BANCA D'ITALIA
EUROSISTEMA

Data Protection Officer's Report

2021

Overview

Rome, March 2022

CONTENTS

Introduction

The year 2021, with the country still in the midst of the health emergency, was one of rising demand for sharing data in pursuit of the public interest, as well as a demonstration of the social and economic value in making personal data available and enabling them to flow within the private sphere. This generated renewed interest in the protection of personal data, driven by public opinion which has become increasingly sensitive to privacy concerns.

At community level, there was a push by the European Union for a structured regulation of the flow of information, specifically personal data, which is taking the form of a 'digital package' designed by the European Commission to facilitate the further use and sharing of (personal) data among a wider range of public sector entities and with private players within the so-called 'data economy'.

The digital euro project, which could result in a digital currency issued by a central bank, has also attracted public interest ever since the ECB began looking into the issue, provided that the safeguards put in place for payment instruments are matched by adequate protection of users' privacy.[1]

The protection of personal data is a critical part of the digital technology framework that, through the expansion of connectivity (e.g. 5G, Internet of Things) and the improvement in methods for capturing and exploiting data, tends to elude European regulation and poses a problem of the 'technological sovereignty' over data flows.

In the Bank of Italy, the Data Protection Officer (DPO), in the person of 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 corporate activities and departments, performed his duties by engaging in constant dialogue with the departments and, in particular, with the Organization Directorate, which serves as the Data Controller for the Bank.

The DPO acts independently, reporting directly to the Bank's top management, and draws up an Annual Report for the Governing Board, which is published on the Bank's website.

1. The legislative framework

The main development last year was the legislature's introduction of several significant changes to the Personal Data Protection Code (Privacy Code, Legislative Decree 196/2003) through Article 9 of Decree Law 139/2021, converted into law as modified by Law 205/2021. Specifically, alongside the existing legal basis, comprised only of laws or regulations, for the processing of data by the public administration for 'the performance of a task carried out in the public interest or in the exercise of official authority' (Articles 6.1 and 6.3 GDPR),[2] the legislature has added 'general administrative acts' and the 'need' to carry out a task in the public interest or

[1] Integrating the digital euro into the payment infrastructure and appropriate technological support are deemed critical to balancing the need for a satisfactory level of protection of users' personal data with the central bank's supervisory power to safeguard the public interests linked to currency circulation (not least of which is combating illegal activities). The European Data Protection Board also weighed in on this matter with a request directed at the ECB and the EU institutions urging them to pursue, as early as the design stage, a high standard of privacy and personal data protection to reinforce the trust of end users in the offering of a digital euro, key factors to its success (EDPB; plenary session of 21 June 2021).

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, General Data Protection Regulation (GDPR).

in the exercise of public authority vested in the originating entity, always in accordance with the principles and the protection of the data subjects' rights and freedoms established by the GDPR.

On an international level, the European Commission has taken important decisions on the regulation of relationships that involve the processing of personal data. Specifically, the following were approved:

- the standard contractual clauses for governing the transfer of personal data to third countries or non-EU organizations to close a gap created by the judgement of the Court of Justice of the European Union of 16 July 2020 which invalidated the Commission's decision on the adequacy of the EU-US Privacy Shield;[3]
- the standard contractual clauses between controllers and processors in an EU context.[4]

2. Consolidation of the DPO's position

Over the last three years, the DPO's activities in the exercise of his duties have become more firmly established, especially those involving interaction with the Bank's various departments, which confer with the DPO, not just as part of the consultation processes under the regulation, but increasingly to seek assistance on questions connected with the privacy protection legislation and with participation in national and European working groups and other forums.

A survey of the network of the DPOs within the European System of Central Banks (ESCB) was conducted in order to compare the solutions adopted by analogous institutions, such as the national central banks and the national competent authorities (NCAs) for supervision. A comparative analysis of the data collected, thanks to the cooperation of a significant number of the DPOs contacted, offers an overview of the various ways in which support for the DPO is structured in the different organizational systems. This bird's eye view has proven helpful to the Bank in designing its own solutions.

The formation last July of an organizational unit dedicated to supporting the DPO (the Support Unit), which became fully functional towards the latter part of the year, marked the fruition of the development of the role and is a sign of recognition of the importance of his duties and his authority as a contact point both inside and outside the Bank.

3. Activities carried out in 2021

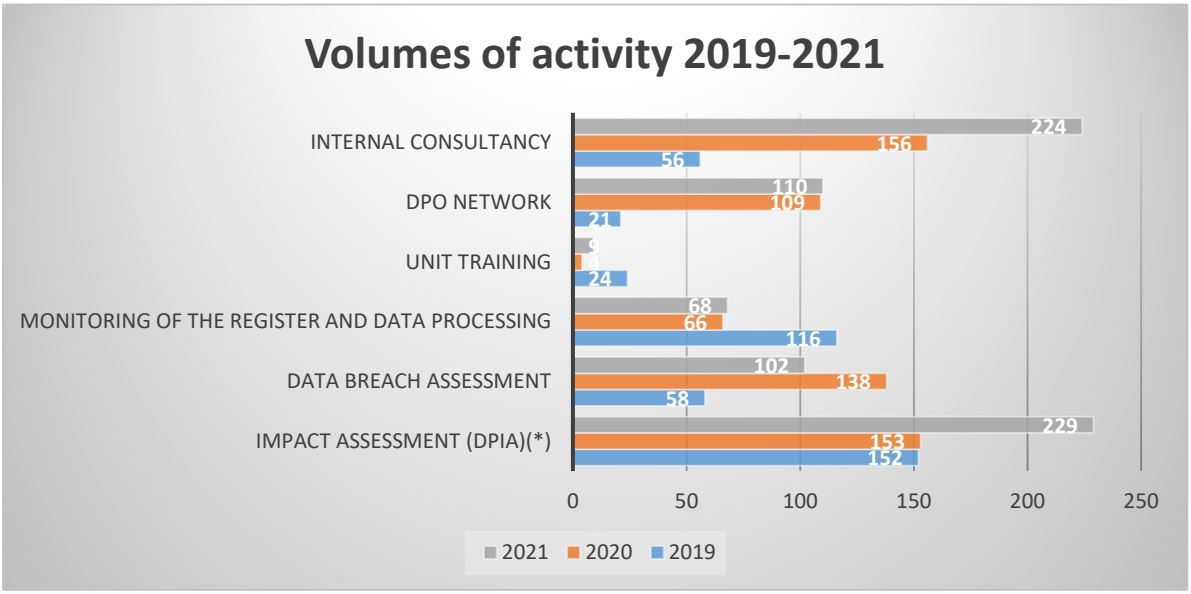
During the year, the DPO's duties expanded even further. In addition to advising the Bank's departments in the course of their normal operations and in launching innovative projects that require an analysis of personal data processing issues, the DPO was in constant contact with other Italian and European authorities.

---

[3] Commission Implementing Decision (EU) 2021/914 of 4 June 2021, implementing the provisions of Article 46.2.c of the GDPR.

[4] Commission Decision 2021/915 of 4 June 2021, implementing the provisions of Article 28.7 of the GDPR and Article 29.7 of Regulation (EU) 2018/1725 (EUDPR). EDPB Guidelines 07/2020, adopted in September 2020, also address this issue.

Most of the DPO's work, in terms of both number and complexity, involved issuing data protection impact assessments (DPIA),[5] a task requiring a thorough analysis and consultation with the departments concerned. Furthermore, the DPO was called on to formulate opinions reconstructing the events leading up to data breaches[6] based on the information obtained from the reporting departments, which were shared with the data controller as provided in the GDPR.



Following the formation of the Support Unit, training programmes were launched towards the end year and are expected to be expanded based on the planned utilization of new staff members.

3.1. Cooperation with the Italian Data Protection Authority

As provided in the GDPR, the DPO cooperates with the Italian Data Protection Authority, serving as the intermediary for all issues regarding the processing of personal data that involve the Bank.

During the year, the DPO met with representatives of the Italian Data Protection Authority to discuss matters including topics of general interest, such as the proper assessment of reports of data breaches, the common data processing rules for the various public entity data controllers, and the conditions regarding the lawfulness of new data processing technologies.

The DPO also took part in meetings with the Authority in the context of a prior consultation process to obtain its legally required opinion on the Bank's proposed Regulation on the processing of personal data in the handling of complaints regarding banking activity.

---

[5] 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, assess the necessity for such processing and the proportionality in terms of minimizing the amount of data used and how long they are stored, examine the risks to the rights and freedoms of the natural persons concerned and determine the security measures to mitigate such risks.

[6] Article 33 of the GDPR.

3.2. Advisory activities of the DPO

The DPO's advisory tasks regarding personal data protection vis-à-vis the internal departments involved, among other things:

- helping to draw up an agreement between the EU's Financial Intelligence Unit (FIU) and the European Commission to enable the Commission to manage FIU.net, the forum through which the various FIUs in the EU share data in carrying out their institutional mandates: specifically, regarding their roles, it was agreed that each FIU would remain the 'data controller' for the personal data processed through FIU.net and remain subject to the obligations envisaged by the GDPR, while the Commission would take on the role of 'data processor' on behalf of the FIU, with the consequent restrictions and obligations imposed by the EUDPR.[7]
- advising on certain compliance issues regarding the call for proposals and the privacy policy for the 'Techsprint' initiative, launched by the Bank together with the BIS Innovation Hub under the Italian G20 Presidency to highlight the potential of new technologies in financial innovation, analysing any problems relating to their regulation and supervision.[8]

The DPO has also become increasingly involved in preparations for the signing of agreements and memorandums of understanding with the central government and other public authorities relating to the statistical analysis and economic research required for the Bank's institutional tasks or the provision of joint services, which in most cases entail the communication and sharing of databases that also contain personal data.

3.3. Monitoring of the Register of processing activities

The DPO's monitoring of the Bank's Register of processing activities in 2021 focused on the periodic monitoring of the set of information contained in the Register. The DPO checks the Register,[9] usually on a half-yearly basis, to verify the comprehensiveness and consistency of the descriptions of the processing operations recorded by the departments concerned (192 as at 31 December).

This monitoring has enabled the Bank to gradually improve the informational capacity of the Register as a personal data protection accountability tool.

---

7 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the European Union institutions, bodies, offices and agencies.

8 The initiative, sponsored together with the Bank for International Settlement, was a public competition of ideas open to developers, designers, creators, data scientists, start-uppers, and digital marketing and communications experts with the goal of expanding the potential of innovative technologies to solve operational problems in the green and sustainable finance sectors covered in the call for proposals.

9 Maintenance of the Register is provided for under Article 30 of the GDPR and is among the main tasks of the Data Controller (and of the DPO). The Register must be kept in written form, including electronic form, and must be exhibited on request to the Italian Data Protection Authority. According to European Guidelines (WP Art. 29, *Guidelines on Data Protection Officers,* 5 April 2017, par. 4.1 and 4.5) for monitoring compliance with the GDPR, the DPO regularly checks the Register to verify the comprehensiveness and consistency of the processing operations recorded, and to assess its overall effectiveness in providing information.

3.4. Data protection impact assessments (DPIA)

In the course of 2021, the DPO advised on 19 DPIAs regarding the processing of data of differing complexity and depth in relation to new projects and procedures involving almost all areas of the Bank.[10]

The impact assessments of new personal data processing operations were conducted, as part of the Bank's institutional functions, with regard to the following significant projects:

- the automation of the collection, processing and analysis of data needed to verify that the officials of all the banks and intermediaries governed by the TUB meet the fit and proper requirements, in line with EU regulations and EBA guidelines;
- the review of operational processes and new IT solutions for assessing the creditworthiness of Italian non-financial corporations and of producer and consumer households through the Bank's In-house Credit Assessment System (ICAS);
- the upgrading of the procedures for collecting and managing data taken from reports by intermediaries and firms on the financing conditions that banks offer their customers;
- the collection of data for and the management of a unified database drawn from the Treasury, SIOPE/SIOPE+, and internal and external statistical sources in order to enable an analysis of developments in the public accounts and the main relationships between the public financial flows and the macroeconomic variables.

During the year, the departments concerned had to conduct impact assessments, using a more streamlined process,[11] of 26 data processing operations, which were chosen from among those that had not undergone a targeted assessment since the GDPR entered into force[12] (a total of 140). These operations, based on their characteristics and their content, needed to be re-examined to confirm their adequacy in terms of compliance and monitoring risks to data subjects.

3.5. Reports of data breaches

In 2021 there were 51 potential data breaches submitted to the DPO for assessment, compared with 69 the previous year. The DPO provided to the Organization Directorate advice on the risk to the rights and freedoms of data subjects for the consequent ascertainment to be made under the GDPR.[13] The reduction in the number of data breaches should be viewed in light of the DPO's work to raise awareness within the branch network. In fact, in the majority of

---

[10] 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 ...'.

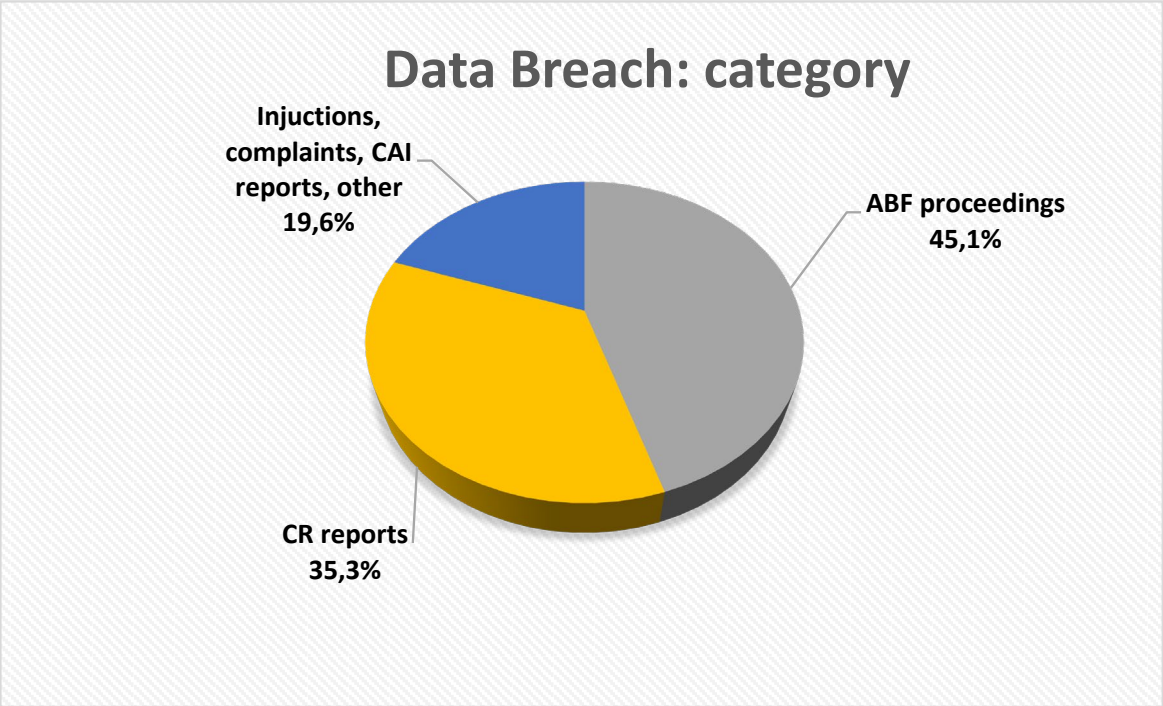
[11] A streamlined DPIA process was allowed for this specific type of processing provided that there have been no change in the residual risk to data subjects.

[12] On 25 May 2018.

[13] The DPO provides advice to the data controller on the factors warranting a more in-depth assessment 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 the Italian Data Protection Authority, not later than 72 hours after having become aware of the breach (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.

cases, the breaches can be traced to operational errors that can be mitigated through remedial actions built around vigorous application of the 'four eyes principle'.

As shown in the figure below, the breaches mainly regarded data contained in the acts of the proceedings before the Banking and Financial Ombudsman (ABF) panels and in the Central Credit Register (CR) reports.



The risks associated with the data breaches led in only one case to a report being made to the Italian Data Protection Authority which, after its investigation, decided to dismiss the report insofar as it related to the adequate protection provided by existing measures.

3.6. The DPO's initiatives

In monitoring the application of the privacy regulations, the DPO can also, on his own initiative, request that checks and assessments be performed to improve the overall compliance of the departments.

Specifically, during the year, discussions were held with the Directorate General for Financial Supervision and Regulation on improving how its various data processing activities are reported in the Register[14] and on engaging in mutual consultation on issues regarding the different supervisory roles played by the NCAs and the SSM-BCE (autonomous controllers, co-controllers or processors) and their consequent respective responsibilities.

[14] The need to identify a specific data processing for each supervisory activity, to align itself with the practices developed at EU level and to be able to manage individually the privacy obligations, was shared by the Directorate General which immediately endeavoured to comply.

The DPO provided to Human Resources and to the Workplace Health and Safety Division information on the Italian Data Protection Authority's new guidelines[15] on data processing by employers and by 'company medical staff, derived from the rules on workplace health and safety (Legislative Decree 81/2008).

In accordance with the guidelines for DPOs in the public sector, the DPO maintained a regular schedule of meetings with the Organization Directorate in its capacity as Data Controller regarding issues involving the application of the privacy rules within the Bank.

On the institutional front, the DPO took part in the conference organized by the Italian National Institute of Statistics (Istat) on 23 June on 'Personal data protection – What is going on in Istat and the outlook' during which he made a speech and took part in the round table on 'Future prospects: Data Protection Officers share their perspective', together with the DPOs of the Italian Revenue Agency, the Italian National Institute of Health and Istat.

4. Participation in DPO networks

4.1. International activity

During their meetings held remotely throughout the year, the data protection officers of the national central banks, the ECB and the NCAs for banking supervision discussed issues of common interest regarding compliance with the European privacy regulations based on the experience of some of the network's members and of the ECB in applying them.

The ECB also decided to adopt organizational solutions that mirror those of the Bank of Italy, forming a specialized unit to support the DPO.

Finally, there was an internal debate within the network concerning the roles of the various participants (controllers, co-controllers and processors) and the division of responsibilities between the ECB-SSM and the NCAs in processing data relating to banking supervision authorization procedures, as well as the necessary future arrangements for compliance with the GDPR.

4.2. National activity

The progressive consolidation of the activities of the network connecting the DPOs of the national independent authorities, formed in 2019 to provide a forum for interinstitutional dialogue on the main data protection issues within their respective agencies, was completed with the approval of the 'Rules on the organization and functioning of the Network of DPO's of the national independent authorities'.[16]

---

[15] Italian Data Protection Authority, 'The role of company medical staff in matters of workplace health and safety including in the present emergency situation', published on 14 May 2021 (only in Italian).

[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 National Commission for Companies and the Stock Exchange, (CONSOB), the National Anti-Corruption Authority (ANAC), the Communications Regulatory Authority (AGCOM), the National Authority responsible for the supervision of Italian pension funds (COVIP), the Italian Strike Guarantee Commission (CGSSE), the Italian Data Protection Authority (GPDP), the Italian Insurance Supervisory Authority (IVASS), the Fund for Energy and

Matters of common interest were addressed at the meetings held during the year. The network also completed and published a paper on the role, autonomy, responsibilities, organizational position and involvement of the DPO in public organizations.

Environmental Services (CSEA) and Italy's single buyer Acquirente Unico S.p.A. (AU). The Rules were approved by an absolute majority at the meeting of 24 September 2021.