Data Protection Officer's Report

2024

Rome, May 2025

BANCA D'ITALIA
EUROSISTEMA

CONTENTS

1. Background

1.1 Scenario and challenges

The current scenario, marked by widespread geopolitical conflicts, is one in which there are heightened threats that could compromise the availability, integrity and confidentiality of information assets owing to pervasive technological change, particularly the growing use of artificial intelligence software integrated into objects, common applications and decision-making processes.

The combined effect of these phenomena, if not adequately controlled and mitigated, may pose a serious threat to the rights and freedoms of individuals, thereby requiring the institutions involved to continue to step up their commitment to protection and the individuals themselves – both on their own behalf and as members of an organization – to become more aware of personal data protection issues.

Analysis of the most recent developments shows that the significant increase in personal data breaches can be traced, not just to deliberate actions by malicious actors who exploit inadequately protected vulnerabilities in systems, but also to the behaviour of the data subjects themselves who, often not suitably aware of the risks associated with using technological devices, unknowingly contribute to the theft of their personal data.

The complexity of the risk scenario outlined demonstrates that the Data Protection Officer's (DPO) monitoring duties cannot be limited to just verifying the compliance of personal data processing activities but, in order to keep up with the expansion in information technology, it must take an interdisciplinary approach, focusing on the organizational and security aspects of the gradual digitalization of operational processes and the greater outsourcing of services.

At the same time, effective privacy protection requires the Data Controller and the DPO to 'stay ahead of the game' by taking a holistic and proactive approach to integrating personal data protection considerations into preliminary stages of reorganizing the directorates' operational processes and identifying security measures that address the new and more complex risk factors posed by evolving technology.

In this scenario, in which previously unidentified threats could emerge, people's awareness of personal data protection issues and their behaviour are critical to mitigate the risks. Alongside improving system and process resilience, it is therefore necessary to provide ongoing, adequate training for staff to raise their awareness of the risks associated with personal data processing and to encourage careful behaviour.

1.2 Developments in the regulatory framework

In recent years, a considerable amount of European legislation has been enacted to standardize the regulation of the effects of the digital uptake in different sectors of the economy and society, as well as in everyday life.

This legislation, which intersects in many ways with the personal data protection rules, does not undermine the application of Regulation (EU) 2016/679 (General Data Protection

Regulation - GDPR) and of national implementing law. Moreover, the legal bases for the processing and flow of personal data remain solely those established by the GDPR.

Furthermore, there remains a gap between the European scope of the regulations and the jurisdictions that regulate data protection and the non-European scale of the large digital information management platforms. Likewise, additional uncertainty may arise from how much importance is given to privacy protection by non-European countries[1] .

1.3 Regulating artificial intelligence

On 1 August 2024, Regulation (EU) 2024/1689 (AI Act[2]) became applicable, with a view to laying down harmonized rules and systematic guidelines on artificial intelligence (AI) in order to ensure that AI is developed in a safe, ethical and reliable manner, balancing the protection of personal data with the use of the information assets to enable AI systems to operate.

The regulation takes a risk-based approach, classifying AI systems according to the harm they may cause to the fundamental rights and freedoms of users. Based on this classification, different rules apply for market authorization and supervision, the disclosure and transparency obligations towards users, and the minimum technical requirements for ensuring continuous human oversight and quality data for training AI systems in order to prevent discrimination and bias from affecting the output.

The new AI Act overlaps significantly with the GDPR, partly for the obvious reason that if AI systems are trained and developed using data on natural persons, it does follow that a legal basis for their processing is required.

In the early months of 2025, Banca d'Italia, in its dual role as an entity interested in the responsible, fair and efficient use of AI technologies and systems and as the future Market Surveillance Authority (MSA) for AI, established an internal Sub-Committee on Artificial Intelligence, a cross-organizational body for the unified governance of the development initiatives undertaken by the Bank's various functions.

1.4 The DPO's tasks

In 2024, the Data Protection Officer performed his tasks[3] by focusing on monitoring compliance with privacy regulations and providing advice to the directorates and users, with the aim of protecting the confidentiality, integrity and availability of personal data.

---

[1] For example, the 2023 EU-US Data Privacy Framework (DPF) (Decision pursuant to Article 45 of Regulation (EU) 2016/679, adopted on 10 July 2023), intended to regulate transatlantic data transfers between the European Economic Area and the United States, might be called into question following recent US policy stances favouring standards that are less restrictive and more conducive to the free movement of data. On that point, see the speech by Agostino Ghiglia, a member of the Italian Data Protection Authority, entitled, *'Dati Usa-Eu, terremoto Trump: ora è rischio caos su diritti e servizi'.*

[2] The regulation will be rolled out gradually. On 2 February 2025, the rules on prohibited AI practices entered into force. The rules on general-purpose AI models and multi-stakeholder governance by the European Commission (via the European AI Office), representatives of the Member States and the national market surveillance authorities for the various sectors concerned, will come into force on 2 August 2025. The rest of the regulation, including the rules on limited- and high-risk AI systems, will become applicable on 2 August 2026.

[3] The DPO's tasks are set out in Article 39 of Regulation (EU) 2016/679 (GDPR) and consist of advising, monitoring in relation to data protection and acting as a contact point for the Italian Data Protection Authority.

The DPO's work was conducted within the framework of the guidelines provided by the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) at national level and the European Data Protection Board (EDPB) at European level, as well as being based on research conducted by the Network for the DPOs of the European System of Central Banks (ESCB) and the Single Supervisory Mechanism (SSM), in addition to the national network of DPOs of the various Italian authorities.

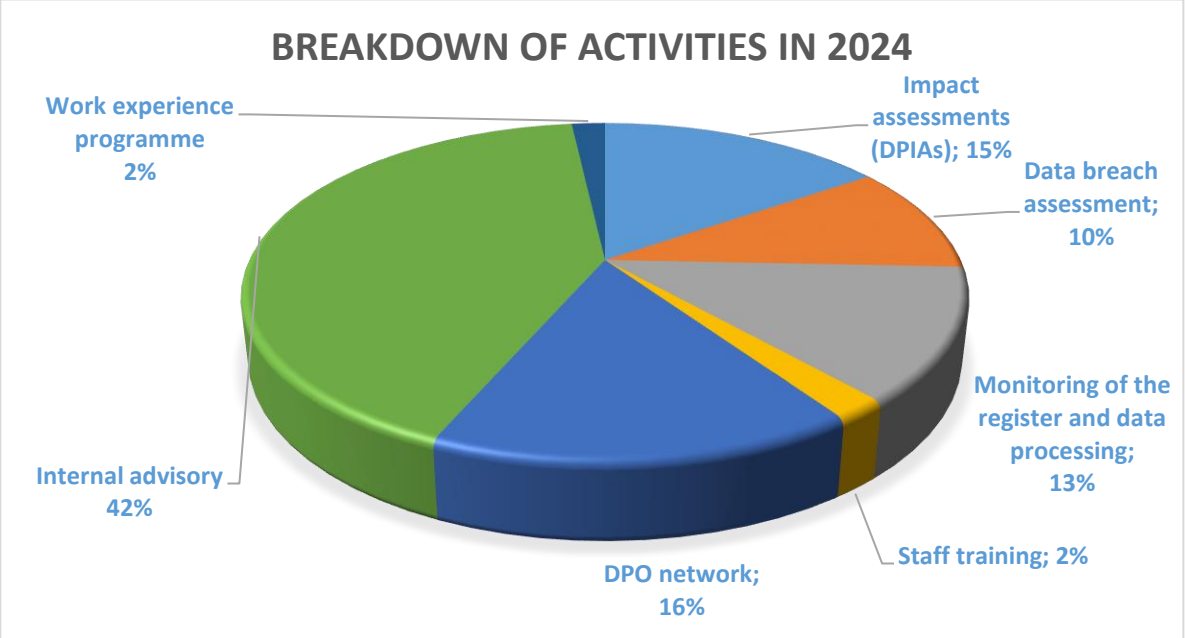
2. Activities carried out in 2024

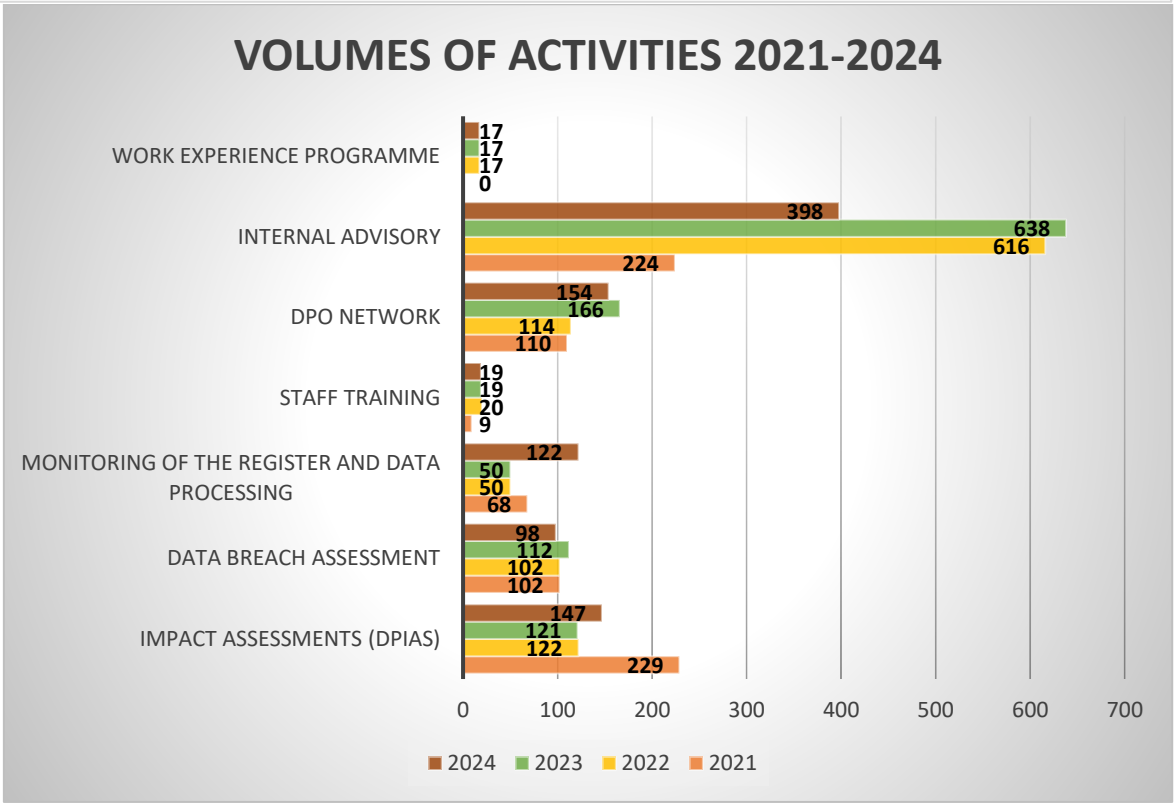
During the year, the DPO and his staff were moved to the Directorate General for Planning, Organization and Accounting. This organizational transfer does not compromise the DPO's independence and impartiality in any way.

The purpose of this change was to enable the DPO to collaborate more closely and efficiently with the Organization Directorate which, in addition to being the Data Controller, is also responsible for promoting the Bank's organizational development by fostering innovation and simplifying the processes and related regulations. This new placement of the DPO lends further impetus to the principle of privacy by design, as it makes it possible to take into account, as early as the planning stage, the implications of changes in organizational structures, regulations and work processes for the protection of personal data. In a similar vein, the DPO participates in the meetings of the IT Committee.

On the whole, more time was devoted to monitoring the Register of Processing Activities, while total internal advisory activities decreased because, despite there being an increase in the amount of work linked to preparations for the digital euro, they required less commitment than was needed in the two years prior, when the DPO's staff took part in the support teams for the winners of the Milano Hub calls for proposals. The volume of activity remained broadly stable in the remaining areas.

The following graphs provide a breakdown of activities in 2024 and a comparison of the volumes for the period 2021-2024.





2.1 Participation in the ESCB/SSM DPO Network.

Over the course of 2024, the meetings of the Network of DPOs of the ESCB Central Banks and the national competent authorities (NCAs) for SSM banking supervision, coordinated by the European Central Bank (ECB), held online and in person at Banco de España, focused on analysing the following issues of common interest:

- privacy protection issues arising in the course of preparations for the digital euro;
- the decisions taken by the European Data Protection Supervisor (EDPS) based on the analyses performed on the Microsoft Dynamics 365 software used by the European Commission and the ECB, specifically on the measures needed to ensure that the data transferred outside the EU/European Economic Area (EEA) receive the same degree of protection as that provided by the GDPR;
- joint controllership agreements between the national central banks and the ECB involving the management of personal data as part of the prudential supervision of credit institutions;
- the debate on the use of AI by European institutions under the regulatory framework introduced by the AI Act (see above) and the prospect of making it compliant with the GDPR; and
- taking stock of lessons learned and future developments after the first five years of application of the GDPR and EUDPR (Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by EU institutions).

2.2 Participation in the national DPO network

The Bank's DPO participates in the meetings of the Network of DPOs of the National Independent Authorities, which serves as an interinstitutional forum for discussion of personal data protection issues.[4]

The main topics discussed, often conducted with the help of university professors and officials from the Italian Data Protection Authority and other authorities, covered various aspects involving the DPO's monitoring and advisory tasks. In particular, during the monthly meetings:

- they analysed how to monitor cyber risk, with the help of recognized national experts;
- with representatives of the Italian Data Protection Authority, they examined some aspects of the application of the rules on the processing of employees' personal data;
- the legislation transposing the Network and Information Systems (NIS2) Directive was analysed with the assistance of staff from the National Cybersecurity Agency.

2.3 Cooperation and dialogue with the Italian Data Protection Authority

The Bank's DPO continued to cooperate throughout the year with the Italian Data Protection Authority on issues of common interest through the Authority's network of banking sector DPOs and those of ABI and Federcasse.

This network provides an important forum for further exploring privacy issues in the banking sector and coordinating any initiatives to harmonize the regulation of activities that involve personal data protection.

[4] The network was set up in accordance with the guidelines of the Italian Data Protection Authority for DPOs in the public sector (Decision no. 186 of 29 April 2021, paragraph 8), and is governed by the rules on the organization and functioning of the network of DPOs of the independent administrative authorities adopted on 24 September 2021.

2.4 Advisory activities

Pursuant to Articles 33 and 35 of the GDPR, the DPO is required to provide advice, mainly through formal opinions (see Sections 2.6 and 2.7) 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.

In addition to this formal advisory activity, the DPO also provides a considerable number of suggestions and recommendations in answer to questions or problems posed by the directorates.

This includes reviewing the privacy clauses contained in agreements or protocols to be signed with public bodies for the performance of institutional tasks. The DPO and his staff contributed further to the project for the creation of a digital euro by analysing privacy issues for the High Level Task Force and for the representatives involved in negotiations at the European Commission to set out the regulatory framework under the 'Proposal for a Regulation on the establishment of the digital euro'.

2.5 Monitoring of the Register of Processing Activities

The Register of Processing Activities is monitored primarily by periodically checking the information contained therein[5] to verify the relevance, consistency, comprehensiveness and effectiveness of the descriptions of the personal data or of the groups of processing operations recorded by the directorates concerned and to encourage them to make any corrections or additions.

A comparison of the information in the Register at 31 December 2024 with that for the prior year shows that the total number of personal data processing operations increased from 209 to 223.

There was an overall improvement in the data quality of the Register due to the addition of more processing descriptions (privacy notices, preliminary assessments conducted, data processor instructions, retention periods).

2.6 Data protection impact assessments (DPIAs)

In 2024, the DPO provided an opinion on 12 data protection impact assessments connected with IT projects or working procedures to be studied or reviewed[6] which, in potentially

5 The Register has to be maintained as set out in Article 30 of the GDPR and is among the main tasks of the Data Controller (and of the Data Processor). The Register must be kept in written form, including electronic form, and must be made available on request to the Italian Data Protection Authority. According to the European Guidelines (Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')', 5 April 2017, paragraphs 4.1 and 4.5) for monitoring compliance with the GDPR, the DPO regularly checks the Register to assess its overall effectiveness in providing information on the processing operations recorded.

6 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

exposing the personal data of the natural persons concerned, required the introduction of adequate safeguards.

2.7 Reports of data breaches

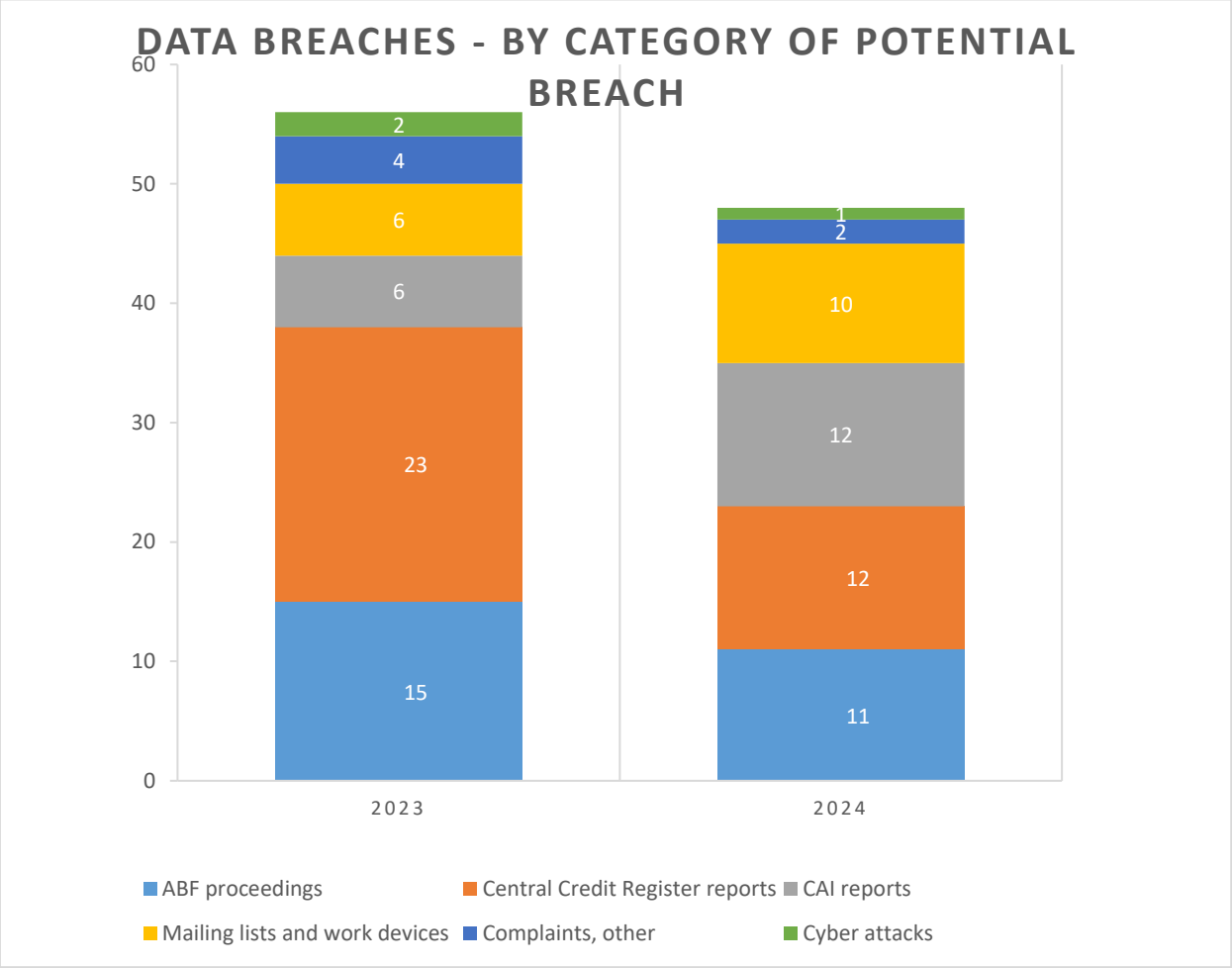
In 2024, a total of 48 potential data breaches were detected and submitted to the DPO for assessment (compared with 56 in 2023). For each event, the DPO provided an opinion for the purposes of communicating under the GDPR about whether there really was a data breach and about the impact of the consequent risks on the rights and freedoms of natural persons.[7]

The risk assessment of the breaches led to one case,[8] which involved an intentional and malicious action by a third party being reported to the Italian Data Protection Authority, pursuant to Article 33 of the GDPR. The graph below shows the number of data breaches recorded in 2023 and 2024 for each area of activity.

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 pursuant to Article 35.4 of the GDPR (see Decision no. 467 of 11 October 2018).

7 The DPO provides an opinion to the Data Controller in cases of loss, alteration or misuse (accidental or unlawful) of personal data amounting to a data breach. Should a data breach be found, Article 33 of the GDPR requires the Data Controller to notify the Italian Data Protection Authority not later than 72 hours after having become aware of it (unless there is a reason for the delay if the notification cannot be made within that strict time limit), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons When, subsequently, the breach poses a high risk to the rights and freedoms of data subjects, the Data Controller shall communicate the breach to the data subjects without undue delay (Article 34).

8 It was a cyber-attack on a service provider carried out by exploiting a zero-day vulnerability.



Most of the breaches were caused by operational errors in communications by the directorates and negligence by data subjects or third parties. In a small number of cases, the data breaches were caused by malicious attacks.