BANCA D'ITALIA
EUROSISTEMA

Data Protection Officer's Report

2020

Rome, February 2021

TABLE OF CONTENTS

Introduction

The fair and transparent use of personal data and the recognition that the power to control such data resides with the natural persons to whom they refer have become increasingly important today in the Public Administration, making it necessary to strike the right balance between these concerns and the performance of tasks in the interest of the wider community.

The Bank of Italy swiftly adapted to the legislative provisions requiring the creation of the role of data protection officer (DPO).[1] In the Bank's organizational chart, this figure coincides with the Managing Director for Internal Audit who, owing to the nature of the position they hold, maintains an impartial stance with respect to all other corporate activities and departments.

Acting autonomously, the DPO liaises with the departments and, in particular, the data controller, a role that in the Bank of Italy falls to the Organization Directorate; he or she reports on their activities directly to the Bank's top management, drawing up an Annual Report for the Governing Board.

In 2020, notwithstanding the legislative constraints introduced to limit the epidemiological risks posed by COVID-19, the activities of the DPO were consolidated. There was broad-ranging interaction with the departments, consultations on privacy issues and data protection impact assessments linked to new projects or procedures and to potential data breaches.

There were increased opportunities for dialogue and liaison with the data protection functions operating within the ESCB, for the formulation of opinions and common positions on compliance with the GDPR of shared or linked data processing operations by different institutions, as well as with national authorities for the analysis of matters of common interest.

The coordination role of the ECB's and SSM's data protection officers has become increasingly important vis-à-vis the DPOs of the EU national central banks. This has been apparent in discussions on the application of the rules and guidelines, in the promotion of agreements to regulate cases where there are joint data controllers and in calls for common initiatives.

1. The legislative framework

In 2020, the legal framework governing personal data protection remained largely unchanged.

The national personal data protection code (hereinafter, the Privacy Code), already completely revised to adapt it to the GDPR, was amended by Law 160 of 27 December 2019. The updated Code provides that the prevention and combating of tax evasion:

– falls within the areas of substantial public interest in which the unauthorized processing of 'special categories of personal data'[2] is permitted;

[1] Regulation (EU) 2016/679 (GDPR). The tasks of the DPO, as set out in Article 39 of the GDPR, include providing advice, monitoring data protection compliance and liaising with the Data Protection Authority (Garante per la protezione dei dati personali), the national supervisory authority pursuant to Article 51 of the GDPR.

[2] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

– is among the cases in which limits may be imposed on the exercise of the rights of the data subjects.

Given that EU and national laws permit, insofar as it is in the public interest, the processing of 'special' data (formerly 'sensitive' data), including those pertaining to criminal convictions and offences (formerly 'legal' data), but require the identification of the procedures and categories of data processing admissible as well as the appropriate guarantees from legal sources of at least regulatory level, the Bank of Italy's internal regulations are currently being revised to include the most complex cases of 'sensitive' and 'legal' data processing by the Bank.[3]

In the course of 2020, the Organization Directorate revised the internal regulations (Circular 257), implementing the legal provisions governing the:

– designation of the data processor and the clause to be inserted into service contracts awarded to third parties that must perform this role;
– coordination of the definition of personal data protection measures with the identification of safeguards stemming from IT security legislation;
– the application of the GDPR to the decentralized management of access to the data contained in the Central Credit Register (CR) and in the Interbank Register of Bad Cheques and Payment Cards (CAI).

Regarding the data protection framework at international level, the European Court of Justice's ruling of 16 July 2020 (case C-311/18, known as *Schrems II*) has made a significant impact. In its judgment, the Court invalidated Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield regulating the conditions for the lawful transfer of data to the USA. It found that it did not ensure a level of protection essentially equivalent to that required today by the GDPR for the rights of the persons whose data were transferred to the United States.[4]

To close the loophole created by the Court's pronouncement, in November, the European Commission began the process for approving new Standard Contractual Clauses (SCCs) to regulate, through the use of standard GDPR-compliant contracts, the transfer of personal data to third countries.

The regulation of personal data transfers outside of the EU has taken on particular importance following the United Kingdom's withdrawal from the European Union.

According to the terms of the EU-UK Trade and Cooperation Agreement stipulated on 30 December 2020, the GDPR shall continue to apply for a transition period of 6 months, during which time any communication on personal data to the United Kingdom can take place based on the same rules valid at 31 December 2020, without being considered a data transfer to a third country.

2. Activities carried out in 2020

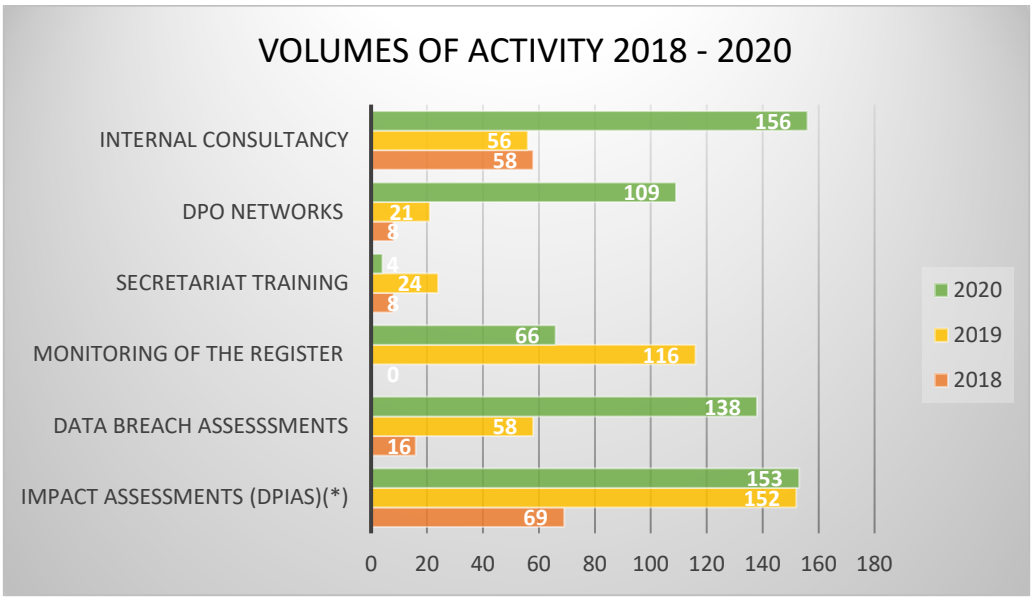
In the course of 2020, the volume of activities of the DPO increased overall. In particular, there was more intensive participation in the DPO networks of the ESCB central banks and of

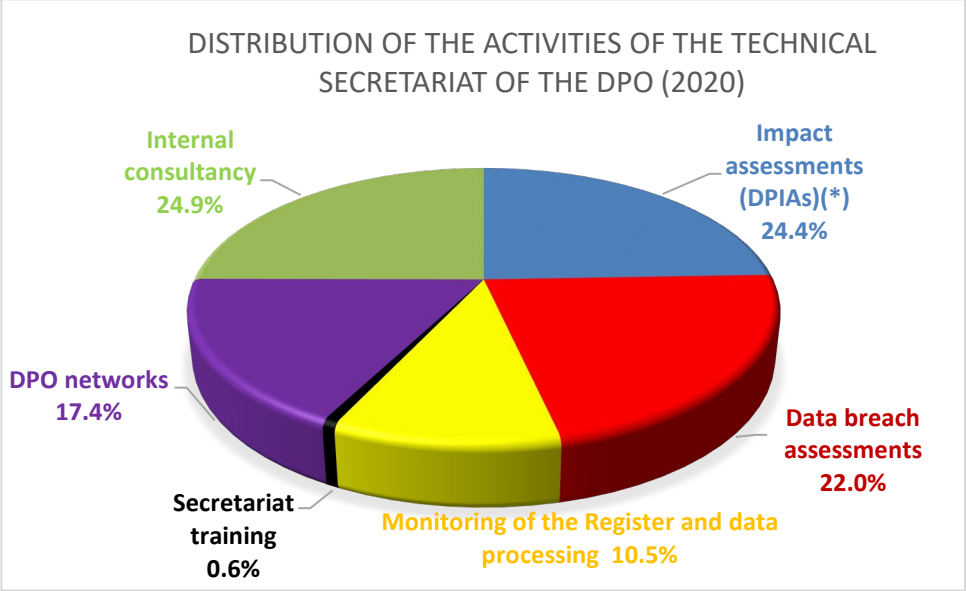
[3] While issued to implement the rules of the Privacy Code, since abrogated (Articles 20 and 21), the Bank of Italy Regulation of 6 November 2015 (published in the Gazzetta Ufficiale No. 271 of 20 November 2015), regarding the 'identification of sensitive and legal data and of the operations that can be carried out', is nonetheless still deemed to be in force by the Data Protection Authority to the extent that it is compatible with the revised legislative framework.

[4] The Privacy Shield was a self-certification mechanism used by companies headquartered in the United States and designed to legitimize the transfer of personal data from the European Union to controllers or processors in the United States, who in turn undertook, through certification, to uphold the principles established by the EU on privacy and to ensure that the parties concerned enjoyed equivalent protections to the European ones.

the national independent authorities, as well as internal collaborations and assessments of potential data breaches.

The activity dedicated to DPIAs(*) and to assessments of individual processing operations, which normally require meetings and interviews with the departments concerned, remains considerable.





(*) A Data Protection Impact Assessment (DPIA) is normally carried out in the wake of technological and organizational changes. It is a process designed to: re-examine how data are handled, assess the need for such operations and their proportionality in terms of minimizing the data used and storage periods, examine the risks to the rights and freedoms of the natural persons concerned and determine the security measures to mitigate such risks.

Approximately three years since this position was created, the DPO has taken on a 'transversal' role, being called on to engage in broad-ranging dialogue with a number of different

institutional and corporate functions. The expansion of his activity, especially in qualitative terms, and the complexity of the relations that have been forged, including at international level, mean that the activities supporting the tasks of the DPO must now be given a structural unit within the Bank's organization.

2.1 Consultancy

Advising on personal data protection vis-à-vis the internal departments has been a significant part of the DPO's activity since the creation of this position.

This function, unlike that inherent in the routine processes regulated by Articles 33 and 35 of the GDPR (data breach and data protection impact assessments), is clearly identified by the rules and recommended by the data protection guidelines.

In the past year, the DPO's advice was requested on a number of matters, including:

- *the review of the internal rules on conflicts of interest*, on which the DPO was consulted in order to identify, in light of the provisions of the GDPR, the legal basis for processing data submitted by employees on potential economic and financial conflicts of interest; the DPO's opinion was also sought regarding the level of confidentiality to be assigned to these data in documents;
- *the handling of duplicate tax codes in the Central Credit Register*. Since the natural persons listed in the Central Credit Register are identified by their personal tax codes, the DPO was asked to advise on how to ensure that the risk of personal data breaches is mitigated in cases of access by data subjects whose tax codes have been changed following a duplication;[5] it was decided to provide the parties concerned with information on the reporting intermediaries that would enable the identification of the position at risk and of the relevant personal data only;
- *the review of a Scientific Cooperation Agreement between the Bank of Italy and the Italian National Institute of Health* (ISS) on research activities relating to data collated by the Bank of Italy,[6] without prejudice to the personal data processing carried out exclusively by the ISS. The consultancy aimed to ensure timely compliance with the rules on personal data protection by modifying the Agreement in order to make more granular data available to researchers[7] and, in a meeting with the DPO of the ISS, by finalizing an Addendum to the agreement;
- *the complete digitization of the 730 joint tax return form;*

[5] The Revenue Agency has specified that in cases in which the alphanumeric tax code generated is identical for multiple subjects, it is necessary to proceed to a differentiation of the tax codes, following the criteria set out in Article 6 of the Ministerial Decree of 23 December 1976 (automatic replacements of one or more numbers starting from the last one with the corresponding alphabetical letters), making it impossible to utilize a duplicate tax code generated according to the standard calculation algorithm.

[6] Drawn from a study on the spread of the Coronavirus epidemic across Italy to assess the possible repercussions for the health system, economic activity and systemic financial stability, as well as the costs and benefits of alternative policies to combat the spread of the virus and to exit the emergency phase.

[7] Permitted through the issuance of a government order authorizing the transfer of pseudonymized data in non-reversible form by the ISS to the affiliated agencies for scientific research purposes.

- *personal data processing within the G7 Cyber Expert Group (CEG).*[8] The DPO was consulted on the criteria for making lawful transfers of personal data to a third country for archiving, with regard to the various procedures contemplated under the GDPR.[9] The opinion expressed, which is shared by the DPOs of the other central banks concerned, initiated a dialogue with the participating institutions;
- *personal data processing in the Securities Financing Transactions Data Store.* As part of the Bank's participation in an ECB project to collect detailed data on securities financing operations in a Data Store, based on the specific European legislation (Securities Financing Transactions Regulation, SFTR), the DPO worked with the Statistical Data Collection and Processing Directorate and the Organization Directorate to define a Memorandum of Understanding on Joint Controllership of the personal data processed in the Data Store by the participating central banks,[10] as well as on a review of the Privacy Statement regarding this data processing, which will be published on the Bank's website.

Finally, the advisory role of the DPO was exercised in participation in internal working groups and constant dialogue with the Organization Directorate on the application of the privacy rules. In particular:

- joint analyses continued on the prevention of personal data breaches, in the light of repeated access by private parties to data held in the Central Credit Register on behalf of third parties;
- compliance of the data processing activities carried out by the Bank as part of its duties as an employer was verified for the management of cases of contraction of COVID-19, in accordance with the guidance issued by the Data Protection Authority.

2.2 Monitoring. Register of processing activities

The monitoring activities of the DPO in 2020 continued according to the two guiding principles identified during the previous year.

A. The periodical monitoring of the set of information contained in the register of processing activities.[11]

The DPO monitors the register of processing activities on a six-monthly basis. These records are among the main elements of the controller's accountability, insofar as they provide an up-to-date picture of the processing operations under way within the organization and are

8 The CEG is responsible for preventing and managing crises in the event of a cyber attack on the international financial sector. Bank of Italy experts participate in the group along with colleagues from other central banks.

9 The conditions for lawful data transfers to non-EU countries set out in the GDPR (Articles 45-49) contemplate: the adoption of adequacy decisions by the European Commission regarding the level of foreign protection, the stipulation of executive protection agreements between the public authorities that export the data, the transposition of Standard Contractual Clauses (SCCs) into contracts approved by the EU Commission, the establishment of control mechanisms based on codes of conduct or certification bodies, the approval by a national supervisory authority of corporate binding rules within transnational business groups and special derogations covering specific situations.

10 In addition to the ECB and Banca d'Italia, the Nationale Bank van België, Deutsche Bundesbank, Banco de España, la Banque de France, la Banque centrale du Luxembourg and De Nederlandsche Bank also took part in the project.

11 The maintenance of the records is envisaged under Article 30 of the GDPR and is among the main tasks of the data controller (or processor). The records must be in writing, including in electronic form, and must be made available on request to the Data Protection Authority.

indispensable for every assessment or risk analysis regarding the potential violation of people's rights.

The monitoring aims to verify the comprehensiveness and consistency of the descriptions of the processing operations recorded therein (190 as at 31 December). Last year, also thanks to the efforts of the Organization Directorate and the DPO to raise awareness of this activity in the Bank's departments, the informational content of the records improved progressively from a variety of perspectives,[12] as did the descriptions of the processing operations undertaken. It is still necessary, however, to identify the conditions for the storage of the data more clearly.[13]

The lack of uniformity among the processing operations recorded by the Bank's departments means that the way in which the information is classified is likely to differ: a more standard approach should be promoted in the future.

B. *In-depth assessments of processing operations.* The analysis is routinely made during meetings with the various Directorates, when the characteristics of the data collection operations are illustrated in the context in which the activities are carried out, to verify their consistency with the information declared in the register.[14]

The assessment activities focused on the data processing activities listed in the records kept by the Directorate General for Property and Tenders.

For the assessment of the different elements (nature of the data processed, purposes and procedures for its collection, designation of authorized employees, legal basis, storage requirements, disclosure to interested parties and so on) a questionnaire was drawn up in accordance with the indications of the DPO Handbook.[15]

In the analysis of individual processing operations, if agreements have been stipulated by the Bank with third parties, it was verified in particular, based on the activities assigned, whether or not these parties were property qualified as processors to act on behalf of the Bank or

---

12 The identification of the legal basis, by adhering more closely to the sources of legitimation set out in the GDPR and of disclosures, by specifying the ways in which they are made and the eventual reasons for exemptions from this obligation (Articles 13 and 14 of the GDPR).

13 Some departments are now working to ensure storage periods are consistent with the principle of minimization. On the issue of data storage, there is the question of how to achieve a regulatory balance between the principle that limits such storage and the integrity of the digital documents containing the data: for Public Administrations in particular, there are uncertainties around how privacy constraints interact with 'mandatory (minimum) retention periods' that remain unresolved by the competent authorities (the Data Protection Authority and Archival Authority). In fact, Article 5(1)(e) of the GDPR stipulates that the personal data must be kept 'for no longer than is necessary for the purposes for which the personal data are processed'; by contrast, Article 10 of Legislative Decree 42/2004 (Code of the Cultural and Landscape Heritage) defines all PA documents as 'cultural properties', which, therefore: i) 'may not be destroyed, damaged or adapted to uses not compatible with their historic or artistic character or of such kind as to prejudice their conservation' (Article 20); and ii) they must be kept (for the periods of time envisaged in the storage plans) and, after 40 years, if the conditions subsist (mandatory (minimum) retention periods), transferred to the historical archives.

14 The Guidelines on Data Protection Officers of 5 April 2017 (pars. 4.1 and 4.5), with reference to Article 39(1)(b) of the GDPR:

15 In the conduct of the DPO's monitoring activities, account is taken of the guidelines proposed in the DPO Handbook 'Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation Handbook' approved by the European Commission in July 2019 in order to harmonize actions at European level.

independent controllers of processing, for the purposes of complying with the data protection obligations; a self-assessment was also promoted based on the inherent risk profiles, in support of the adequacy assessment at the time of the existing protection measures.

To identify the processing operations that should undergo assessments as a matter of priority, the principle of selecting interventions based on the relative risk to the data subjects will continue to be upheld, which the European regulation places at the centre of the monitoring activity of the DPO.

2.3 Data protection impact assessments (DPIA)

In the course of 2020, the DPO advised on 13 DPIAs regarding the processing of data of differing complexity and breadth, in relation to new projects and procedures involving a number of areas in the Bank.[16]

As part of its institutional functions, the impacts on personal data processing were assessed with regard to the following projects:

- the evolution of the SWIFT network, used by domestic applications in the payment infrastructures to interact with national and international counterparts;
- the construction of platforms to exploit the information flows of transactions acquired pursuant to Regulation (EU) 2012/648 (EMIR) and Regulation (EU) 2015/2365 (STFR);
- a review of the collection and payment procedures performed by the State Treasury Service;
- information and management by the bodies tasked with defining crisis management procedures;
- the development of over-the-counter procedures for branches and the Central Administration for managing the accounting department.

Several aspects of personal data protection were also re-examined vis-à-vis the open web platform called the Citizen's Bureau[17] and two Financial Intelligence Unit (FIU) projects to rationalize the management of suspicious transaction reports.

On the corporate side, the implications of data processing were examined regarding:

- whistleblowing by workers and employees of goods and service providers operating in the Bank;
- notification services to users of the Bank's website for newsletters, publications and news items;
- certain data concerning the health of employees, which the Bank as an employer is obliged to record under worker health and safety legislation;
- the management of hybrid postal services;
- the creation of an online portal for 730 tax returns.

Regarding the assessment of technical data protection measures, simplification initiatives were promoted to identify, with the help of the Directorate General for Information Technology, the security measures that can be considered 'recurrent,' insofar as they are routinely envisaged

[16] Article 35 of the GDPR stipulates 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 ...'.

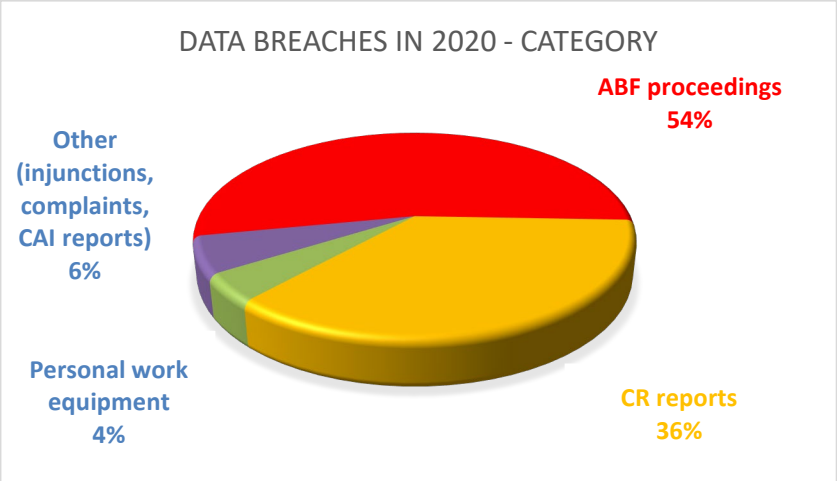
[17] The Bureau permits citizens to present requests to access the data held in the CAI, file customer complaints, report operational irregularities on the part of supervised intermediaries (including whistleblowing reports) and make requests for information on supervisory activity, the CR and the CAI.

by all services provided directly by the Bank's IT function. The aim is to facilitate the departments in the presentation of their impact assessments. This innovation, which has already been agreed, will be transposed into internal regulations in 2021.

2.4 Reports of data breaches

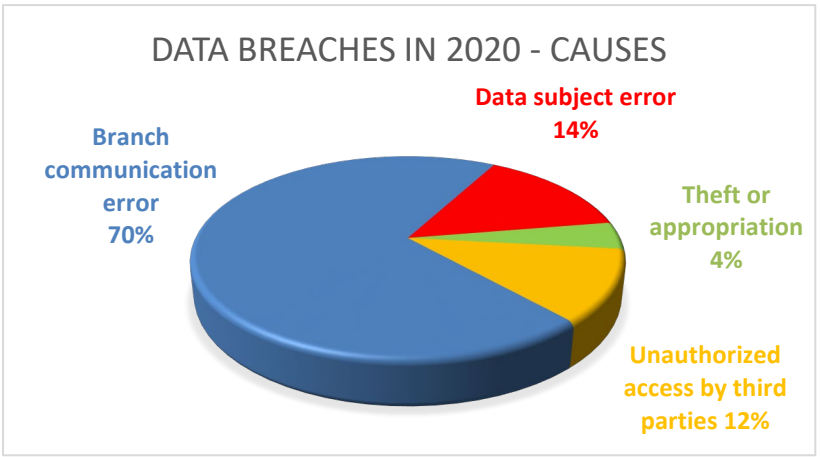
The analysis of potential data breaches in compliance with the GDPR is the basis of the controller's accountability, who is obliged to put in place all the measures designed to prevent the risk of non-compliant processing of personal data and of civil liability because of a breach of confidentiality that harms the interested parties.

When a data breach occurs, Article 33 of the GDPR obliges the data controller to notify the competent Data Protection Authority within 72 hours of it being made aware of this (unless, when the notification cannot be made within that strict deadline, it is able to justify a delay). If it subsequently emerges that the breach poses a high risk to individual rights and freedoms, it must also notify the parties concerned without undue delay.



As shown in the chart, the events verified last year mostly concerned the data contained in proceedings before the panels of the Banking and Financial Ombudsman (ABF) and in the reports of the Central Credit Register (CR).

An analysis of the causes of these events (see the chart) shows that most stemmed from mistaken transmissions of data to third parties during operating processes carried out by the branch territorial network (communication error by the entity). In many cases, the event was caused by the data subjects themselves (data subject error) and by unlawful access to data by third parties (unauthorized access by third parties) linked to the possibility of acquiring information online; criminal acts (theft or misappropriation) were a residual cause, limited to a few cases of theft of personal work devices (laptops).



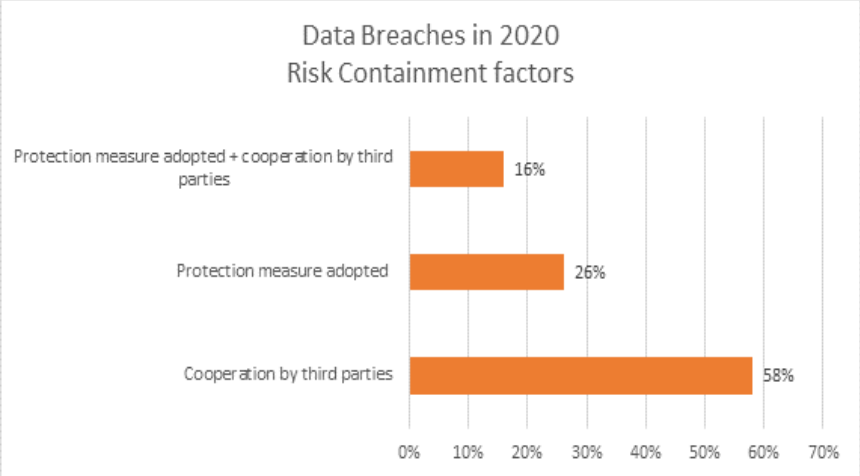
The most significant information to emerge from the survey of data breaches relates to the data contained in the CR reports, which by their nature are especially sensitive, with most breaches ascribable to the new online data collection procedure.

Following the launch of the Citizen's Bureau application, enabling the online release of CR reports to persons in possession of public digital identity credentials (SPID),[18] there were repeated and multiple cases of unauthorized access on behalf of third parties by entities declaring they had the necessary self-certification credentials which, in subsequent checks, turned out to be untrue or, in some cases, by entities forwarding the request without any third party authorization.

Regarding this last category of data breaches, the risks stemming from the violations led to a report being made to the Data Protection Authority by the Statistical Data Collection and Processing Directorate (RES), competent in this field, which adopted measures suited to filtering access on behalf of another natural person and to reducing the risk of reports being extracted unlawfully.

Regarding the other data breaches, the assessment of the facts has not given rise to any reporting obligation to the Data Protection Authority, given the negligible level of risk determined in light of the precautions adopted in the specific cases.

Moreover, examining the initiatives taken in a number of cases to prevent any harmful repercussions shows that the main factor that subsequently helped to limit this risk was the cooperation of third parties that were accidentally involved as erroneous recipients of data (see the chart).



3 The DPO's activities in the ESCB and independent national authorities

The application of EU regulations concerning personal data protection within the European System of Central Banks (ESCB) and by the supervisory authorities in the Single Supervisory Mechanism (SSM) has raised the question of the roles played by these authorities and the related responsibilities in personal data processing linked to shared activities in the respective institutional contexts.[19]

[18] This application, designed to facilitate user access, enables the immediate releases of reports to both natural and legal persons (which can also contain information on natural persons), through accreditation with SPID and self-certification of authorization to acquire the data.

[19] While the provisions are essentially equivalent, it is necessary to bear in mind that on the question of personal data

The regulations provide that, when the purposes and means of personal data processing are determined together by two or more controllers, these shall be considered joint controllers: this makes it incumbent on them – in the absence of a specific regulation in EU law – to determine, in a Memorandum of Understanding (MoU) on joint controllership for the processing of personal data, the respective roles and responsibilities for compliance with the obligations, with special regard to disclosure and to the exercise of the rights of data subjects.

The definition of joint controller memoranda for the data presupposes detailed preparatory work to analyse the data processing to be made in relation to the characteristics of the various institutional actors. It also implies the involvement of DPOs from a number of participating institutions for a joint discussion of the various regulatory aspects.

The centralization of some functions at the ECB-SSM and the relative concentration at just a few NCBs of shared services provided on behalf of the entire ESCB call for the definition of different roles in the area of privacy. In discussions on this point, in which reference was mostly made to the stance taken by LEGCO, in the case of data processing made 'on behalf' of the entire system, the qualification of 'Joint controller that offers the service' was identified, instead of the data processor acting on behalf of the joint controllers.

Last year, the DPO was asked to assist in the examination and drafting of some parts of the MoU on joint controllership, specifically:

- on the rules governing ESCB-shared IT services;
- on the Securities Financing Transactions - Data Store, set up by the ECB with seven other central banks, including the Bank of Italy.

Towards the end of the year, consultations got under way as part of the preparatory works for the drafting of joint controllership memoranda on personal data processing in the field of supervisory authorizations and for the coordination of the related requirements under the GDPR: more initiatives and consultations will likely follow on this topic.

The annual session of the DPO network within the ESCB/SSM was held on 30 October with the objective of promoting shared practices by the DPOs in the institutions to which they belong. The session examined the repercussions of the European Court of Justice ruling known as 'Schrems II' on the regulation of personal data transfers outside of the EU, progress on the definition of joint controllership agreements for the shared processing of personal data and the role of the DPO network in the context of the ESCB.[20]

Moreover, in the course of the year, meetings were streamed for the select group comprising the DPOs of the ECB and the four NCBs that manage the shared payment system infrastructures (Target Services - TARGET 2, T2S, TIPS and ECMS) for the definition of a

protection in Europe vis-à-vis natural persons, the ECB is subject to Regulation (EU) 2018/1725 (EUDPR), which sets out the rules applicable to EU institutions in this area.

[20] Within this forum, it is worth recalling the Bank's participation in the survey promoted by the Banco de España to study the degree of implementation of the GDPR by central banks and by the supervisory authorities in the ESCB/SSM. The final report on the survey, which was conducted as part of the Schuman Programme, was published in September 2020 on the Banco de España website.

common position on compliance of the Target Services with the GDPR, with special regard to the data protection measures in the TIPS-MPL infrastructure.[21]

As part of the Cyber Information and Intelligence Sharing Initiative (CIISI), set up to share information, strategies, techniques and procedures to improve the protection of European public financial institutions against cyber threats, the Bank's DPO was consulted by his counterpart in the ECB, together with his peers from the other central banks, to express an opinion as to the advisability of drafting a joint controllership agreement on the information shared. Based on the elements examined, in agreement with the DPOs of the other NCBs, the DPO submitted a reasoned opinion opposing the need for such regulation, given the scarce eventuality of personal data being gathered and the fiduciary nature of relations within the initiative.

In 2020, the Bank continued to participate in the DPO network linking the independent national authorities, which was established to share experiences and opinions on the main issues in the area of personal data protection and on the operational guidelines adopted by the respective administrations.[22]

Periodic meetings were held during which, also thanks to the analysis of internal and external rapporteurs, matters of common interest were discussed.[23]

Of particular importance was the online seminar organized on 18 November by the Bank's DPO and the DPO of ARERA, the coordinator of the network, on the issue of 'Data protection and processing of the independent authorities. Focus on responsibilities and sanctions'. A large audience took part, comprising officials and employees from all the network's authorities, who showed great interest in the matters discussed (organizational arrangements of the DPO, legal bases, sanctions, responsibilities).

The seminar was opened by the DPO of the Bank, who briefly illustrated the history of the institution of the Data Protection Officer (DPO) in the Bank of Italy, following the application of the GDPR in the EU, which made the creation of this position and its inclusion in existing organization charts obligatory for all Public Administrations.

The DPO stressed how conflicting needs can arise between carrying out the Bank of Italy's institutional activities and the need to guarantee the protection of citizens' privacy and of the firms with which the Bank comes into contact and to exercise the powers entrusted to it by law, which in some cases place strict limits on the right to confidentiality.

---

[21] The meetings were organized by the ECB's Directorate General Market Infrastructure and Payments, which illustrated the technical and operational characteristics of the infrastructures in order to facilitate the assessments by the DPOs.

[22] The Group comprises the DPOs from the Italian Regulatory Authority for Energy, Networks and Environment (ARERA), the Italian Transport Regulation Authority (ART), the Italian Competition Authority (AGCM), the Companies and Stock Exchange Commission (CONSOB), the National Anti-Corruption Authority (ANAC), the Communications Regulatory Authority (AGCOM), the Pension Fund Supervisory Authority (COVIP), the body that regulates strikes in the field of essential services (CGSSE), the Data Protection Authority (Garante privacy), and the Italian Insurance Supervisory Authority (IVASS).

[23] In particular: the procedures for conducting Data Protection Impact Assessments (DPIAs); the role and position of the DPO in public authorities; the administrative and civil responsibilities of the Public Administration for non-compliance with the GDPR and the Privacy Code; the transfer of data to non-EU countries; compliance of the health checks imposed by the COVID-19 epidemic. Moreover, in a meeting with the Monuments and Fine Arts Office of Lazio, the questions of the storage of digital documents by the independent administrative authorities and of the effects of the GDPR on archives and the preservation of document flows were discussed.

The DPO acknowledged that the principle of transparency that guides administrative activity in the day-to-day operations of the Bank has now superseded previous arrangements that placed a heavier emphasis on confidentiality.

Given that the theme of the meeting was sanctions, the DPO highlighted some problem areas, such as the application of the privacy safeguards to public organizations, i.e. the possible qualification of the sanction imposed on the processor as a revenue liability and the duplication of personal responsibilities (of management, who must answer to the revenue agency for the measure censuring Public Administrations and of the DPO, who is sanctioned directly) which risks leading to a lack of cooperation on the part of administrations, with effects on transparency and on the release of information on institutional activities.

4. Future developments

In ensuring that all the typical tasks are carried out (monitoring of the data processing records and relative assessments, opinions on DPIAs and data breaches), in the near term the work of the DPO will have to take account of the likely increase in cooperation at supranational level and the rapid evolution of data processing arrangements that the Bank is called on to put in place when carrying out its functions.

As to the first aspect, it will be necessary to ensure a balanced definition of the roles and responsibilities in shared personal data processing within the ESCB, the effective execution of the joint consultancies and ongoing participation in the DPO network.

Regarding the second aspect, it will likely also prove necessary to expand the monitoring activities of data processing compliance, especially of those that can most affect the image and responsibilities of the Bank of Italy, through a careful selection process based on intrinsic risk, with a particular focus on data processing activities that are outsourced to third parties.

Finally, in order to consolidate the Bank's accountability as data controller, in compliance with a specific provision of the GDPR, it will be necessary to verify over time the adequacy of existing data protection measures, in relation to changes in the processing rules and procedures for processing them.

The Organization Directorate has launched a campaign to review 'extant' data processing activities, i.e. the ones in place prior to the application of the GDPR, which has highlighted the need to submit a large number of cases to an impact assessment. The cooperation of the DPO in this area will be directed toward identifying ways to simplify the DPIA process in order to complete the adequacy assessments of all data processing within a reasonable timeframe.