BANCA D'ITALIA
EUROSISTEMA

Data Protection Officer's Report

2022

Rome, March 2023

CONTENTS

Introduction

In 2022, the scenario for the protection of personal data and for the monitoring activities of the Data Protection Officer (DPO) grew more complex.[1]

In the public sector, in particular, the widespread digitalization of processes, activities and interactions with the public is proceeding at an ever-faster pace, with a rising volume of data exchanged and the consequent need for compliance with the personal data processing rules.

* * *

1. The legislative framework

Last year marked the start of a busy season for EU regulation of the digital world and the use of data (personal and otherwise), effective as from 2023[2] and paving the way for the necessary coordinated application of the new rules with the GDPR.[3] Specifically:

- Regulation (EU) 2022/868 on European data governance establishes the regulatory framework to allow firms to reuse certain categories of public sector data where justified and necessary to provide a service in the general interest;
- Regulation (EU) 2022/1925 on digital markets governs the activity of so-called 'gatekeepers', i.e. undertakings that provide online intermediation services of various sorts (e.g. search engines, social networks, video-sharing platforms, web browsers, cloud computing or online advertising) and that owing to their size and operations serve as a gateway for digital connectivity and can control access to the digital market;[4]
- closely connected with this regulation is the newly enacted Regulation (EU) 2022/2065 on other digital intermediary services (for example, online marketplaces, content-sharing platforms, online travel and accommodation platforms, app stores and social networks), which, inter alia, regulates liability for the use of intermediated data and also calls for the establishment of the corresponding national supervisory authorities.

---

1 The Managing Director for Internal Audit, who, owing to the nature of the post he occupies, maintains an impartial stance with respect to all other business activities and departments, serves as the Bank's DPO. The DPO's tasks are set out in Article 39 of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) and consist of providing advice, monitoring data protection compliance and liaising with the Italian Data Protection Authority (*Garante per la protezione dei dati personali*), the national competent authority pursuant to Article 51 of the GDPR.

2 Application of EU regulations is usually deferred to a date after their formal entry into force in order to give the various Member States time to comply with them.

3 This is particularly true in relation to the hierarchy of regulations, the harmonization of the forms of protection of the fundamental rights and freedoms of individuals and the coordination of the various supervisory activities by the supervisory authorities involved.

4 More specifically, the regulation forbids gatekeepers to combine personal data from core platform services with personal data from any other services provided by the gatekeeper or with personal data from third-party services unless the end user has given their specific consent. Furthermore, it provides that it should be easy for the end user to modify or withdraw consent.

2. Activities carried out in 2022

There was a marked increase in providing advice to the Bank's directorates through programmes and projects that required an analysis of personal data processing issues, including in connection with dealings with other public administrations, as well as through the participation in two support teams formed to follow the development of projects selected by Milano Hub from its Call for Proposals 2021, and through a greater dialogue with the Italian Data Protection Authority.

The DPO continued to assess reports of potential personal data breaches by reconstructing the events leading up to them to determine whether a breach occurred[5] and to participate in the networks built with the DPOs of the national independent authorities and between the DPOs of the national central banks and national competent authorities (NCAs) within the ESCB.

The DPO also formulated opinions to accompany data protection impact assessments (DPIAs),[6] pertaining mainly to the concentration and development of IT projects that involve managing personal data. In addition, the DPO monitored the Bank's processing of personal data, focusing primarily on the structure and consistency of the reporting by the directorates, drawing on the record of processing activities referred to in Article 30 of the GDPR.

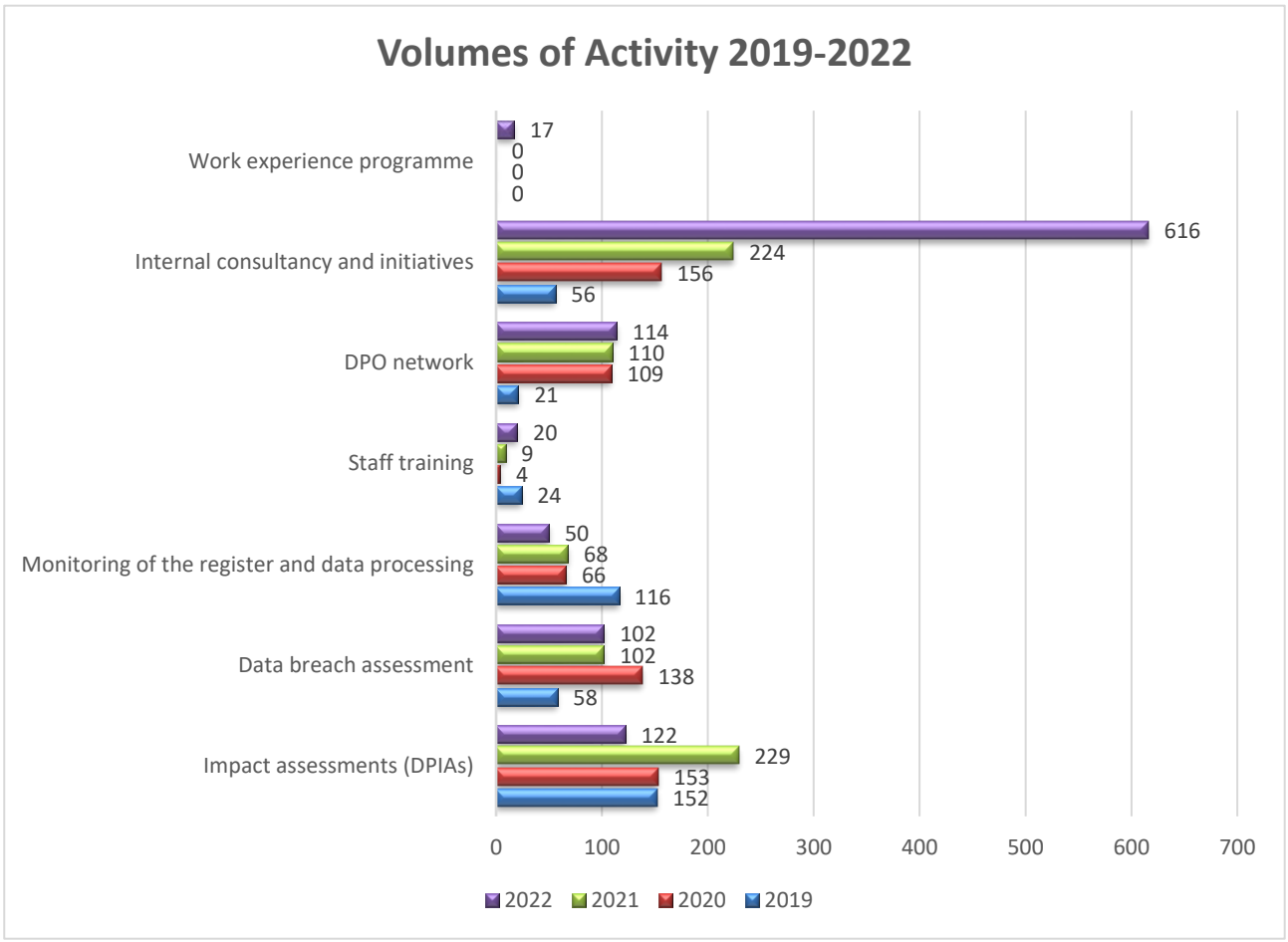
There was an increase in the specialized training provided to the DPO's staff in 2022 to take account of the changes in the environment in which they perform their advisory and monitoring tasks. Finally, for the first time the DPO's staff hosted a group of Rome high school students, from 13 to 17 June 2022, as part of the Bank's work experience programme (*Percorsi per le competenze trasversali e per l'orientamento* - PCTO) for the 2021-22 academic year.

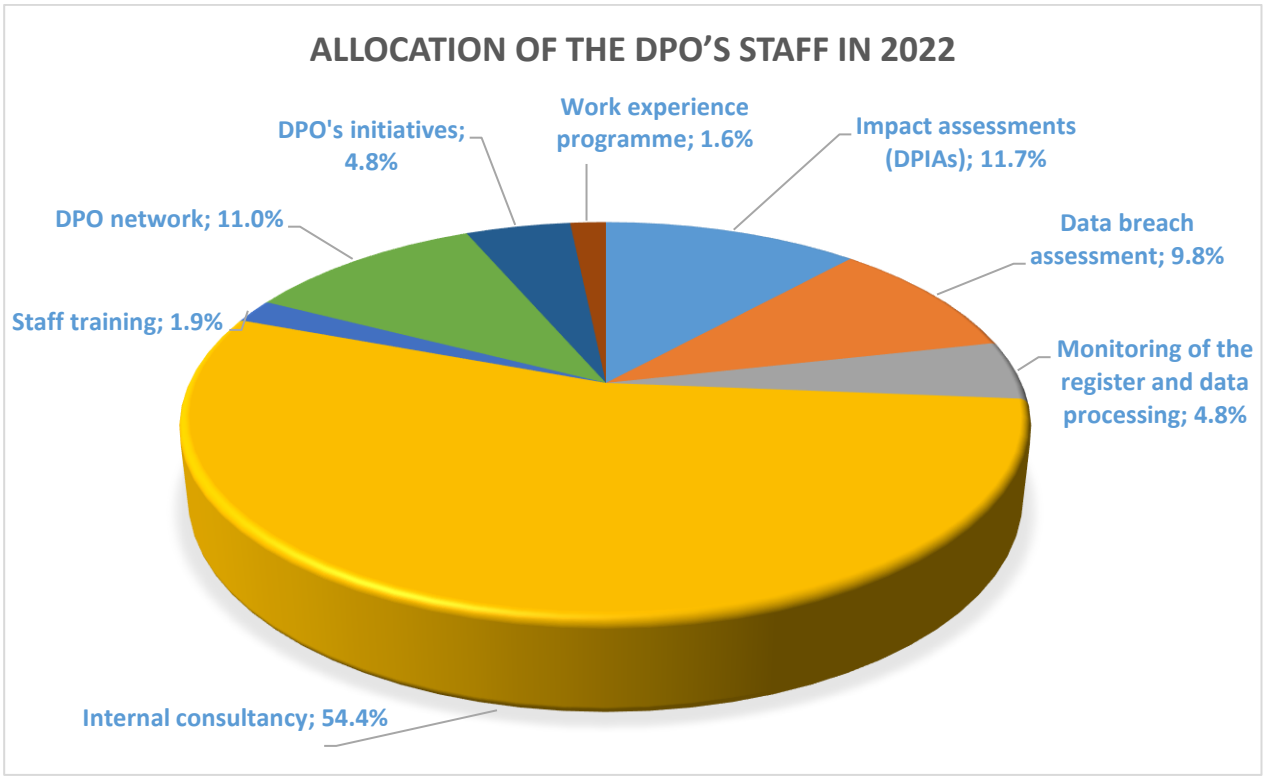
The following charts show the volumes of the DPO's activities compared with previous years and the internal allocation of staff to each category.

The following sections describe in greater detail the work carried out in the various areas covered by the DPO.

5 Article 33 of the GDPR.

6 The Data Protection Impact Assessment (DPIA) is a process that is designed - as a rule following technological and organizational changes - to re-examine how data are processed, to assess the necessity for such processing and its proportionality in terms of minimizing the amount of data used and how long they are stored, to examine the risks to the rights and freedoms of the natural persons concerned and to determine the appropriate security measures to mitigate such risks.


Volumes of Activity 2019-2022
Work experience programme
17
0
0
0
Internal consultancy and initiatives
616
224
156
56
DPO network
114
110
109
21
Staff training
20
9
4
24
Monitoring of the register and data processing
50
68
66
116
Data breach assessment
102
102
138
58
Impact assessments (DPIAs)
122
229
153
152
0
100
200
300
400
500
600
700
2022
2021
2020
2019


ALLOCATION OF THE DPO'S STAFF IN 2022
DPO's initiatives; 4.8%
Work experience programme; 1.6%
Impact assessments (DPIAs); 11.7%
DPO network; 11.0%
Data breach assessment; 9.8%
Staff training; 1.9%
Monitoring of the register and data processing; 4.8%
Internal consultancy; 54.4%

2.1 Cooperation and dialogue with the Italian Data Protection Authority

The DPO, as part of the duty to monitor the Bank's compliance with personal data processing rules in the course of its activities, necessarily cooperates with the Italian Data Protection Authority and responds to the Authority's requests to the Bank.

During the year, the DPO also collaborated on performing an in-depth analysis, requested by the Authority, of the compliance of the Bank's Register of Entities with the personal data protection rules. They provided detailed information on the breadth of processing operations performed, the specific aims pursued, the nature of the personal data processed, the procedures for their collection, the legal basis within the hierarchy of sources that govern the powers of the Bank pursuant to Article 6(3)(b) of the GDPR and Article 2-*ter* of the Privacy Code, as well as the observance of the other principles set out in the GDPR and the exercise of rights by the data subjects.

2.2 Advisory activities of the DPO

The DPO provides advice regarding personal data protection by engaging in ongoing dialogue with the Bank's directorates and, in particular, with the Organization Directorate. This task was systematically incorporated in the 6th update of Circular 257/2004 published in October 2022. There was a considerable increase in advisory activities during the year in response to the volume and variety of situations calling for application of and compliance with the privacy regulations.

In addition to formulating opinions on data breaches and data protection impact assessments pursuant to Articles 33 and 35 of the GDPR, advice was provided on a wide range of cases, regarding, among other things:

- the drawing up of two agreements between the Bank and the National Cyber Security Agency (*Agenzia per la Cybersicurezza Nazionale* - ACN), in accordance with Article 15 of Law 241/1990, for sharing information and cooperating to defend against cyber threats and to manage the computerized portions of the competitive hiring process;
- the Regulation on the processing of personal data by the Bank in handling complaints regarding the transparency of contractual terms and conditions, fair dealings between banks and their customers, and the rights and obligations of the parties to payments services contracts, areas in which the Bank acts in the public interest;[7]
- the conclusion of an accreditation agreement for the operation of an analysis laboratory with remote access between ISTAT and the Bank in accordance with Article 5-*ter* of Legislative Decree 33/2013, concerning access for scientific purposes to raw data collected for statistical purposes by national statistics system (SISTAN) entities and agencies. In terms of privacy considerations, ISTAT is the Data Controller for the data processed and the Bank is the Data Processor under Article 28 of the GDPR with respect to the operation of the lab.

[7] The regulation forming the legal basis for the data processing was issued based on Articles 6.3.b, 9.2.g and 10 of the GDPR, and Articles 2-*ter*, 2-*sexies*, paragraph 1, and 2-*octies*, paragraph 3, of Legislative Decree 196/2003 (Privacy Code). The regulation received the prior favourable opinion of the Italian Data Protection Authority (Measure no. 78 of 24 February 2022) pursuant to Articles 36.4 and 58.3.b of the GDPR.

-

2.3 Monitoring of Registers of processing activities

The DPO's monitoring of the Bank's Registers of processing activities in 2022 focused on periodically checking the information contained in therein[8] to verify the comprehensiveness and consistency of the descriptions of the processing operations recorded by the directorates concerned (214 as at 31 December).

The Registers were checked, as usual, on a half-yearly basis, revealing that:

- the increase in the number of processing operations recorded resulted from the different categorization of the activities or work processes based on their specific nature, especially those relating to supervisory activities, in line with the practices developed at EU level;
- the internal distribution of processing operations is highly uneven across the directorate generals and other Bank's directorates and is especially concentrated within the Directorate Generals for Human Resources, Communications and Information, for Markets and Payments Systems and, more recently, for Financial Supervision and Regulation (110 processing operations in total);
- information quality improved significantly owing to the progressive identification of factors as either mandatory or supplemental in descriptions of the processing operations;
- a large number of processing operations report the data retention periods.

2.4 Data protection impact assessments (DPIAs)

During the year, for ten data protection impact assessments (DPIAs) the DPO provided his opinion on data processing operations whose potential to expose the data subjects to risk, along with the specific adequate protection measures, was re-evaluated in relation to IT projects or work processes being studied or revised.[9]

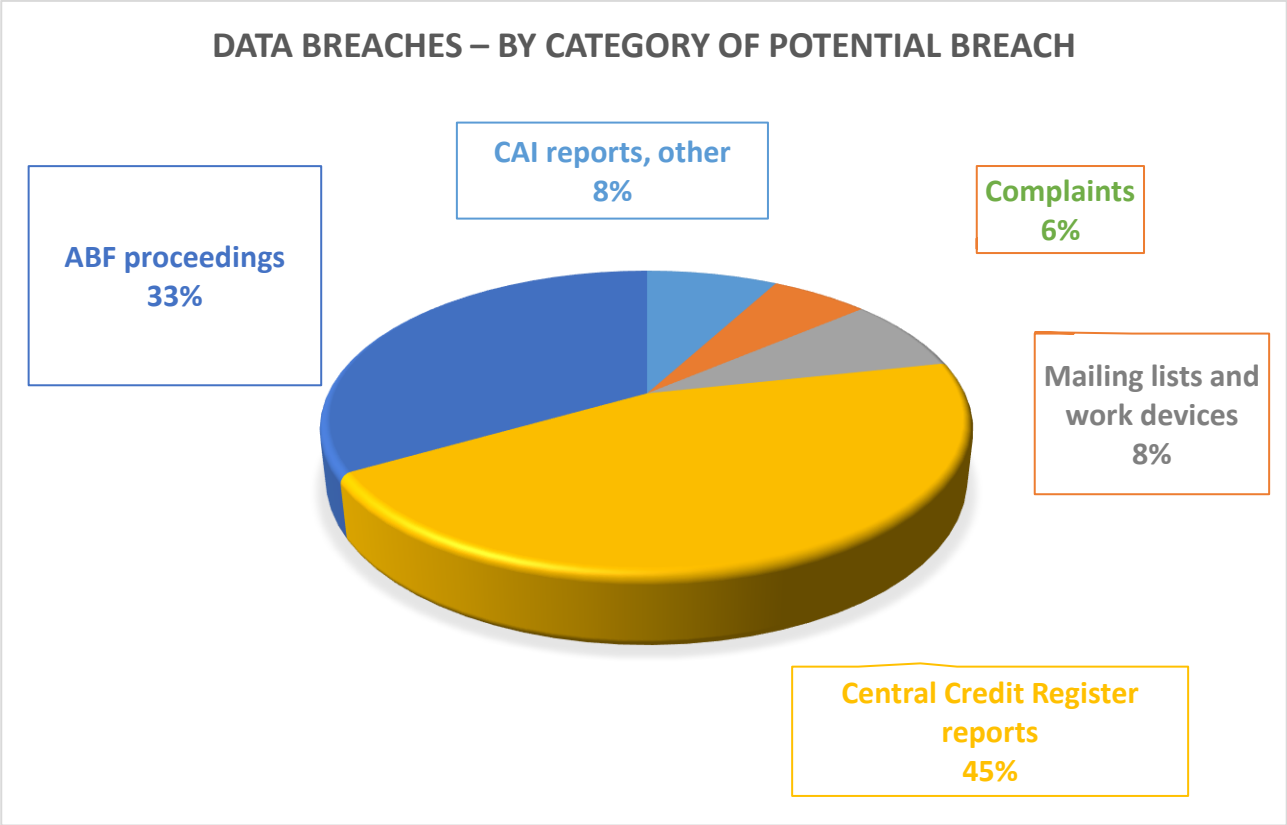
2.5 Reports of data breaches

There were 51 potential data breaches submitted to the DPO for assessment in 2022, the same number as the previous year. Regarding these potential breaches, the DPO advised the

8 Maintenance of the Registers is provided for under Article 30 of the GDPR and is among the main tasks of the Data Controller (and of the Data Processor). The Registers must be kept in written form, including electronic form, and must be made available on request to the Italian Data Protection Authority. According to European Guidelines (WP Art. 29, Guidelines 5 April 2017, paragraphs 4.1 and 4.5) to monitor compliance with the GDPR, the DPO regularly checks the Registers to verify the comprehensiveness and consistency of the processing operations recorded, and to assess their overall effectiveness in providing information.

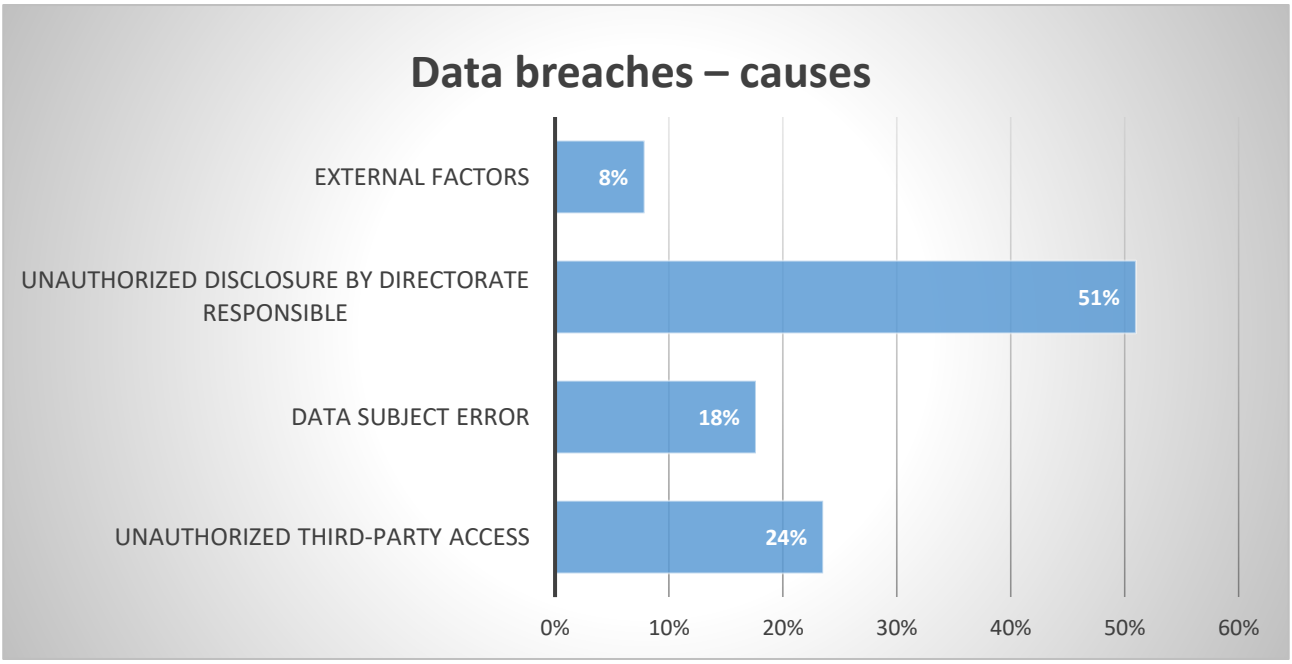
9 Article 35 of the GDPR provides that: "*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to 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 ...*". An impact assessment must be performed when the acquisition and management of data involve the processing of particularly important personal data, processing on a large scale or involving the use of innovative technologies, and in all the situations indicated by the Italian Data Protection Authority pursuant to Article 35.4 of the GDPR (see Measure no. 467 of 11 October 2018). The DPO also contributed in some cases to the preliminary assessment of whether a DPIA is required (e.g. purchase of new anti-malware software by the Bank for domestic systems and for support systems for TARGET services).

Organization Directorate on the risk to the rights and freedoms of data subjects to assist it in making any subsequent decisions under the GDPR.[10]



An analysis of the causes of such events reveals that data breach risk prevention actions must focus primarily on better protecting the transmission of data required for the various activities carried out (see the chart below).

[10] The DPO provides an opinion to the Data Controller that sets out in greater detail the factors to be assessed in the case of loss, alteration or accidental disclosure of personal data amounting to a data breach. When a data breach is discovered, 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 justified reason for the delay, where it is not feasible to provide notification within such period) and to also notify the data subjects without undue delay if the breach poses a risk to their freedoms and rights.



No notification to the Italian Data Protection Authority (pursuant to Article 33 of the GDPR) was necessary in nearly all the cases of a suspected data breach given the negligible level of risk posed to data subjects in the various situations due to the precautions taken. The risk assessments pertaining to these breaches led in just one case to a notification being made,[11] while in another case the Italian Data Protection Authority sent a request for information regarding an investigation it was conducting.

2.6 DPO's initiatives

In monitoring the application of the privacy regulations, 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.

Support teams were assigned to follow the development of the ten projects selected, based on the Call for Proposals 2021,[12] for inclusion in Milano Hub by contributing their expertise based on the characteristics of each project and on the needs expressed by the candidates chosen. Specifically, the DPO's staff sat on the support teams for two projects: 'Alternative Scoring by Digital Data Insights' (deposit and lending sector) and 'WoX Edge: a customer-centric and inclusive smart speaker for the bank branch of the future' (payments sector).

As part of his work to spread awareness of the privacy rules and provide training on them to other Bank's directorates,[13] the DPO introduced a series of initiatives for preventing potential personal data breaches.

---

[11] This related to someone gaining online access to a legal person's Central Credit Register records through false self-certification. The situation was also reported to the judicial authorities.

[12] The competition of ideas focused on the theme: 'The contribution of artificial intelligence in improving the provision of banking, financial and payment services to businesses, households and the public administration, paying particular attention to financial inclusion, adequate consumer protection, and data security.'

[13] See Article 39.1.b of the GDPR: '*The data protection officer shall have at least the following tasks: (...) b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and (...) awareness-raising and training of staff involved in processing operations, and the related audits*'.

More specifically, on 17 November 2022, the DPO organized an in-house seminar for the directorates in the Rome Head Office on data protection and related cybersecurity issues. The seminar was also streamed to the branch offices. The data protection officer of the Italian National Institute of Health, an expert in data protection and data security management, spoke at the seminar.

The main topics addressed were protecting personal data from modern threats, with specific reference to those indicated in the GDPR: protection of fundamental rights and freedoms, accountability, and technical and organisational measures for ensuring personal data security.

3. Participation in DPO networks

3.1 International activity

During their meetings held throughout the year, the Network of DPOs of the national central banks and the NCAs for banking supervision, coordinated by the ECB, discussed issues of common interest regarding compliance with the European privacy regulations. They examined compliance issues regarding: the use of cloud services[14] by the ECB as part of a customer relationship management tool project, the impact assessment for which was submitted for prior consultation to the European Data Protection Supervisor (EDPS); the ESCB collaboration prototyping project for a new communications and document-sharing system based on Microsoft Teams in which 14 central banks, including the Bank of Italy, are taking part; the Artificial Intelligence Playbook drafted by the ECB on the adoption of AI solutions in conformity with Regulation (EU) 1725/2018 (EUDPR), which must be revised once the European regulation on artificial intelligence is approved; the conclusion of a new agreement with the institutions concerned for a centralized platform managed by the EBA (called 'EuReCa') for anti-money laundering and counter-terrorism financing.[15]

The Network is expected to be asked to contribute, in 2023, to the drafting of a new joint controllership agreement for the division of responsibilities between the ECB-SSM and the NCAs in processing data relating to banking supervision authorization procedures.

[14] Following the judgment of the Court of Justice of the European Union of July 2020, which invalidated the European Commission's adequacy decision authorizing the transfer of personal data from the European Union to the United States on the rationale that the level of protection was essentially equivalent to that required by the GDPR (Article 45.2.a).

[15] The central database was established in accordance with Article 9a of Regulation (EU) No 1093/2010, (the 'EBA Regulation').

3.2 National activity

The DPO is a standing member of the Network of DPOs of the national independent authorities,[16] formed after the GDPR became applicable to provide a forum for inter-institutional dialogue on data protection issues within their respective agencies.[17]

At the end of 2022, after three years of remote meetings, the Bank proposed that the Network launch a new season of regular, in-person meetings, hosting the first one of the new year. The meeting of 23 January 2023 was opened by the Bank's DPO, who emphasized the importance of the work done by the Network since the GDPR came into effect and highlighted the Bank's long-standing focus on protecting personal data, demonstrated by units it has dedicated to this task.

In opening the meeting, the DPO stressed certain aspects that are particularly important for the Bank:

- attention to the issue of cybersecurity, fuelled by continual threats to the privacy of persons and institutions, and the application of artificial intelligence to the world of finance, in which personal data represent the key resource for the functioning of the algorithms, but also rest on constant compliance with regulatory restrictions on automated decision-making and profiling;
- the project to create the digital euro, which is gradually taking shape under the leadership of the Italian member of the executive board of the European Central Bank, for which protecting privacy was identified as one of the key concerns of the public (43 per cent of those responding to the public consultation held by the ECB in 2020).

[16] 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 Fund for Energy and Environmental Services (CSEA) and Italy's single buyer Acquirente Unico S.p.A. (AU), as well as the DPO of the Italian National Institute of Statistics (ISTAT) as an observer.

[17] The Network is governed by the 'Rules on the organization and functioning of the Network of DPOs of the national independent authorities' approved by an absolute majority on 24 September 2021.