Posteitaliane

PRIVACY PROTECTION INSIGHTS[1]

[1] Content prepared in order to comply with disclosure requirements of S&P Global rating agency

INDEX

The Group's commitment to privacy protection

Over the years, the Poste Italiane Group has attributed great importance to the issue of personal data protection, constantly strengthening its corporate regulatory framework and to ensure full compliance with current provisions and what is regulated within the General Data Protection Regulation (GDPR).

In this context, Poste Italiane has developed a Corporate Policy on Personal Data Protection and Privacy Guidelines and a Personal Data Protection Management System, the latter introduced with the aim of ensuring uniform data management at Group level. The regulatory framework, consisting of procedures, guidelines and policies, is applied in relationships with all partners and suppliers to ensure correct management of risks related to the topic of privacy in all of the Group's operations.

Failure to comply with the standards defined by the system, which may lead to violations, may result in the application of disciplinary sanctions to employees, in accordance with the provisions of the Poste Italiane CCNL (National Collective Labor Agreement). These sanctions become gradually more severe according to the seriousness of the breach (written warning, fine, suspension from work without pay, dismissal without notice, etc.).

The Guidelines define the corporate privacy model and implement the principles of Privacy by Design and Privacy by Default, underlining the Company's obligation to ensure adequate protection of personal data from the design phase of products/services and IT systems, as well as ensuring compliance with privacy legislation in the predefined process of data collection and processing. Poste Italiane is also committed to ensuring proper management of data protection risks, by carrying out the periodic supervisory review process at the Group level, as set out in Article 32.

The management of risks related to breaches of privacy safeguards or data violations is embedded into the broader risk model of the Poste Italiane Group. Specifically, risks and opportunities related to the issue of privacy protection have been mapped in the Enterprise Risk Management (ERM) area. By way of example, the following risks were identified as relevant:

- Computer system malfunctions and/ or IT system security failures that may lead to personal data breaches, loss or compromise of information, operational blockages or slowdowns, customer disruptions;
- Non-compliance with privacy regulations Processing of personal data in violation of applicable regulations;
- Inadequate use of big data and artificial intelligence, leading to increased privacy violations.

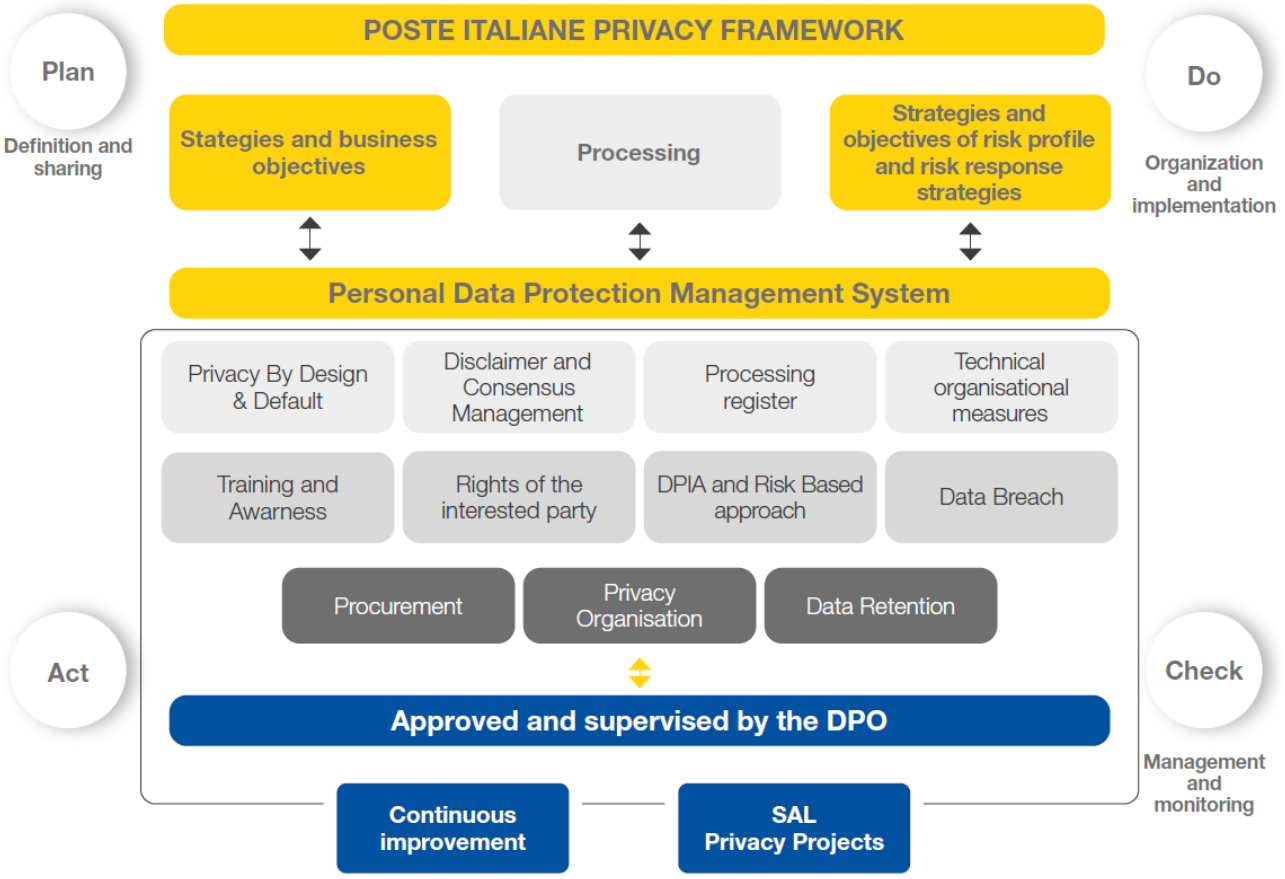
To ensure the highest standards of personal data protection, the Group conducts annual audits in order to verify the privacy policy compliance. Specifically, these audits are conducted both internally through the Group's functions and externally (through third-party audits) as part of the audits conducted for obtaining and maintaining ISO 27001 and ISO 20001 certifications.

1. The Privacy framework of Poste Italiane

In order to ensure adequate levels of confidentiality, integrity and availability of data, information and services provided to customers, Poste Italiane has also developed and adopted a specific Privacy framework.

This framework provides a comprehensive overview of the intervention areas in which the relevant organizational and technical frameworks that have been developed operate, in order to

provide ongoing monitoring of the progress achieved and encourage continuous improvement of the management system.



Poste Italiane has designated for the entire Group the figure of a Data Protection Officer (DPO), a privacy expert responsible for evaluating and directing the management of personal data processing by the data controller, in compliance with applicable data protection regulations, with particular reference to the provisions of the GDPR, and in a perspective of continuous improvement.

In line with this approach, the Privacy function ensures nomophylactic oversight at Group level for all responsibilities relating to personal data protection issues and coordinates the development of the aforementioned framework.

The Privacy Service Centre operates within this function and its task is to represent a single point of reference for customers in matters of privacy and to collect and manage efficiently and centrally all the requests received from customers, such as requests for access, rectification or integration and deletion of personal data and changes in the consent given, also monitoring their progress in order to identify any opportunities for improving business processes.

The Privacy Service Centre, due to its approach towards continuous improvement, unique handling of customer requests and correct compliance with regulatory provisions, is certified for its information security management system according to ISO 27001:2013 and for personal data protection according to ISO 27701:2019, through which Poste Italiane's Privacy function is able to

demonstrate the compliance of certified services with the GDPR and other data privacy requirements.

2. The processing of customers' personal data

In accordance with the provisions of the GDPR, which the Poste Italiane Group complies with, the Company provides comprehensive information to customers on the processing of personal data, ensuring that the data subjects are provided with information on: the nature and use of the information collected; the duration of data storage in the company's archives; data protection methods; and policies on data sharing with third parties (public and private entities). Poste Italiane also provides for the possibility for the customer to decide on the methods of collection, use, storage and processing of their data, including: the possibility of adopting the Opt-out option; the requirement for explicit and binding consent (the so-called Opt-in), necessary to lawfully process personal data; the right to access personal data held by the Company; the right to data portability, requesting the transfer of personal data to other service providers; the right to rectification, requesting the correction of inaccurate or incomplete personal data; and the right to erasure (also known as the "right to be forgotten"), requesting deletion of personal data.

ANNEX | Number of customers whose data were used for secondary purposes

Customers whose data were used for secondary purposes (%)	2021	2022	2023	2024
Percentage of customers whose data were used for secondary purposes (%)	0	0	0	0