APPROFONDIMENTI IN MATERIA DI TUTELA DELLA PRIVACY[1]

[1] [1] Contenuto redatto al fine di soddisfare i requisiti di divulgazione dell'agenzia di rating S&P Global.

INDICE

L'impegno del Gruppo in termini di tutela della privacy

Nel corso degli anni il Gruppo ha attribuito una grande importanza al tema della protezione dei dati personali, potenziando costantemente il proprio sistema normativo aziendale e per garantire la piena compliance alle disposizioni vigenti e a quanto disciplinato all'interno del *General Data Protection Regulation* (GDPR).

In tale contesto, il Gruppo Poste Italiane ha predisposto una *Policy* Aziendale in materia di Protezione Dati Personali e delle Linee Guida *Privacy* e Sistema di Gestione della protezione dei dati personali, queste ultime introdotte con l'obiettivo di garantire una gestione dei dati uniforme a livello di Gruppo. Il sistema normativo, composto da procedure, linee guida e politiche, viene applicato nei rapporti con tutti i *partner* e fornitori per assicurare una corretta gestione dei rischi legati al tema della *privacy* in tutte le operazioni del Gruppo.

Il mancato rispetto degli *standard* definiti dal sistema, che può condurre al verificarsi di violazioni, può comportare l'applicazione di sanzioni disciplinari ai dipendenti, secondo quanto previsto dal CCNL di Poste Italiane. Tali sanzioni sono gradualmente più severe in base alla gravità della violazione (ammonizione scritta, multa, sospensione dal servizio con privazione della retribuzione, licenziamento senza preavviso ecc.).

Le Linee Guida definiscono il modello aziendale della *privacy* e attuano i princìpi di *Privacy by Design* e *Privacy by Default*, sottolineando l'obbligo dell'Azienda di assicurare un'adeguata protezione dei dati personali fin dalla progettazione dei prodotti/servizi e dei sistemi informatici, nonché di garantire il rispetto della normativa *privacy* nei processi predefiniti di raccolta e trattamento dei dati. Poste Italiane si impegna, inoltre, a garantire una corretta gestione dei rischi in materia di protezione dei dati, attraverso l'esecuzione del processo periodico di riesame da parte della Direzione a livello di Gruppo, come disposto all'art. 32.

La gestione dei rischi di compromissione dei presidi a tutela della *privacy* e di violazione dei dati è integrata nel più ampio modello di rischio del Gruppo Poste Italiane. In particolare, i rischi e le opportunità relativi al tema della gestione della privacy sono stati mappati in ambito *Enterprise Risk Management* (ERM). A titolo esemplificativo, sono stati identificati come rilevanti i seguenti rischi:

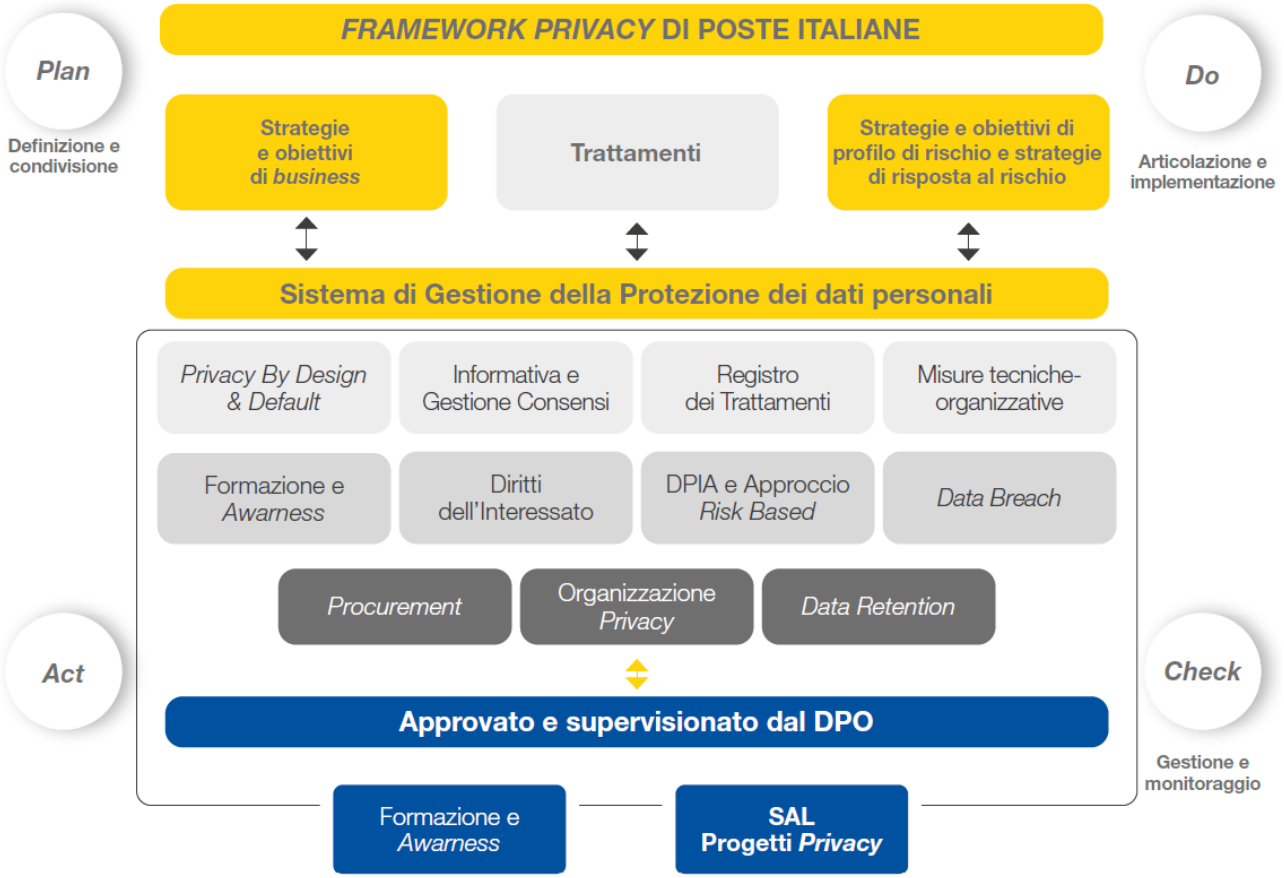
- Malfunzionamento e/o carenze nella sicurezza dei sistemi informatici che possono comportare violazioni di dati personali, perdita o compromissione di informazioni, blocchi o rallentamenti delle attività operative, nonché disservizi nei confronti della clientela;
- Mancato rispetto della normativa sulla *privacy*. Trattamento dei dati personali in violazione delle disposizioni normative vigenti;
- Uso inadeguato dei *big data* e dell'intelligenza artificiale e aumento delle violazioni della *privacy*.

Per garantire i massimi *standard* di protezione dei dati personali, il Gruppo effettua annualmente degli *audit* al fine verificare la conformità della propria *Policy* sulla *Privacy*. Nello specifico, tali *audit* vengono condotti sia internamente attraverso le funzioni del Gruppo, che esternamente (mediante verifiche di terze parti) nell'ambito delle verifiche realizzate per l'ottenimento e il mantenimento delle certificazioni ISO 27001 e ISO 20001.

1. Il Framework Privacy di Poste Italiane

Al fine di garantire adeguati livelli di riservatezza, integrità e disponibilità dei dati, delle informazioni e dei servizi erogati alla clientela, Poste Italiane ha inoltre sviluppato e adottato un apposito *Framework Privacy*.

Tale *framework* fornisce la ricognizione delle aree d'intervento in cui operano i relativi presidi organizzativi e tecnici sviluppati, al fine di offrire con continuità il monitoraggio dei progressi raggiunti e favorire il miglioramento continuo del sistema di gestione.



Poste Italiane ha individuato per tutto il Gruppo la figura del Data Protection Officer, soggetto esperto di *privacy* che assume la responsabilità di valutare e indirizzare la gestione del trattamento dei dati personali da parte del titolare, in ottemperanza alla normativa in materia, con riferimento in particolare a quanto disposto dal GDPR, e nell'ottica di un *continuous improvement*.

In coerenza con tale impostazione, la funzione Privacy garantisce un presidio unico a livello di Gruppo per tutte le responsabilità relative alle tematiche di protezione dei dati personali e coordina lo sviluppo del suddetto *framework*.

Il Centro Servizi Privacy opera all'interno di tale funzione ed è incaricato di rappresentare un punto di riferimento unico in materia privacy per i clienti, nonché di raccogliere e gestire in maniera efficiente e centralizzata tutte le istanze che pervengono da quest'ultimi, come ad esempio le richieste di accesso, rettifica o integrazione e cancellazione dei dati personali e di variazione dei consensi espressi, monitorandone altresì l'andamento, al fine di identificare eventuali opportunità di perfezionamento dei processi aziendali.

Il Centro Servizi Privacy, in ragione del suo approccio verso il miglioramento continuo, la peculiare gestione delle richieste dei clienti e la corretta compliance alle disposizioni normative, è certificato per il proprio sistema di gestione per la sicurezza delle informazioni in accordo allo *standard* ISO 27001:2013 e per la protezione dei dati personali secondo lo *standard* ISO 27701:2019, attraverso cui la funzione *Privacy* di Poste Italiane è in grado di dimostrare la conformità dei servizi certificati al GDPR e ad altri requisiti sulla *privacy* dei dati.

2. La protezione dei dati personali dei clienti

In virtù delle disposizioni del GDPR a cui il Grippo Poste Italiane aderisce, l'Azienda fornisce ai clienti un'informativa completa sul trattamento dei dati personali, assicurando che all'interessato vengano fornite informazioni su: natura e utilizzo delle informazioni raccolte; durata della conservazione dei dati negli archivi aziendali; modalità di protezione dei dati; politiche di comunicazione dei dati a terzi (soggetti pubblici e privati). Poste Italiane prevede inoltre la possibilità per il cliente di decidere le modalità di raccolta, utilizzo, conservazione ed elaborazione dei propri dati, tra cui: la possibilità di adottare l'opzione Opt-out; la richiesta di manifestazione esplicita e vincolante del consenso (c.d. Opt-in), necessaria per poter procedere legittimamente al trattamento dei dati personali; il diritto di accesso ai dati personali in possesso della Società; il diritto alla portabilità dei dati, richiedendo il trasferimento dei dati personali ad altri fornitori di servizi; il diritto alla rettifica, richiedendo la correzione di dati personali inesatti o incompleti; e il diritto alla cancellazione (noto anche come "diritto all'oblio"), richiedendo la cancellazione dei dati personali.

ANNEX | Numero di clienti i cui dati sono stati usati per scopi secondari

Clienti i cui dati sono stati usati per scopi secondari (%)	2021	2022	2023	2024
Percentuale di clienti i cui dati sono stati usati per scopi secondari (%)	0	0	0	0