione (es. website).

2.3.3 Tipologie di Consensi: Persone fisiche e giuridiche o soggetti assimilabili

Relativamente ad un cliente, persona fisica (c.d. «Interessato»), il GDPR prevede che il trattamento dei dati personali avvenga esclusivamente previo consenso espresso, preventivo, informato e libero di quest'ultimo (articoli 7 e 8 GDPR). Inoltre, se il consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

In fase di acquisizione di un cliente — persona fisica o soggetto assimilabile — Kipoint, per i trattamenti di cui è Titolare, sottopone all'Interessato quattro tipologie di consensi di natura facoltativa e revocabili in qualsiasi momento:

- Il consenso a Kipoint per la proposizione commerciale di prodotti o servizi di Kipoint, di SDA, di Poste Italiane e delle società del Gruppo Poste Italiane;
- Il consenso a Kipoint per la proposizione commerciale di prodotti o servizi di soggetti terzi non appartenenti al Gruppo Poste Italiane;
- Il consenso a Kipoint per la profilazione, ai fini della proposizione di offerte personalizzate e del miglioramento della qualità dei prodotti o servizi di Kipoint;
- Il consenso a Kipoint per la comunicazione dei dati attinenti il proprio profilo a Capo Gruppo e alle Società del Gruppo Poste Italiane, ai fini della proposizione di offerte personalizzate e del miglioramento della qualità dei prodotti o servizi di queste ultime.

Kipoint ritiene siano da individuarsi quali persone fisiche e possibili soggetti Interessati, le seguenti categorie a titolo esemplificativo ma non esaustivo: privato cittadino, libero professionista, lavoratore autonomo, amministratore di condominio.

Relativamente alla persona giuridica, si precisa che qualsiasi ente, associazione o soggetto assimilabile non è qualificabile come soggetto «Interessato», bensì come «Cliente». Inoltre, il GDPR è da ritenersi applicabile quale disciplina soltanto per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Per le persone giuridiche, qualora si intenda trattare i dati di quest'ultime con sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore, per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, è richiesto, all'atto dell'acquisto o sottoscrizione di un determinato prodotto/servizio, per i trattamenti di cui è Titolare Kipoint, di sottoporre due tipologie di consensi di natura facoltativa e revocabili in qualsiasi momento:

- il Consenso a Kipoint per la proposizione commerciale di prodotti o servizi di Kipoint, di Poste e/o delle Società del Gruppo Poste Italiane, con modalità automatizzate (es. email, SMS, MMS);
- il Consenso a Kipoint per la proposizione commerciale di prodotti o servizi di soggetti terzi non appartenenti al Gruppo Poste Italiane con modalità automatizzate (es. email, SMS, MMS).

L'Informativa privacy da sottoporre alle persone fisiche e giuridiche o soggetti assimilabili, prima o contestualmente alla raccolta dei dati, è distinta in:

a) servizi e/o prodotti principali;

b) servizi e/o prodotti accessori.

Nella prima occasione utile in cui un cliente prospect sottoscrive un servizio e/o prodotto principale deve essere fornita allo stesso - persona fisica, giuridica o soggetto assimilabile - l'Informativa privacy con annesso modulo per il rilascio dei consensi facoltativi (modulo km.001.00 “Informativa per il trattamento dei dati personali”). Ove la sottoscrizione vada a buon fine, il cliente prospect diventa actual.

2.3.4 Data Protection Impact Assessment

Il Titolare del trattamento ha l'onere di effettuare una valutazione d'impatto privacy — anche attraverso i Delegati e Sub Delegati al trattamento - sui trattamenti effettuati e/o previsti qualora gli stessi presentino un rischio elevato per i diritti e le libertà delle persone fisiche.

Il *Data Protection Impact Assessment:*

- Ha l'obiettivo di prevenire ed identificare in anticipo i possibili rischi che possono derivare dalle attività di trattamento svolte dal Titolare/Delegato del trattamento e di definire le misure di sicurezza tecniche ed organizzative adeguate ai livelli di rischio rilevati;

- Viene eseguito sotto la responsabilità del Titolare al trattamento, e per esso, dei Delegati al trattamento con l'eventuale supporto delle Funzioni specialistiche ed è soggetto alla costante supervisione e sorveglianza del DPO;
- Viene applicato ai nuovi trattamenti ed è da considerarsi parte integrante del processo di Privacy by Design e non si esaurisce nella fase di progettazione, ma è da intendersi come un processo continuativo, che deve essere condotto iterativamente sul trattamento anche ogni qualvolta il medesimo subisca una variazione significativa.

In particolare, il Delegato/Sub Delegato al trattamento, in raccordo con il responsabile dell'iniziativa progettuale (ove non dovesse coincidere), assicura lo svolgimento della valutazione d'impatto sulla protezione dei dati personali ("DPIA") nei casi in cui si preveda, a titolo esemplificativo e non esaustivo:

- Lo sviluppo di nuovi servizi o trattamenti, che a titolo esemplificativo, potrebbero comportare l'utilizzo di nuovi applicativi che prevedono di trattare dati personali;
- Un intervento significativo sui servizi e/o trattamenti aventi a supporto applicativi esistenti che trattano o che potrebbero trattare dati personali;
- L'attivazione di un nuovo servizio che potrebbe richiedere una nuova attività di trattamento dei dati personali;
- Una modifica ad un processo di business esistente che potrebbe modificare le attività di trattamento dei dati personali o richiederne nuove;
- L'attività di esternalizzazione di servizi che prevedono il trattamento di dati personali;
- Una qualsiasi attività che potrebbe avere un impatto diretto/indiretto sui trattamenti di dati personali esistenti.

All'esito della valutazione d'impatto, il Titolare può decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'Autorità di Controllo competente per ottenere indicazioni su come gestire il rischio residuale. L'Autorità non ha il compito di autorizzare il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del Titolare e può, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58 GDPR, nello specifico, dall'ammonimento del Titolare alla limitazione o al divieto di procedere al trattamento.

Pertanto, l'intervento delle Autorità di Controllo è principalmente ex post, ossia si colloca successivamente alle determinazioni assunte autonomamente dal Titolare.

Le valutazioni effettuate e le decisioni assunte devono essere documentate e conservate, per conto del Titolare, dal Delegato del trattamento, al fine di dimostrare il rispetto del principio di accountability.

2.3.5 Misure di sicurezza

Kipoint, in qualità di Titolare del trattamento e in ottemperanza agli articoli 25 e 32 GDPR, mette in atto misure organizzative e tecniche adeguate per garantire ed essere in grado di dimostrare, che:

- Il trattamento è effettuato conformemente al Regolamento;
- Il livello di sicurezza sia adeguato al rischio e comprenda un procedimento per testare, verificare e valutare regolarmente l'efficacia delle misure stesse, al fine di garantire la massima sicurezza del trattamento ed il miglioramento continuo con una pianificazione pluriennale.

Secondo i chiarimenti forniti dall'Autorità Garante per la Protezione dei Dati, l'elenco di misure di sicurezza cui al all'art. 32, par. 1 del GDPR è una lista aperta e non esaustiva. Pertanto, risulta superato il precedente obbligo generalizzato di adozione di misure "minime" di sicurezza, poiché la valutazione di adeguatezza è rimessa, caso per caso, al Titolare e al Responsabile del trattamento, in rapporto ai rischi specificamente individuati dall'articolo 32 GDPR. L'adozione del suddetto documento, tuttavia, rimane una pratica incentivata, allo scopo di contestualizzare il complesso delle misure di sicurezza adottate e messe in campo.

Per attestare l'adeguatezza delle misure di sicurezza adottate, è facoltà del Titolare del trattamento di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione.

Inoltre, per garantire i massimi livelli di conformità, i Delegati al trattamento devono tenere conto delle eventuali Linee Guida o buone prassi emanate in materia dall'Autorità Garante per la Protezione dei Dati.

2.3.6 Esercizio dei diritti dell'Interessato

Kipoint, in qualità di Titolare, attribuisce significativo rilievo all'esercizio dei diritti dell'Interessato previsti dal Regolamento (cfr. principi di riferimento del Capo III del GDPR). In particolare, l'Azienda garantisce l'esercizio dei diritti previsti dal Regolamento mediante un processo di gestione delle richieste effettuate dagli Interessati con riferimento ai seguenti diritti:

- Diritto di accesso (articolo 15, GDPR): l'Interessato ha il diritto di ottenere da Kipoint, in qualità di Titolare del trattamento, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, ottenere l'accesso ai dati personali;
- Diritto di rettifica (articolo 16, GDPR): l'Interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo;
- Diritto all'oblio (articolo 17, GDPR): l'Interessato ha il diritto di ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali;
- Diritto di limitazione (articolo 18, GDPR): l'Interessato ha il diritto di ottenere la limitazione del trattamento per alcuni casi espressamente indicati dal GDPR;
- Diritto alla portabilità dei dati (articolo 20, GDPR): l'Interessato ha il diritto di ricevere in un formato strutturato, i dati personali forniti che lo riguardano e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento, senza impedimento alcuno;
- Diritto di opposizione (articolo 21, GDPR): l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

Il termine per la risposta da fornire all'istanza dell'Interessato, per ciascuno dei diritti sopra riportati (compreso il diritto di accesso) è pari a un mese, estendibile fino a tre mesi in casi di particolare complessità. Il Titolare deve fornire un riscontro all'Interessato entro un mese dalla richiesta, anche in caso di diniego.

Rientra nelle responsabilità del Titolare la valutazione della complessità del riscontro all'Interessato e la definizione dell'ammontare dell'eventuale contributo da chiedere all'Interessato, in caso di richieste infondate o eccessive, anche ripetitive (articolo 12, paragrafo 5, GDPR); in quest'ultimo caso il Titolare può tenere conto dei costi amministrativi sostenuti.

Il riscontro all'interessato deve avvenire in forma scritta, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere fornito oralmente, solo se esplicitamente richiesto dall'Interessato (articolo 12, paragrafo 1 e articolo 15, paragrafo 3, GDPR). La risposta fornita deve essere completa, "intelligibile", concisa, trasparente e facilmente accessibile, e deve utilizzare un linguaggio semplice e chiaro.

I processi aziendali assicurano l'assolvimento dei citati doveri del Titolare, per il tramite del Progetto Governance IT

Pertanto, è compito primario delle strutture aziendali che ricevono direttamente istanze da parte degli Interessati curane la tempestiva trasmissione verso il Progetto Governance IT Quest'ultimo cura l'istruttoria e l'indirizzamento alle strutture interne competenti.

2.3.6.1 Diritto di accesso

Il Titolare deve fornire, tra le altre informazioni, il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. Nell'ambito delle informazioni da fornire non rientrano le "modalità" del trattamento.

Kipoint, aderendo alla raccomandazione del Garante Privacy, intende consentire agli interessati di consultare da remoto e in modo sicuro. L'esercizio di tale diritto, ove consentito dagli strumenti di accesso e dalla gestione in sicurezza dei dati/informazioni, sarà inoltre collegato al diritto di portabilità dei dati.

2.3.6.2 Diritto di cancellazione (diritto all'oblio)

Il diritto "all'oblio" si configura come un diritto dell'Interessato alla cancellazione dei propri dati personali in forma rafforzata.

L'esercizio dei diritti previsti dall'articolo 7, paragrafo 3, lettera b) del Codice Privacy e ora articolo 15 e seguenti del GDPR veniva già garantito da Kipoint. Tale diritto, ad oggi, ha un campo di applicazione più esteso, poiché l'interessato può richiedere la cancellazione dei propri dati, per esempio, anche a seguito della revoca del consenso al trattamento (per maggiori dettagli si veda l'articolo 17, paragrafo 1 del GDPR).

2.3.6.3 Diritto alla limitazione del trattamento

Trattasi di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'articolo 7, paragrafo 3, lettera a) del Codice: in particolare, deve essere esercitabile sia in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi) sia qualora l'interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si opponga al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del Titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato, a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

2.3.6.4 Diritto alla portabilità dei dati

Il diritto alla portabilità dei dati (articolo 20, GDPR) non si applica ai trattamenti non automatizzati (pertanto non viene applicato agli archivi o ai registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'Interessato (pertanto, a titolo esemplificativo, non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare) e impatta solo i dati che siano stati forniti dall'Interessato al Titolare.

Il diritto di portabilità dei dati è collegato al diritto di accesso sicuro e alla gestione in sicurezza dei dati.

2.3.7 Responsabili Esterni

Kipoint, in ottemperanza dell'articolo 28 del GDPR, in qualità di Titolare, ove ritenga opportuno, ricorre ad un Responsabile Esterno per l'esecuzione per proprio conto di specifiche attività di trattamento. In tali ipotesi, pertanto, è prevista la nomina di un Responsabile Esterno con un atto formale a norma del diritto dell'Unione Europea. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato.

Il processo di nomina del Responsabile si articola in diverse fasi, attraverso le quali viene designato il Responsabile Esterno con atto formale che fornisce indicazioni circa le responsabilità, i doveri e i limiti del mandato. Segue poi il monitoraggio del rapporto, inteso a verificare il rispetto dei requisiti riportati nell'atto di nomina e la corretta operatività, prevenendo anche i casi di revoca della nomina, in ipotesi di mancato rispetto degli stessi da parte del Responsabile Esterno. Possono, infine, essere previsti alcuni casi in cui il Responsabile Esterno possa nominare un altro Responsabile (Sub-Responsabile) al trattamento, previa autorizzazione di Kipoint.

2.3.8 Trasferimento di dati personali in Paesi extra-UE

Kipoint e in generale il Gruppo di Poste Italiane effettua di norma trattamenti di dati personali nell'ambito di servizi gestiti nel territorio dell'Unione Europea. Per alcuni servizi, il trasferimento dei dati in un Paese fuori del territorio dell'UE è richiesto dall'interessato ed è parte dell'esecuzione del contratto (es. servizio Internazionale). In merito, il trasferimento di dati personali verso un paese terzo extra UE è ammesso se la Commissione UE ha adottato una decisione di adeguatezza di tale Paese terzo affinché garantisca un livello di protezione adeguato (articolo 45, GDPR).

Nell'ipotesi di trasferimento dei dati verso Paesi per i quali non vi sia una decisione della Commissione UE, il trasferimento è consentito solo se vi sono le garanzie adeguate previste dall'articolo 46 del GDPR, se si osserva la procedura delle norme vincolanti d'impresa (articolo 47, GDPR), ovvero per le ipotesi di deroga in specifiche situazioni, stabilite dall'articolo 49 del Regolamento.

Pertanto, nel caso in cui una o più Funzioni di Kipoint abbiano motivate esigenze di trasferire dati personali fuori dall'Unione Europea, i rispettivi Delegati al trattamento, fuori dai casi descritti dall'articolo 45 del GDPR, devono sottoporre il caso alla valutazione del DPO per il tramite del Gruppo di Lavoro Privacy, per la verifica della sussistenza delle condizioni previste dagli articoli 46 e ss. del GDPR.

Prima di effettuare la richiesta di consultazione del DPO, la Funzione richiedente deve verificare la sussistenza di specifiche garanzie tassativamente elencate dal GDPR, con riguardo all'adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione Europea. Le decisioni di adeguatezza assunte prima dell'entrata in vigore del GDPR restano valide fino a loro eventuale revisione o modifica (articolo 45, paragrafo 9 e articolo 96, GDPR).

In assenza di decisioni di adeguatezza della Commissione, il Delegato al trattamento che abbia interesse a trasferire dati fuori dall'UE deve raccogliere gli elementi utili affinché:

1. possano essere valutate le garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dal soggetto terzo, destinatario dei dati, residente fuori dall'UE;
2. in assenza di garanzie adeguate, sia motivato l'utilizzo di deroghe al divieto di trasferimento applicabili in conformità all'articolo 49 del GDPR.

Nel dettaglio, se il Paese terzo non è tra quelli oggetto di decisione di adeguatezza da parte della Commissione Europea, Kipoint, in qualità di Titolare del trattamento, richiede al soggetto terzo, Responsabile del trattamento, come condizione necessaria per effettuare il trasferimento, l'adozione alternativamente di:

- Clausole Contrattuali Standard emanate dalla Commissione Europea, con le quali il soggetto terzo si impegna a trattare i dati personali in conformità con la normativa comunitaria;
- un Codice di Condotta o ad uno dei meccanismi di certificazione approvati dal Garante per la Protezione dei Dati Personali.

In assenza delle condizioni sopra descritte ed in applicazione dei principi di deroga ammessi dall'articolo 49 del GDPR, il Delegato al trattamento può effettuare il trasferimento dei dati se: l'Interessato ha espressamente consentito al trasferimento dopo essere stato informato dei possibili rischi, o quando tale trasferimento è necessario per l'esecuzione di un contratto a favore dell'Interessato o per importanti motivi di ordine pubblico, interessi vitali o, infine, per accertare, esercitare o difendere un diritto in sede giudiziaria.

2.3.9 Cancellazione dei dati (Data Retention)

Kipoint, in qualità di Titolare e in ottemperanza ai principi del GDPR, stabilisce i termini per la conservazione dei dati personali, al fine di assicurare che gli stessi non vengano mantenuti per un periodo superiore a quello necessario al conseguimento delle finalità per le quali il dato è trattato, alternativamente per i termini previsti in l'esecuzione di obblighi di legge. Pertanto, è garantita l'adozione di misure tecnico - organizzative necessarie affinché i dati personali siano conservati per un periodo di tempo adeguato alle finalità„ nonché in caso di richiesta da parte del soggetto interessato opportunamente rettificati o cancellati.

A tal fine, sotto la responsabilità del Titolare del trattamento, deve essere stabilito per ogni tipologia di trattamento, e in relazione alla base giuridica e alle finalità di trattamento, il periodo di massima conservazione. Nel caso di nuovi trattamenti, tale valutazione viene svolta in coerenza con il principio Privacy by default e il tempo di conservazione viene tracciato nel Registro delle attività di trattamento.

A valle del raggiungimento delle finalità del trattamento e scaduti i termini legali per la conservazione dei dati, essi vengono cancellati e/o resi non disponibili, fatti salvi eventuali avvenimenti, previsti dal Regolamento, che ne impongano il mantenimento per un ulteriore periodo.

Inoltre, in funzione del diritto "all'oblio", quale richiesta di cancellazione a cura dell'Interessato dei propri dati personali in forma rafforzata, si prevede l'obbligo per il Titolare del trattamento di cancellare i dati, ed in caso di pubblicazione dei dati personali dell'Interessato (ad esempio su un sito web) di informare della richiesta di cancellazione altri Titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" *(Faq Garante Privacy in relazione all'articolo 17, paragrafo 2 GDPR).*

2.3.10 Notifica di violazione dei dati personali all'Autorità di controllo (Data Breach)

Kipoint, in qualità di Titolare del trattamento, in caso di violazione dei dati personali che comportino rischi per i diritti e le libertà degli interessati, procede alla notifica al Garante Privacy senza ingiustificato ritardo ed entro 72 ore dalla rilevazione (articoli 33 e 34, GDPR). Qualora il rischio per i diritti e le libertà degli Interessati sia elevato, oltre alla notifica al Garante, il Titolare del trattamento è tenuto a darne comunicazione all'Interessato, segnalando la natura della violazione senza ingiustificato ritardo e mediante un linguaggio semplice e chiaro. Il Titolare del trattamento deve, inoltre, documentare le violazioni dei dati personali subite, anche se non notificate all'Autorità di Controllo e non comunicate agli Interessati, nonché le relative circostanze e conseguenze ed i provvedimenti adottati (articolo 33, paragrafo 5, GDPR) al fine di renderli disponibili, su richiesta, al Garante in caso di accertamenti. Il Gruppo di Lavoro Privacy fa da facilitatore presso il DPO delle azioni necessarie e si incarica della notifica al Garante ed agli interessati.

2.4 Formazione e Cultura Privacy

L'AD, con il Gruppo di Lavoro Privacy, la funzione CA/TA/Privacy di Poste Italiane e le competenti strutture in ambito formazione di Capo Gruppo, supporta le altre funzioni di Kipoint affinché provvedano *a:*

- Definire ed aggiornare i piani di formazione e sensibilizzazione periodici in materia di protezione dei dati personali. Tali corsi potranno avere carattere generale ed orientati a tutto il personale dipendente, o essere mirati per specifici ruoli e responsabilità in ambito Privacy. Attraverso tali piani, sono identificati i destinatari dell'attività di formazione per ciascuna funzione aziendale e/o per ruoli specifici di risorse e sono definite le modalità di erogazione della stessa
- Predisporre il materiale formativo, indirizzando le attività propedeutiche all'erogazione dei corsi e monitorandone l'avvenuta partecipazione ed esito.

Le funzioni Kipoint considerano la formazione quale misura organizzativa indispensabile e, con il supporto delle competenti Funzioni aziendali, pianificano il fabbisogno formativo e coinvolgono il proprio personale incaricato delle attività di trattamento agli eventi formativi e di sensibilizzazione.

2.5 Cooperazione con l'Autorità di Controllo

Il Data Protection Officer coopera, su richiesta, con l'Autorità di Controllo e provvede a:

- Gestire le relazioni con l'Autorità Garante per la Protezione dei Dati in merito alle tematiche di conformità o nell'ambito di indagini conoscitive sull'applicazione del Regolamento, coordinando le attività necessarie per l'evasione delle risposte;
- Gestire, avvalendosi delle competenti funzioni aziendali, i reclami indirizzati al Garante dalla clientela, fornendo gli opportuni riscontri;
- Fornire assistenza e collaborazione al Titolare del trattamento nella gestione degli eventi di non conformità, assicurando l'adozione delle misure tecniche ed organizzative adeguate rispetto ai requisiti del GDPR.

2.6 Ruoli e responsabilità

Il Modello Organizzativo Privacy di Kipoint è costituito dalle seguenti figure:

- **Titolare** è Kipoint., rappresentata dall'Amministratore Delegato;
- **Data Protection Officer (DPO):**
  - è stato introdotto dal GDPR in qualità di esperto in materia privacy, con il compito di favorire l'osservanza della normativa e verificare l'efficacia delle misure che il Titolare ha elaborato e strutturato;
  - è nominato dal Titolare, ai sensi dell'articolo 37 del Regolamento UE 2016/679 e si avvale del supporto della Funzione CA/TA/Privacy in ambito Poste Italiane e del Tavolo Permanente Coordinamento Privacy in ambito Kipoint per lo svolgimento dei compiti assegnati;
- **Delegati al trattamento**: sono le persone fisiche che, designate dal Titolare del trattamento per iscritto, lo rappresentano per quanto riguarda gli obblighi relativi alle norme del GDPR. I Responsabili pro-tempore delle funzioni organizzative di primo livello sono nominati Delegati al Trattamento;
- **Incaricati** sono i dipendenti di Kipoint autorizzati al trattamento dei dati personali.