BANCA D'ITALIA
EUROSISTEMA

Data Protection Officer's Report

2023

Rome, May 2024

CONTENTS

Introduction

In 2023, the Data Protection Officer's (DPO) advisory and monitoring efforts[1] helped support the gradual digital transition of the Bank's processes and products.

The DPO is focused on the risks stemming from the advent of new technologies, the offshoring and internationalization of activities, which involves cultivating a more comprehensive technological understanding to be able to assess privacy risks and to develop systems and applications that ensure adequate protection by design.

This contributes to solidifying the DPO's reputation and perception of reliability in the Bank of Italy.

* * *

1. The legislative framework

The *Proposal for a Regulation on the establishment of the digital euro* was published in June 2023 as part of the digital euro project. As concerns privacy compliance, the stated objective of the Proposal is to ensure a high level of privacy in payments in line with EU personal data protection legislation (Regulation (EU) 2016/679 and Regulation (EU) 2018/1715).

Also of great importance was the European Commission's adoption on 10 July 2023 of the adequacy decision on the EU-US Data Privacy Framework (DPF)[2] which aims to regulate transatlantic flows of personal data and to overcome the objections raised by the Court of Justice of the European Union in the *Schrems II* judgment of July 2020.

In addition, mention should be made of:

- at European level, the approval by the European Parliament and the Council of the Regulation laying down the legal framework on artificial intelligence (the 'Artificial Intelligence Act');
- at national level, the approval of Law 193/2023 on the right of former oncological patients to not disclose or answer questions about their medical history (so-called 'cancer survivors' right to be forgotten').

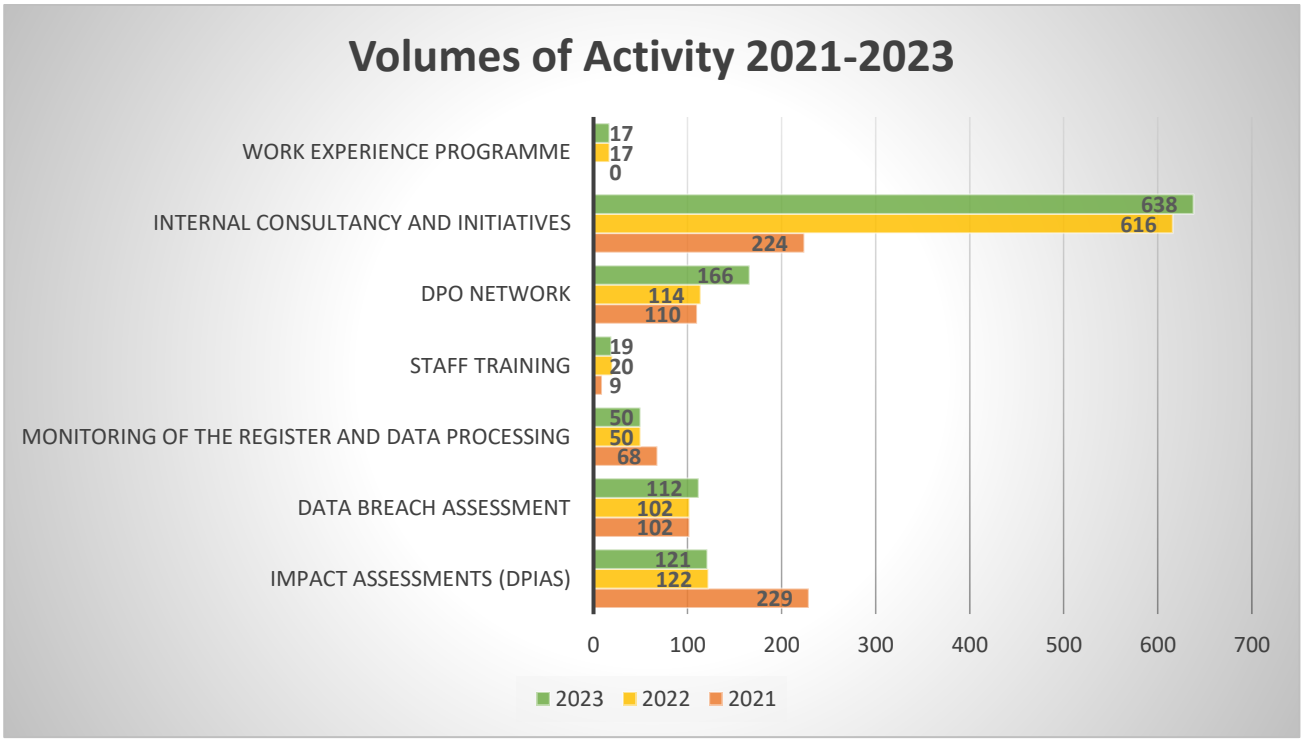
[1] See Article 39 of Regulation (EU) 2016/679 (GDPR).

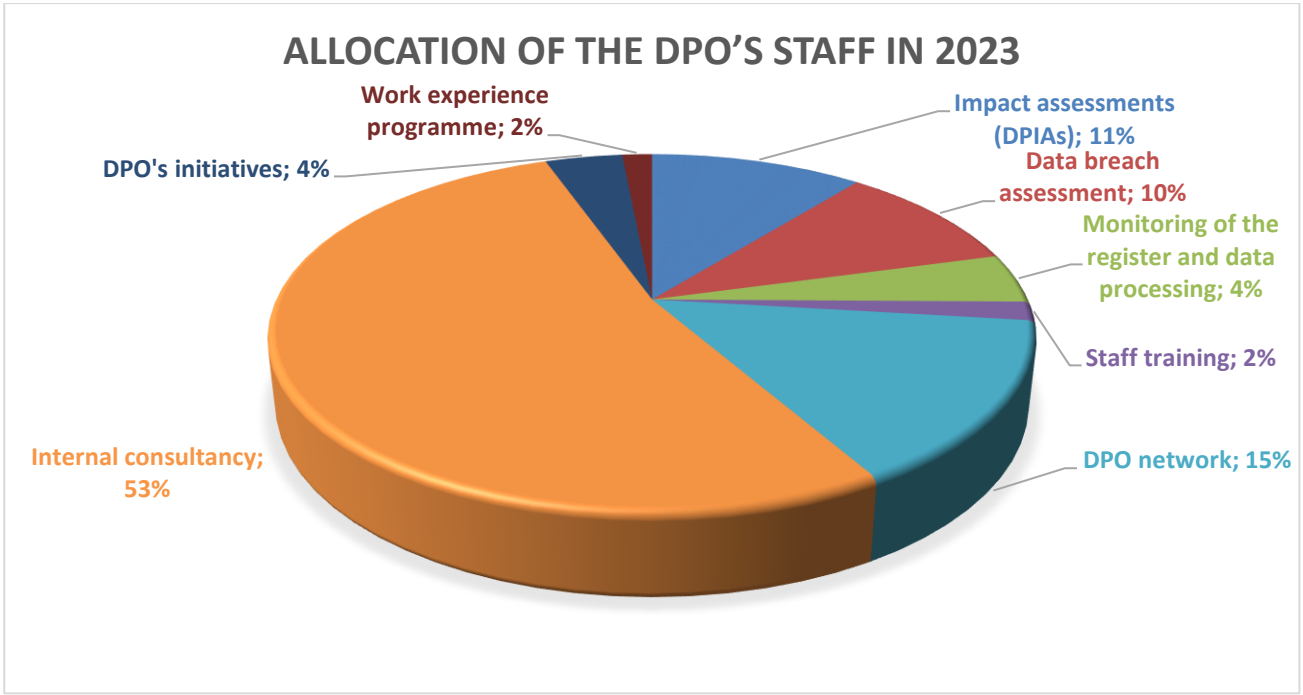
[2] The EU-US DPF is based on a system of certification by which US organizations commit to a set of privacy principles indicated in the decision. These certifications, to be renewed annually, are subject to the investigatory and enforcement authority of the US Federal Trade Commission (FTC) or the US Department of Transportation (DoT), as well as a number of obligations including deletion of personal data when they are no longer necessary for the purpose for which they were collected, continuity of protection when personal data are shared with third parties, equivalent level of protection for special categories of data, special rules for so-called 'onward transfers', i.e. transfers of personal data from an EU-US DPF certified organization to a third party controller or processor, irrespective of whether the latter is located in the United States or in a third country outside the US (accountability for onward transfers).

2. Activities carried out in 2023

In 2023, the DPO continued to gradually expand the function of providing advice to the directorates and engaging in dialogue with external parties in specific national and European networks. There was also emphasis on specialized training for the DPO's staff.

The following graphs show the volumes of the DPO's activities according to the company management system.





2.1 Cooperation and dialogue with the Italian Data Protection Authority

During the year, the Data Protection Authority focused on the figure of the DPO, the safeguarding of the DPO's duty to monitor compliance with personal data processing rules and the DPO's ongoing involvement in the activities of data controllers. The Privacy Authority intended to resume dialogue with public and private sector DPOs to take stock of the experience they have gained in the five years since the GDPR took effect and to identify areas requiring intervention to strengthen the role of the DPO.[3]

Also during the year, the network of banking sector DPOs, of which the Bank is part, continued to collaborate, coordinated by the Privacy Authority. The network set up a permanent working group to study business phenomena and coordinate initiatives to harmonize the regulation of activities involving the protection of personal data.

2.2 Consultancy activities

The DPO advises the directorates on how to apply the privacy rules by formulating opinions on data breaches and data protection impact assessments pursuant to Articles 33 and 35 GDPR, offering suggestions and recommendations on the issues raised by the directorates, in constant collaboration with the Organization Directorate.

In many cases, consultancy activity involved reviewing the privacy clauses contained in agreements or protocols to be finalized with public bodies that are necessary for the performance of institutional tasks.

The DPO's consultancy activity during the year dealt with numerous other specific issues on which the various directorates sought the opinions or guidance of the DPO in collaboration with the Organization Directorate (e.g. privacy notices connected with the activities of the branch network; documentation for the appointment of medical staff; questions about the legal grounds and data storage periods for specific processing activities; privacy issues involving with external providers acting as data processors; compliance with the legal grounds for requiring impact assessments; questions on disposing off digital documentation; and business privacy risk assessment methods).

2.3 Monitoring of Register of processing activities

The DPO's monitoring of the Bank's Register of processing activities in 2023 focused on periodically checking the information contained therein[4] to verify the comprehensiveness and consistency of the descriptions of the processing operations recorded by the directorates concerned (209 as at 31 December) and to encourage them to make any corrections or additions.

It was found that:

- the number of processing operations decreased slightly (from 215 to 209) as a result of the redefinition of the scope of the processing for which the various directorates are responsible;

[3] The Privacy Authority has always paid close attention to the strategic function of the DPO, in particular in promoting compliance with privacy rules within organizations, and to the DPO's ability to serve as value added within the organization.

[4] Article 30 GDPR.

– the internal distribution of processing operations is highly uneven and is especially concentrated within the Directorate General for Human Resources and Information, and in the Directorate Generals for Markets and Payments Systems and for Financial Supervision and Regulation (104 processing operations in total);
– the quality of the information recorded continues to improve as a result of further clarification on the mandatory items to be included in the descriptions, such as the procedures for issuing privacy notices and guidelines on data storage periods.

Overall, this points to the directorates taking greater care in keeping records of their processing operations, leading to an improvement in the quality of the information contained in the Register.

Finally, the DPO, along with the Organization Directorate, conducted a review of the Register, updating the list of circumstances in which the Bank processes personal data owned by other public administrations with which it has signed inter-institutional collaboration agreements.

2.4 Data protection impact assessments (DPIAs)

In 2023, the DPO provided an opinion on eight data protection impact assessments (DPIAs) for processing operations relating to IT projects or work processes being studied or revised that could potentially expose natural persons to risk.[5]

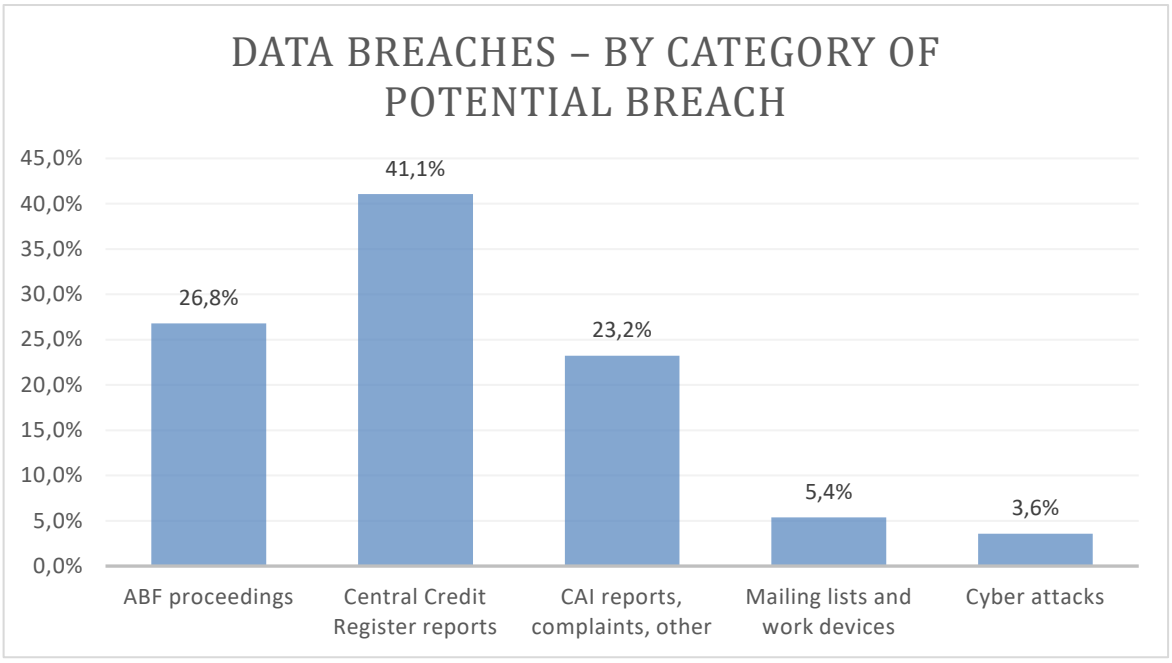
2.5 Reports of data breaches

In 2023, 56 data breaches were detected and reported. The DPO provided, for each event, an opinion on whether there was really a data breach and the impact of the consequent risks on the rights and freedoms of natural persons, for the purposes of communication under the GDPR.[6]

As in the previous year, reports of breaches were most concentrated in the areas of access to the Central Credit Register, followed by management of ABF proceedings. Incidents involving the communication of CAI reports, the handling of complaints regarding banks, and the use of mailing lists were less frequent. The risk of attempted cyber attacks, due to the potential harm they could cause, showed up for the first time this year time among potential data breaches (see the graph below).

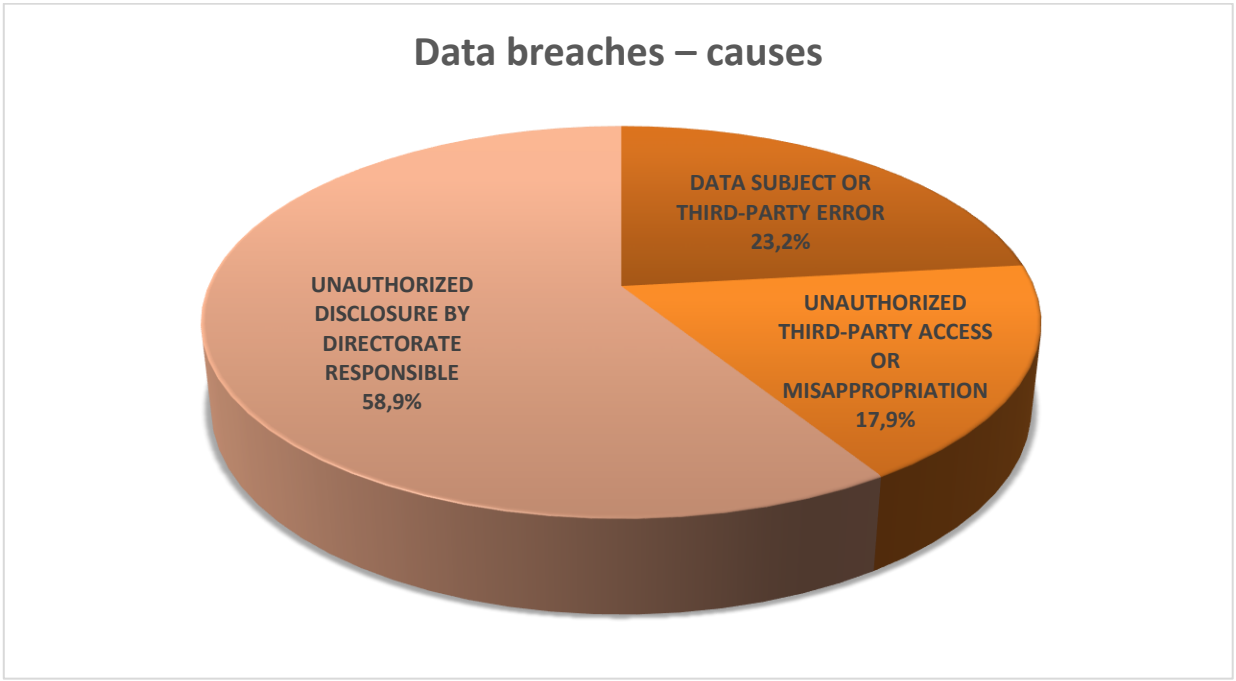
[5] Article 35 GDPR.

[6] Article 33 GDPR.



'Other' includes cases of data breaches occurring in the course of the Bank's various activities, including, by way of example, administrative activities relating to secretarial duties and court orders.

Among the causes of breaches, operational error in communication by the directorates is the main one, followed by those made by data subjects or third parties and by wilful misconduct carried out by malicious actors (see the graph below).



2.6 DPO's initiatives

The DPO can also, on his own initiative, request that checks and, where necessary, assessments be performed to improve the overall compliance of the directorates.

The 14 projects selected for Milano Hub in response to the 2022 Call for Proposals, which focused on the application of distributed ledger technology (DLT) to banking, financial, insurance and payment services, also made use of a cross-sector team on privacy consisting of the Organization Directorate, the Legal Services Directorate and the DPO's staff.

3. Participation in DPO networks

3.1 International activity

In meetings held throughout the year, the Network of DPOs of the national central banks and of the national competent authorities for banking supervision, coordinated by the European Central Bank (ECB), began discussions that focused mainly on four issues of common interest:

- issues that arose during the investigation phase on the issuance of a digital euro relating to privacy concerns and the interest shown by the public in maintaining their confidentiality in carrying out transactions, which was viewed as the second most important factor, after security;
- issues that arose from the use of Microsoft Dynamics 365-based software for the communications and document sharing system;
- issues related to data sharing within the Eurosystem under joint controllership agreements involving the management of personal data in the context of the prudential supervision of credit institutions under the Single Supervisory Mechanism (SSM) and the ECB.

3.2 National activity

The activity of the Network of DPOs of the National Independent Authorities,[7] of which the Bank's DPO is part, began in January 2023 with the meeting held at the Bank's Conference Centre.

The Bank's DPO introduced some topics of clear interest to the network in the new year:

- the rising awareness of cyber security;
- the application of artificial intelligence, in particular in the world of finance.

The following topics were discussed in the regular meetings:

[7] In addition to the Bank of Italy's DPO, the Network includes the DPOs of the Italian Regulatory Authority for Energy, Networks and Environment (ARERA), the Italian Transport Regulation Authority (ART), the Italian Competition Authority (AGCM), the Italian Companies and Stock Exchange Commission (CONSOB), the National Anti-Corruption Authority (ANAC), the Italian Communications Authority (AGCOM), the Italian Pension Fund Supervisory Authority (COVIP), the Italian Strike Guarantee Commission (CGSSE), the Italian Data Protection Authority (GPDP), the Italian Insurance Supervisory Authority (IVASS), the Italian National Cybersecurity Authority (ACN), the Fund for Energy and Environmental Services (CSEA) and Italy's single buyer Acquirente Unico S.p.A. (AU), the Authority for Children and Adolescents (AGIA), as well as the DPO of the Italian National Institute of Statistics (ISTAT) as an observer.

- the use of tracking/monitoring tools offered by third-party providers in configuring public administration websites and digital services, with regard to the associated risk of transferring data outside the European Economic Area;

- the results of the survey launched by the EDPB under the Coordinated Enforcement Framework (CEF) on the use of cloud-based services by the public sector.

On 24 November 2023, the Network of DPOs organized a seminar, hosted by the Italian Competition Authority, on 'The principle of privacy by design and by default in the Public Administration', during which presentations by the Privacy Authority, the President of the National Anti-Corruption Authority (ANAC), and representatives of the National Cybersecurity Authority (ACN) and the National Institute of Statistics (ISTAT), further explored data processing design according to the principles of the GDPR, digitalization in the new Public Contract Code, the Cyber Resilience Act and the processing of personal data using artificial intelligence in the public administration and in official statistics.