Data Protection Officer's Report

2025

Rome, May 2026

BANCA D'ITALIA
EUROSISTEMA

CONTENTS

1. Background

In an environment shaped by an increasingly complex regulatory framework and by the pervasive impact of technological innovation, including through the growing use of artificial intelligence-based applications, the Data Protection Officer (DPO) monitors compliance with the General Data Protection Regulation (GDPR) and provides advice on its application.

Against this background, in 2025 the DPO promoted regular engagement with external stakeholders to support Banca d'Italia's ongoing alignment with the guidance of the Italian Data Protection Authority and with emerging best practices at both the national and European levels. The DPO also consolidated its role as a stable and qualified point of contact for other institutions by participating in cooperation forums with the Italian Data Protection Authority in the banking and insurance sectors, as well as in meetings of national and European DPO networks.

Dialogue and coordination with the relevant organizational units within the Bank were further strengthened in order to assess privacy impacts and identify risk mitigation measures as early as possible in all projects involving the processing of personal data.

Finally, at a time when the large-scale and automated collection of personal information is increasing individuals' exposure to cyber threats and making people the primary target of cyberattacks, the DPO promoted initiatives to raise staff awareness. These initiatives sought to strengthen understanding of the risks associated with the processing of personal data, foster a strong culture of data protection throughout the Bank, and encourage behaviour that is consistently careful, responsible and aligned with the security measures in place.

2. Developments in the regulatory framework

On 19 November 2025, the European Commission presented the 'Digital Omnibus', a draft legislative package comprising three proposed regulations aimed at streamlining and simplifying the EU's rules on data sharing and digital technologies. The package also proposes amendments to the GDPR, with a view to simplifying certain aspects of its application in light of the issues that have emerged during the seven years since its entry into force, and to taking account of matters arising from the application of Regulation (EU) 2024/1689 on artificial intelligence (AI Act).

At the domestic level, the Artificial Intelligence Law (Law 132/2025) entered into force on 10 October 2025. This law aligns the national legal framework with the provisions of the AI Act and establishes specific safeguards for the use of new technologies in the public sector. Its aim is to strike a balance between the opportunities offered by the latest innovative tools and the high level of protection that must be guaranteed for citizens' fundamental rights and freedoms.

This law designates two bodies as national authorities for artificial intelligence: the Agency for Digital Italy (Agenzia per l'Italia Digitale, AgID) for promoting AI development, and the National Cybersecurity Agency (Agenzia per la cybersicurezza nazionale, ACN) for supervisory and enforcement activities. Market supervision powers were instead entrusted, within their respective areas of competence, to Banca d'Italia, CONSOB and IVASS.

Finally, following the recent amendment to Law 193/2023 on equal treatment, non-discrimination and the right to be forgotten for those who have recovered from cancer,[1] Banca d'Italia and CONSOB will be responsible, within their remits, for issuing the implementing provisions relating to transactions involving contracts for banking, financial and investment services and to the conclusion or renewal of such contracts.

3. Tasks of the Data Protection Officer

In 2025, the DPO carried out its activities in line with the guidance issued by the Italian Data Protection Authority at the national level and by the European Data Protection Board (EDPB) at the European level. Account was also taken of the work carried out within the institutional forums in which the DPO participates on behalf of the Bank: the Data Protection Officer networks of the European System of Central Banks (ESCB) and of the Single Supervisory Mechanism (SSM), the national DPO network of independent authorities, and the cooperation forums established with the Italian Data Protection Authority for the banking and insurance sectors (see Sections 3.1, 3.2 and 3.3).

The DPO's monitoring and advisory activities focused on strengthening compliance and accountability across the Bank. Specifically, coordination channels and opportunities for engagement with the Bank's organizational units were further expanded in order to involve the DPO at an increasingly early stage in all projects affecting personal data. This helped ensure that data processing activities could be assessed in a timely and integrated manner, and that risks could be mitigated before projects are deployed.

With this in mind, the DPO's participation in the meetings of the Information Technology Committee and in the work of the AI Subcommittee plays a key role. It also reflects the Bank's strong commitment to safeguarding fundamental rights across all areas of its activities. Furthermore, the organizational framework for privacy management was completed following the conclusion of an agreement between the DPO and the Organization Directorate,[2] which performs data controller functions and is responsible for promoting the Bank's organizational development. This process began in 2024, when the DPO and his team were transferred to the Directorate General for Planning, Organization and Accounting.

The organizational framework was further strengthened through the appointment of privacy coordinators within the Bank's Directorates. This helped to apply the principle of privacy by design more effectively, by ensuring that the implications for personal data protection are considered from the outset when changes to organizational structure, regulations and processes are planned in response to organizational developments and technological innovation.

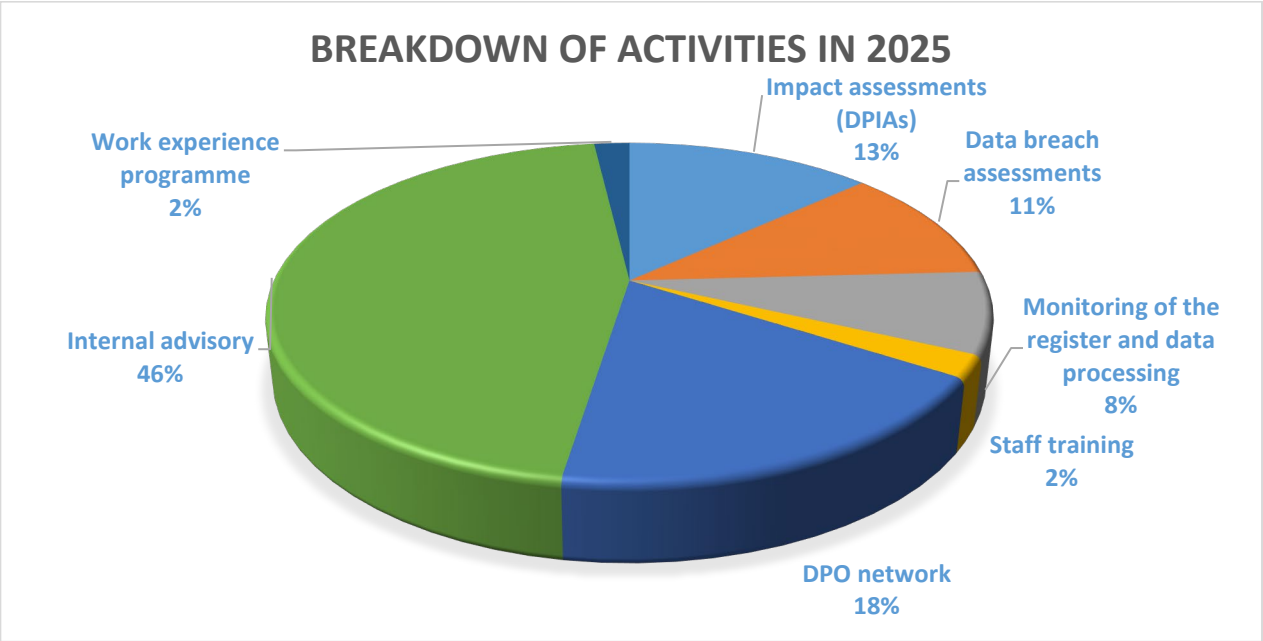
In June 2025, pursuant to Article 37.3 of the GDPR, Banca d'Italia and IVASS designated a single DPO. The appointment is intended to foster meaningful synergies between the two

[1] Legislative Decree 212/2025, Articles 3 and 6. The new provisions also entrust the two institutions with monitoring compliance with the rules adopted within their jurisdictions.

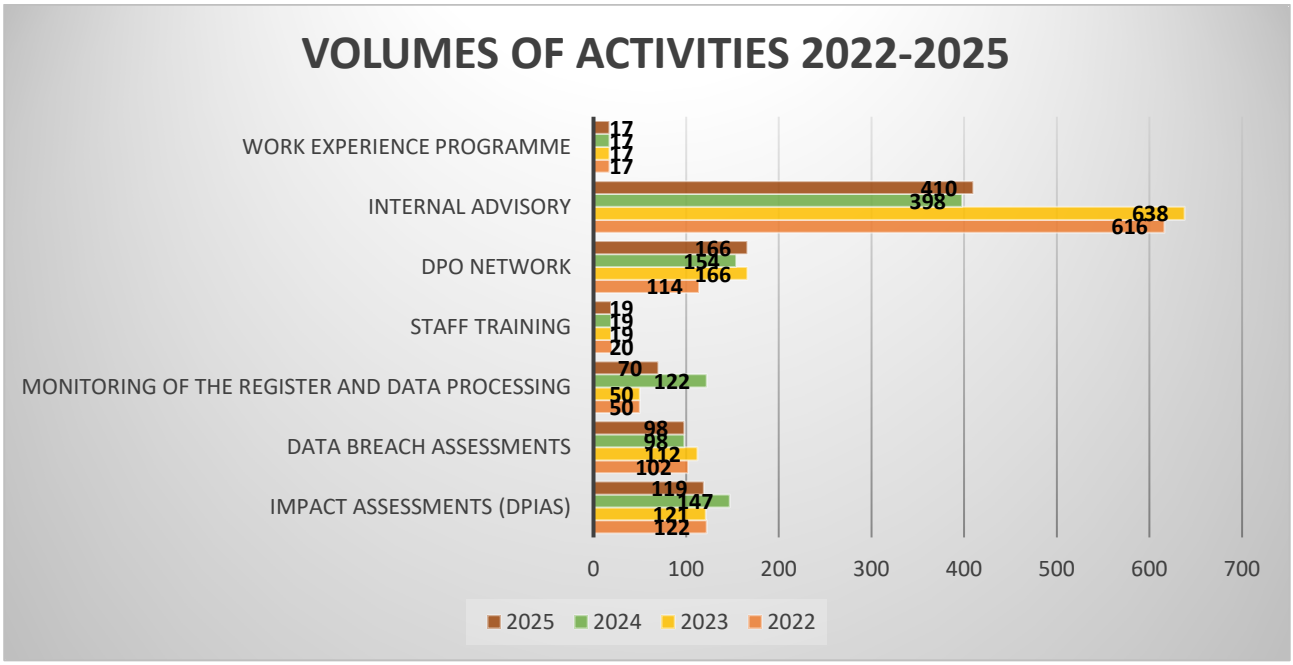
[2] Agreement 700776 of 1 April 2025 between the Organization Directorate and the DPO and his team, supplementing Agreement 1885049 of 30 September 2024 adopted following the organizational reform affecting the DPO and his team.

institutions, reflecting the similarities in their data protection processes, methodologies and operating procedures, as well as their shared commitment to recognizing and safeguarding fundamental rights, including the right to privacy.

The graphs below provide a breakdown of activities carried out in 2025 and a comparison of activity volumes for the period 2022-25.



[§] The quantification of activities is based on data recorded in the ASTRA system.



The work carried out by the DPO and his team is described in detail in the following sections, divided by area of responsibility.

3.1 Participation in the ESCB/SSM DPO Network

Over the course of 2025, the DPO Network of the European System of Central Banks and of the national competent authorities (NCAs) responsible for banking supervision within the SSM, coordinated by the ECB's DPO, met both online and in person at the Deutsche Bundesbank. Through these meetings, as well as written procedures, participants examined a number of issues of common interest:

- coordination activities between the Legal Committee (LEGCO) and the Network of DPOs on personal data protection governance at the European level, following up on the findings of the Internal Audit Committee's report;
- an analysis of the privacy implications of the solutions developed for the various components of the digital euro;
- the ESCB project for a centralized data management platform (Common Data Management, CDM);
- the review of a joint controllership agreement relating to the processing of personal data within the new European Collateral Management System (ECMS);
- the privacy roles of the ECB and the national central banks within the Integrated Reporting Framework (IReF), an ESCB project aimed at developing a single statistical reporting platform;
- a proposed template for a joint controllership agreement to be used in cases involving the ESCB and/or the SSM.

3.2 Participation in the national DPO Network

The Bank‘s DPO participates in the meetings of the DPO Network of the National Independent Authorities,[3] which serves as an interinstitutional forum for discussion of personal data protection issues.

Thanks to contributions from officials of the Italian Data Protection Authority and other authorities, the monthly meetings addressed a number of current issues of common interest, relating to the DPO’s monitoring and advisory activities. These included:

- the opinion issued by the National Anti-Corruption Authority on 30 January 2025 concerning measures that may restrict the collection of personal data from the internet by third parties for the purpose of training generative AI models (web scraping);
- discussions on the National Public Sector Recruitment Portal, governed by the Ministerial Decree of 3 November 2023;

[3] In addition to the Bank’s DPO, supported by his team, this Network brings together the DPOs of several Italian authorities: the Regulatory Authority for Energy, Networks and the Environment (ARERA), the Transport Regulation Authority (ART), the Competition Authority (AGCM), the Companies and Stock Exchange Commission (CONSOB), the National Anti-Corruption Authority (ANAC), the Communications Authority (AGCOM), the Pension Fund Supervisory Authority (COVIP), the Strike Guarantee Commission (CGSSE), the Data Protection Authority (GPDP), the Insurance Supervisory Authority (IVASS), the National Cybersecurity Agency (ACN), the Fund for Energy and Environmental Services (CSEA), the single buyer Acquirente Unico S.p.A. (AU) and the Authority for Children and Adolescents. The DPOs of the Italian National Institute of Statistics (Istat), the Agency for Digital Italy (AgID) and Italy’s group purchasing body (Consip S.p.A.) also participate as observers.

- guidelines for strengthening the resilience of general government, in line with Article 8 of Law 90/2024;
- the seminar organized by the Italian Data Protection Authority on the processing of employees' personal data.

The Network organized a seminar on AI and general government, bringing together the Presidents of the Italian Data Protection Authority, the Agency for Digital Italy (AgID), the National Cybersecurity Agency (ACN) and the Prime Minister's Office Commission on Artificial Intelligence, as well as academics and members of the professional community.

3.3 Cooperation and dialogue with the Italian Data Protection Authority

In 2025, the established cooperation framework with the Italian Data Protection Authority continued to provide valuable opportunities for discussion on issues of common interest. Within this framework, the Bank's DPO participated in the Network of DPOs from the banking sector, the Italian Banking Association (ABI) and Federcasse, coordinated by the Italian Data Protection Authority.

This Network is an institutional forum for examining privacy-related issues affecting the banking and insurance sectors and for coordinating regulatory provisions with a potential impact on the protection of personal data.

With specific regard to promoting privacy compliance in banks' activities, a review was launched of the supervisory provisions currently in force that have implications for access to personal data. The aim was to encourage discussion and shared proposals for strengthening the compliance of employees' access to customers' banking data and for identifying risk mitigation measures.

In preparation for the implementation of Article 75 of Regulation (EU) 2024/1624 (the Anti-Money Laundering Regulation, AMLR), discussions were initiated on partnerships for information sharing (PISs). These are cooperation arrangements between private and/or public entities that may involve the sharing of information on the customers of participating intermediaries, as well as on the transactions they carry out.[4]

3.4 Advisory activities of the DPO

Pursuant to Articles 33 and 35 of the GDPR, the DPO is required to provide advice, mainly through formal opinions (see Sections 3.6 and 3.7) before the start or upon modification of structured processes in the form of data protection impact assessments (DPIAs) and in response to incident reports potentially involving personal data breaches.

[4] This provision, which will apply from 10 July 2027, sets out the substantive and procedural requirements with which such partnerships must comply. It also assigns AML supervisory authorities (in Italy, Banca d'Italia for the financial sector) responsibility for verifying compliance with those requirements and provides, where necessary, for consultation with personal data protection authorities.

In addition to this formal advisory activity, the DPO also provides a considerable number of suggestions and recommendations in response to questions and issues raised by the Bank's organizational units.

With regard to the digital euro project, the DPO and his team continued to contribute to the assessment of privacy-related issues arising from the work of the High-Level Task Force and during the negotiations at the European Commission aimed at defining the regulatory framework for the Proposal for a Regulation on the establishment of the digital euro.

3.5 Monitoring the Register of Processing Activities

Monitoring of the Register of Processing Activities is carried out primarily through periodic reviews of the information entered in the Register.[5] The purpose of these reviews is to verify that the information recorded by the responsible organizational units is relevant, consistent, complete and effective in describing individual processing activities or groups of processing activities, and to recommend any necessary corrections or updates.

A comparison of the Register as at 31 December 2025[6] with the position described in the previous Report shows an overall increase in the number of personal data processing activities, from 223 to 235. This reflects the introduction of new processing activities resulting from new responsibilities assigned to the Bank and from the increasing complexity and digitalization of its work processes.

3.6 Data protection impact assessments (DPIAs)

During 2025, the DPO issued opinions on eight DPIAs relating to IT projects and work procedures under development or review.[7] As these initiatives could pose risks to the personal data of the individuals concerned, appropriate safeguards were introduced to ensure adequate protection.

3.7 Data breach reports

In 2025, 49 potential personal data breaches were identified and submitted to the DPO for assessment, compared with 48 in 2024. For each incident, the DPO provided the data controller

---

5 The maintenance of the Register of Processing Activities is one of the principal obligations imposed on data controllers (and processors) under Article 30 of the GDPR. The Register must be kept in writing, including in electronic form, and must be made available to the Italian Data Protection Authority upon request. In accordance with European guidelines (Article 29 Working Party, Guidelines, 5 April 2017, paragraphs 4.1 and 4.5), the DPO regularly reviews the Register in order to assess the overall effectiveness of the information it contains on the processing activities recorded.

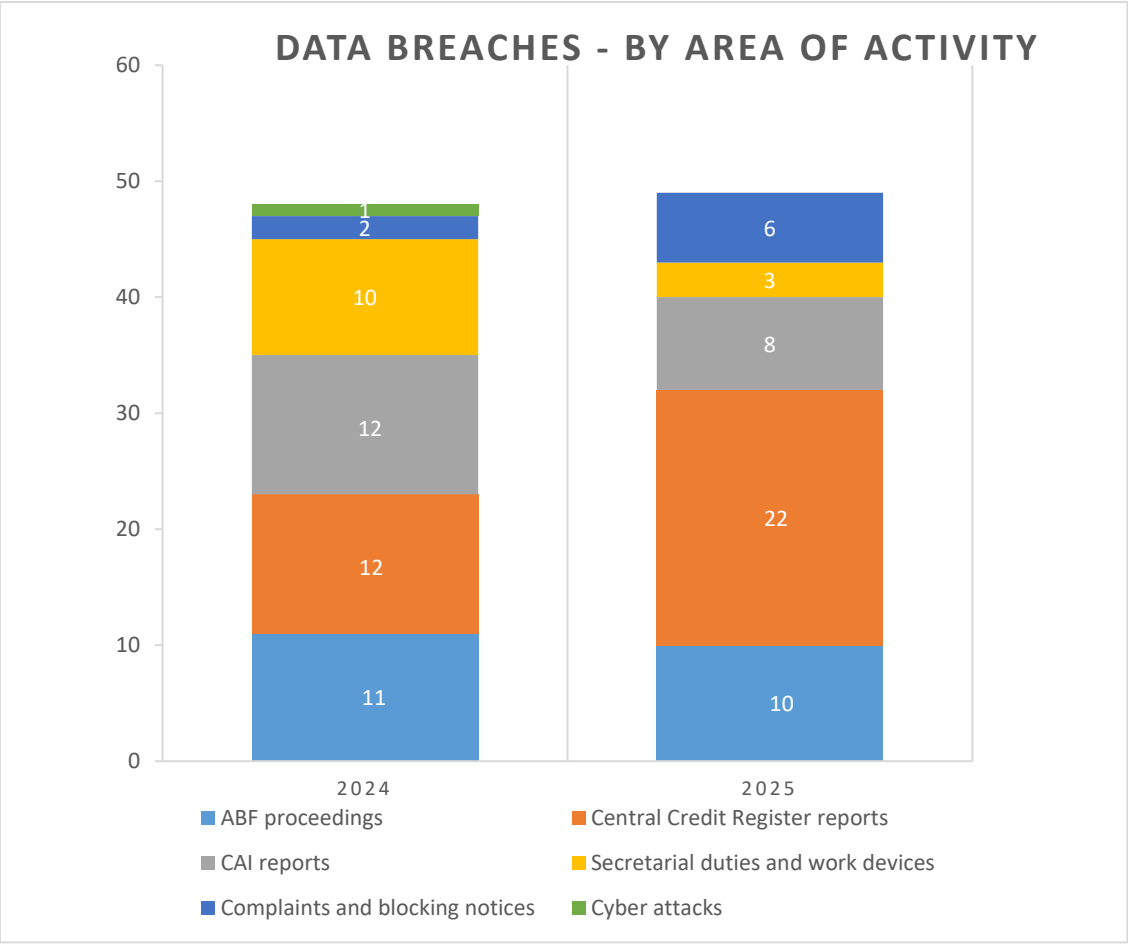
6 To improve efficiency, from 2025 onwards the monitoring period has coincided with the calendar half-year, so as to align it with the reference period used for other assessments of the Bank's activities.

7 Article 35 of the GDPR provides that: '*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [...] The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*' Impact assessments are necessary when the acquisition and management of information involve the processing of personal data of particular importance or on a large scale or with the use of innovative technologies, and in all the cases identified by the Italian Data Protection Authority under Article 35.4 of the GDPR (see Decision no. 467 of 11 October 2018).

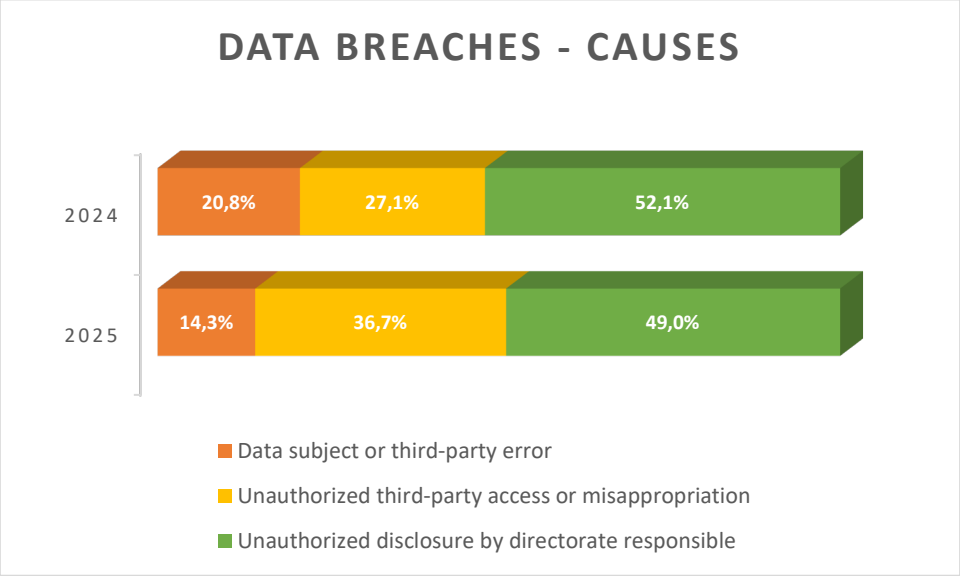
with an opinion on whether the reported event constituted a personal data breach and on the resulting level of risk to individuals' rights and freedoms, for the purposes of any action required under the GDPR.

The risk to the data subjects concerned was considered negligible in all cases. In two cases, the DPO recommended notifying the Italian Data Protection Authority pursuant to Article 33 of the GDPR.

Most of the reported personal data breaches concerned access to the Central Credit Register (Centrale dei Rischi, CR), the handling of proceedings before the Banking and Financial Ombudsman (Arbitro Bancario Finanziario, ABF), and the disclosure of records held in the Interbank Register of Bad Cheques and Payment Cards (Centrale di Allarme Interbancaria, CAI).



Just over half of the breaches were attributable to negligent or malicious conduct by data subjects or by third parties. The remainder resulted from operational errors made by Bank staff in communications with external parties.



3.8 DPO awareness-raising initiatives

As part of its oversight responsibilities regarding the application of data protection legislation, the DPO promoted an awareness-raising campaign, organized in collaboration with the Bank's Directorate General for Information Technology, on the evolving cyber threat landscape and the protection of personal data in the digital age. The campaign highlighted the importance of adopting informed behaviours and the need to ensure that the protection of personal data is taken into account from the design stage of IT platforms and systems.

The DPO also held a number of meetings involving staff from several organizational units and from IVASS, during which the principles of data protection legislation and the safeguards for reducing the risk of personal data breaches in the workplace were presented.