THE GDPR IN EUROPEAN CENTRAL BANKS AND COMPETENT AUTHORITIES
An Overview

2020

BANCO DE ESPAÑA
Eurosistema

Aleksandra Magdziarz and Beatriz Pardo

THE GDPR IN EUROPEAN CENTRAL BANKS AND COMPETENT AUTHORITIES – An Overview [*]

Aleksandra Magdziarz [**]

EUROPEAN CENTRAL BANK

Beatriz Pardo

BANCO DE ESPAÑA. GENERAL SECRETARIAT, GOVERNANCE AND TRANSPARENCY DIVISION

(*) This report is the outcome of a project hosted by the Banco de España in the third edition of the Schuman Programme that commenced in September 2019. It has been drafted by Aleksandra Magdziarz, under the guidance of Beatriz Pardo, on behalf of the Governance and Transparency Division, led by María Luisa Boronat. The Schuman Programme is an ECB initiative to promote employee mobility in the field of the ESCB and the SSM. It is open to all ESCB and SSM staff members, with no limits as to age or business area. The main purpose of the Programme is to provide multi-directional, project-based, external work experience of six to nine months, running from September to May.

(**) Aleksandra Magdziarz is a senior supervisor at the European Central Bank.

2020

Abstract

This report is the outcome of the Schuman Programme project undertaken by the Banco de España to study how the ESCB/SSM institutions have interpreted the most important aspects of the GDPR. It takes stock of the information received through a questionnaire on the implementation of the GDPR in the context of central banks' and competent authorities' activities, distributed to 37 institutions. The GDPR leaves many aspects open for interpretation and, in order to comply diligently with the accountability principle, the Banco de España considers it relevant to know how those aspects have been interpreted by institutions in other European jurisdictions that perform similar tasks to those of the Banco de España. As GDPR implementation is ongoing, this report aims at sharing best practices and ways of implementing the requirements of this regulation in various European central banks and competent authorities. It should be seen as a starting point for initiating a deeper discussion on various practical implementation tools and methods.

The more coherent the common approach to the GDPR in various European central banks and competent authorities is, the better their common understanding of and compliance with the GDPR will be.

Keywords: data protection, privacy, GDPR, General Data Protection Regulation, personal data, Schuman Programme.

JEL classification: K24, K38, K00.

Resumen

El presente informe es resultado de un proyecto del Programa Schuman desarrollado por el Banco de España con el objeto de estudiar la interpretación de las instituciones del SEBC/SSM respecto de los aspectos más importantes del RGPD. El mismo ha sido elaborado a partir de información recabada a través de cuestionarios distribuidos a 37 instituciones que han tenido en cuenta el contexto del funcionamiento de los bancos centrales y las autoridades competentes europeas. Dado que el RGPD deja muchos aspectos abiertos a interpretación, el Banco de España, con el fin de cumplir diligentemente con el principio de responsabilidad proactiva, considera relevante conocer el enfoque de instituciones de otras jurisdicciones europeas que realizan funciones similares a las del Banco de España. Dado que la implantación del RGPD es una tarea en continua ejecución, el presente informe desea compartir las mejores prácticas e interpretaciones aportadas por los bancos centrales y autoridades competentes de Europa respecto de los requisitos del reglamento. Por todo ello, debe considerarse como un punto de partida para iniciar un debate más profundo sobre los instrumentos y procedimientos que puedan ponerse en práctica para potenciar el cumplimento de la norma.

Así, cuanto más coherente sea el enfoque del RGPD por parte de los diversos bancos centrales y autoridades competentes europeas, mejor será su entendimiento común de la norma y su cumplimiento.

Palabras clave: protección de datos, privacidad, RGPD, Reglamento General de Protección de Datos, datos personales, Programa Schuman.

Códigos JEL: K24, K38, K00.

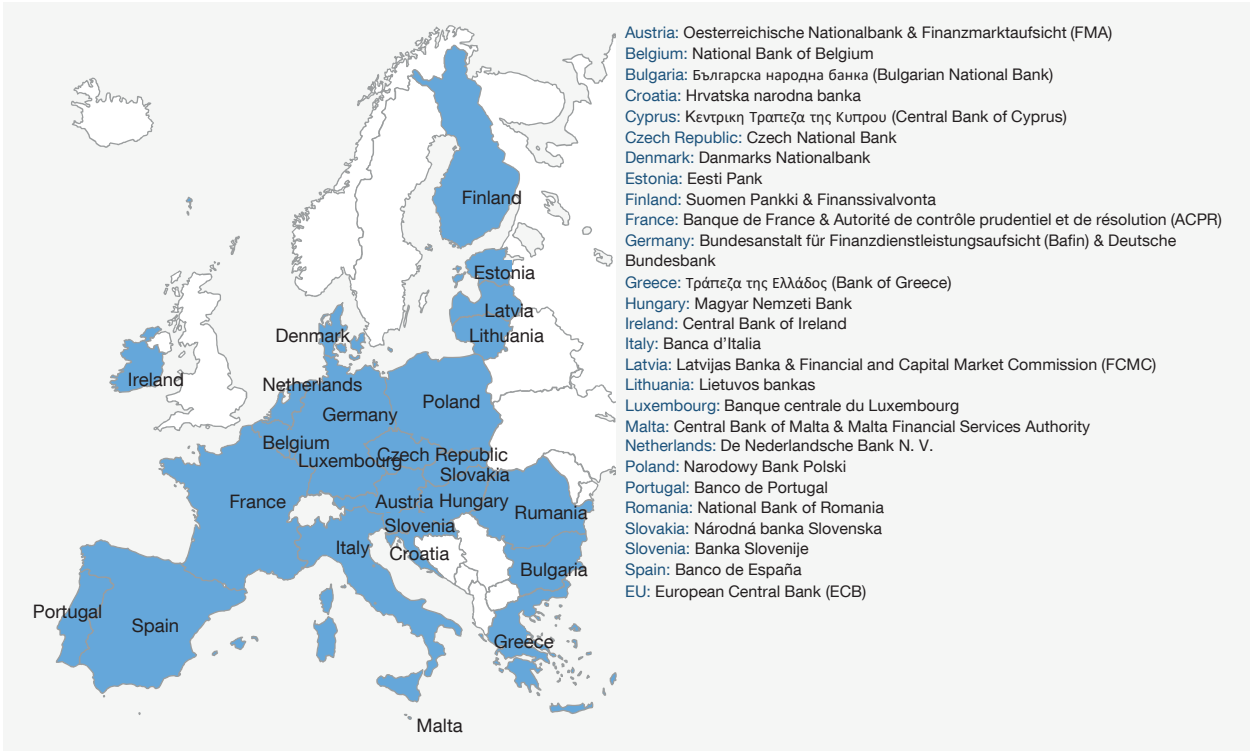
Contents

1 Introduction

This report is the outcome of the Schuman project undertaken by the Governance and Transparency Division of the Banco de España. The aim of the project is to learn how European central banks (NCBs) and competent authorities (NCAs) have implemented Regulation (EU) 2016/679 (GDPR)[1] and, in particular, how they have interpreted the most important aspects of the GDPR (e.g. how they are recording data processing activities, relations with data processors, data protection impact assessments, data subjects' rights or transfers of personal data to third countries).

For this purpose, a questionnaire containing 65 questions was prepared.[2] To make this exercise as user-friendly as possible, the structure of the questionnaire followed the structure of the GDPR, with references to the articles of this Regulation noted at the heading of each section. In addition, more than 70% of the questions were drafted as single or multiple choice. By mid-December 2019 the questionnaire had been distributed among 37 institutions – the NCBs and NCAs of the EU-27, the Bank of England (BoE) and the European Central Bank (ECB)[3] – through the mailing list of the ESCB Data Protection Officer (DPO) Network. This distribution channel was first consulted with the ECB DPO, who agreed that this would be the suitable forum for engaging in this project.

Figure 1
PARTICIPATING ESBC/SSM INSTITUTIONS



SOURCE: Own elaboration.

1 https://eur-lex.europa.eu/eli/reg/2016/679/oj.

2 For the questionnaire, please see Annex 1.

3 For the full list of participating authorities, please see Annex 2.

Of the 37 authorities consulted (see Figure 1), 33 NCBs/NCAs submitted their full or partial answers to the questionnaire, with the last one being provided on 5 March 2020. No response was received from four authorities: *Finantsinspektsioon* (Estonian NCA), *Commission de Surveillance du Secteur Financier* (CSSF) (Luxembourg NCA), *Sveriges Riksbank* (Swedish NCB) and the Bank of England (UK NCB).

As the structure of the questionnaire mostly mirrors the structure of the GDPR, the chapters of this report are also ordered in the same manner. First, the current legal framework in each jurisdiction is outlined by answering whether national legislation further detailing the GDPR has been enacted in the country concerned and whether the national data protection authority (DPA) has issued any relevant guidelines. Thereafter, the focus of the report shifts to practical implementation aspects of the GDPR, paying special attention to recording of processing activities (Art. 30 GDPR) and special circumstances for data processing (Arts. 6 - 11 GDPR), compliance with transparency obligations (Arts. 13 and 14 GDPR), processing of rights requests (Art. 12 and Arts. 15 - 23 GDPR), implementation of privacy by design and by default (Art. 25 GDPR), regularisation of relations with data processors and joint data controllers (Arts. 26 and 28 GDPR), processing of personal data breaches (Arts. 33 - 34 GDPR), performance of DPIAs[4] (Arts. 35 - 36 GDPR), structure and functions of DPOs (Arts. 37 - 39 GDPR) and regularisation of transfers to third countries (Arts. 44 - 50 GDPR). This structure should allow the reader to navigate easily between the chapters of this report and the GDPR.

For purposes of clarity, in this report those institutions acting as both NCB and NCA in their respective jurisdictions shall be referred to as "*[nationality]* NCB/NCA".

4 Data Protection Impact Assessment.

2 Applying the GDPR in different jurisdictions

The GDPR became directly applicable throughout the European Union (EU) from 25 May 2018. It replaces the Data Protection Directive 95/46/EC[5] and aims to provide harmonisation of the legal data protection regime across all the EU Member States.

Nevertheless, the new GDPR has still left room for EU Member States to detail further aspects through national legislation. As a result, all EU Member States except Slovenia have passed national laws to supplement the GDPR. For more information in this regard, **Annex 3** provides a chart with all the national legal provisions further detailing the GDPR to date.

Almost all national DPAs have also provided additional guidance on implementation of the GDPR. Even though this guidance is not legally binding, it explains how the DPAs interpret the GDPR provisions and forms a basis for their enforcement actions. The guidelines issued encompass topics ranging from general implementation of the GDPR to more specific decisions, such as the disappearance of a postal package containing personal data.[6] In addition, the DPAs from Bulgaria, Croatia, Italy, Poland and Spain have worked together to draw up "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".[7] **Annex 4** has a list of all the DPA guidelines considered sufficiently relevant by the participating NCBs/NCAs in each jurisdiction.

The information provided in **Annex 3** and **Annex 4** does not replace a case-by-case study should an issue need to be addressed in a certain jurisdiction, but they aim to provide valuable background and a starting point on which to base any further analysis.

5 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

6 https://finlex.fi/fi/viranomaiset/tsv/2019/20190401.

7 https://www.fondazionebasso.it/2015/wp-content/uploads/2019/07/T4DATA-MANUAL-2019.pdf.

3 Records of processing activities (Art. 30 GDPR)

Art. 30 GDPR requires that each controller maintain a record of the processing activities under its responsibility and enumerates the minimum information that needs to be recorded about each processing activity.

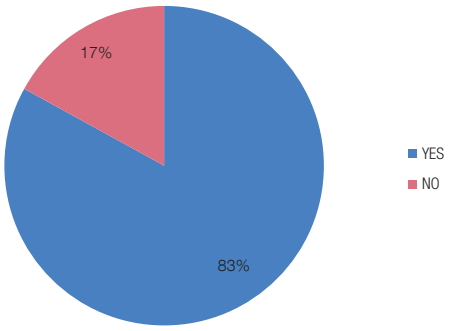
Mapping and registering the amount of information required about each processing activity undertaken by an institution is usually the starting point of GDPR implementation. Therefore, this part of the report deals with aspects concerning the practical approach to complying with this obligation.

3.1 Contact person in departments involved in personal data processing

Mapping every processing activity undertaken by a NCB/NCA requires in-depth knowledge of the types of processing activities undertaken in the institution. On account of the sheer number of different processing activities, it is essential to establish efficient ways of communicating with different business areas. One possible way to approach this task is by establishing a network of contact persons appointed by the business areas involved in personal data processing to interact with the DPO. According to the answers provided by the respondents, 83% of the authorities have appointed a contact person in the business areas involved in data processing to interact with the DPO on personal data matters (see Chart 1). Appointing a contact person should not be construed as a limiting factor, as the DPO should be able to address a question to any employee and the employee should be obliged to assist the DPO. However, the contact person should be someone with a deep understanding of the specific processing activity and should, therefore, be a primary source of information for the DPO.

Chart 1

HAVE THE AREAS INVOLVED IN PERSONAL DATA PROCESSING APPOINTED A CONTACT PERSON TO DEAL WITH THE DPO?



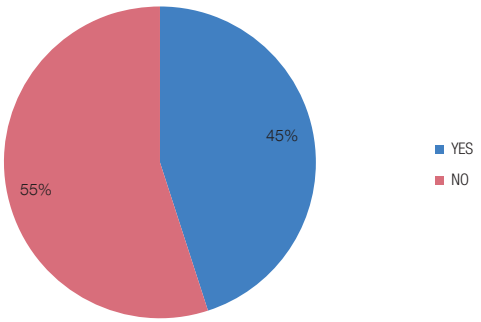
SOURCES: ESCB/SSM institutions (Annex 2).

3.2 Content of the records of processing activities

The next important factor when recording processing activities is how to structure the content of the records. The minimum requirements as to the information that needs to be recorded on each of the processing activities are stipulated in Art. 30 GDPR. However, 14 NCBs/NCAs have reported

that they record information over and above the minimum requirements to enhance compliance with other GDPR obligations (see Chart 2). The most common supplementary information concerns the source of the personal data, the legal basis for the processing, the level of risk associated with the processing and the need to conduct a DPIA.

Chart 2
DO YOU RECORD ADDITIONAL INFORMATION THAN THAT REQUIRED BY ART.30 GDPR?



SOURCES: ESCB/SSM institutions (Annex 2).

From the information provided by the NCAs/NCBs, the most comprehensive record of processing activities is kept by the Czech NCB/NCA's DPO, who records all the following information:

- ref. number;
- name;
- description;
- business unit ('owner' of the processing activity);
- contact person;
- number (of an aggregated processing activity);
- name (of an aggregated processing activity);
- list of ref. numbers of processing activities constituting an aggregated processing activity;
- most concerned/significant business unit for the aggregated processing activity;
- name of the purpose under which a processing activity is classified in the privacy notice;

— external / internal privacy notice;

— notes to the privacy notice (special circumstances, e.g. whether they need to be printed out);

— purpose of processing;

— legal basis;

— types of personal data (i.e. further refinement: categories and specific types of personal data);

— processing of special categories of personal data;

— legal grounds for processing of special categories of personal data;

— processing of personal data relating to criminal convictions and offences;

— source of personal data;

— retention period (length of a retention period, including, where appropriate, with a link to a code number of retention period as listed in the CNB disposal/shredding plan);

— start of a retention period;

— justification for a retention period;

— categories of employees to whom personal data are disclosed and identification of the business unit they belong to;

— data processors;

— recipients;

— automated / manual means of processing;

— whether an IT system is used in the processing;

— name of the involved IT system;

— share of agenda processed in an IT system (in %);

— internal documents (determining personal data processing covered by a processing activity);

— external documents (determining personal data processing covered by a processing activity);

— automated individual decision-making (Y/N);

— automated individual decision-making – measures to protect the data subject's rights and legitimate interests (Art. 22(2) GDPR);

— restrictions on data subjects' rights;

— personal data breaches;

— preliminary DPIA (registration number, last performance, reason for the last performance (a change or lapse of a default period of time));

— whether a DPIA is to be conducted (Y/N);

— DPIA details such as registration number, last performance and reason for the last performance (e.g. a change or lapse of a default period of time).

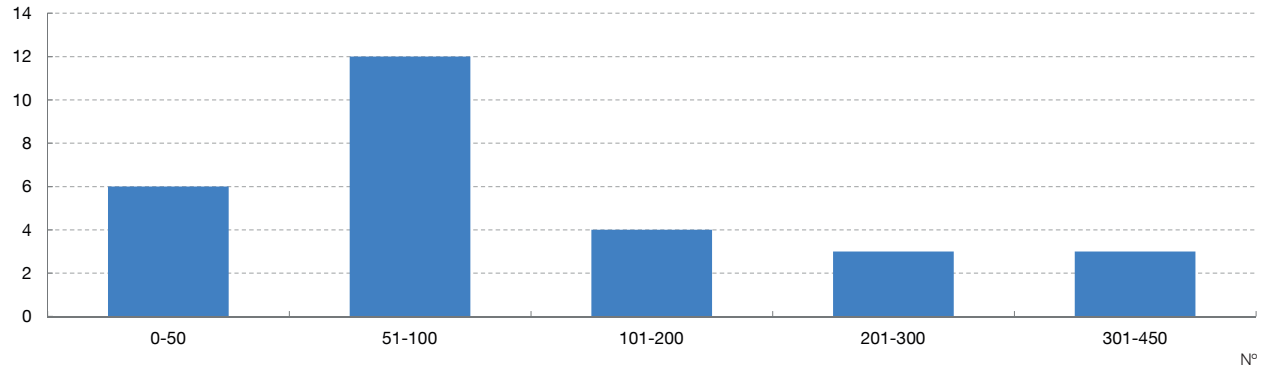
3.3 Number of processing activities

In terms of the number of processing activities, the figures reported by the participating NCBs/NCAs vary immensely, ranging from 16 to 550 pre-grouping and from 22[8] to 417 post-grouping (see Chart 3). In the jurisdictions where the NCA is separate from the NCB, it is noteworthy that the number of processing activities reported for the NCA were significantly lower than the number reported for the NCB. The following chart shows the grouping of NCBs/NCAs by the number of processing activities reported. For the purposes of this chart, for NCBs/NCAs that do not apply any grouping methods (or are still in the process of grouping and, therefore, have not provided any post-grouping numbers), the number of final processing activities reported is either the post-grouping or pre-grouping number.

8 The NCB/NCA that reported 16 processing activities pre-grouping did not state the number of processing activities post-grouping.

Chart 3

NUMBER OF AUTHORITIES ACCORDING TO THE FINAL NUMBER OF PROCESSING ACTIVITIES REPORTED

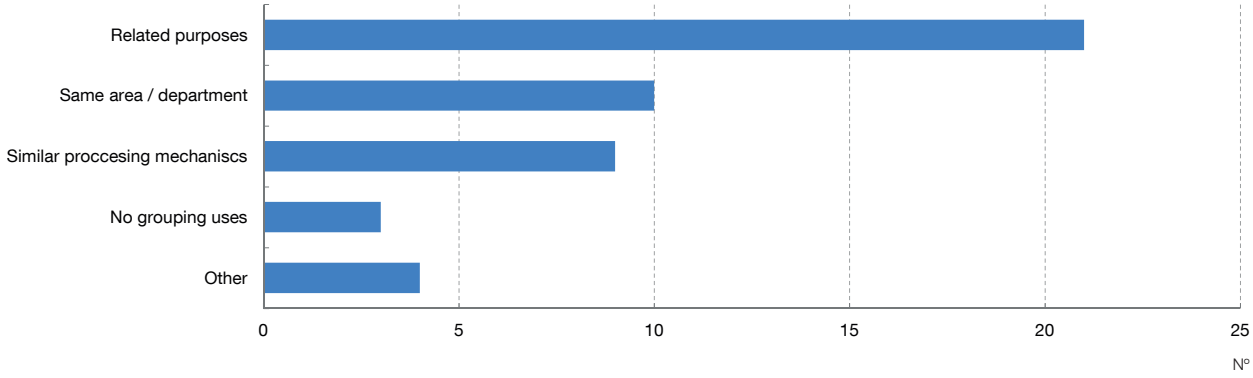


SOURCES: ESCB/SSM institutions (Annex 2).

Chart 4 presents the breakdown of the criteria most commonly used for grouping purposes. Three NCBs/NCAs stated that they do not perform any grouping. In terms of other criteria that are used for grouping, two NCBs/NCAs stated that they perform supra-grouping either for the purpose of privacy notices (for the sake of clarity, ease of reading/understanding) or for recording of processing activities in a public register.

Chart 4

NUMBER OF NCBs/NCAs USING GROUPING CRITERIA



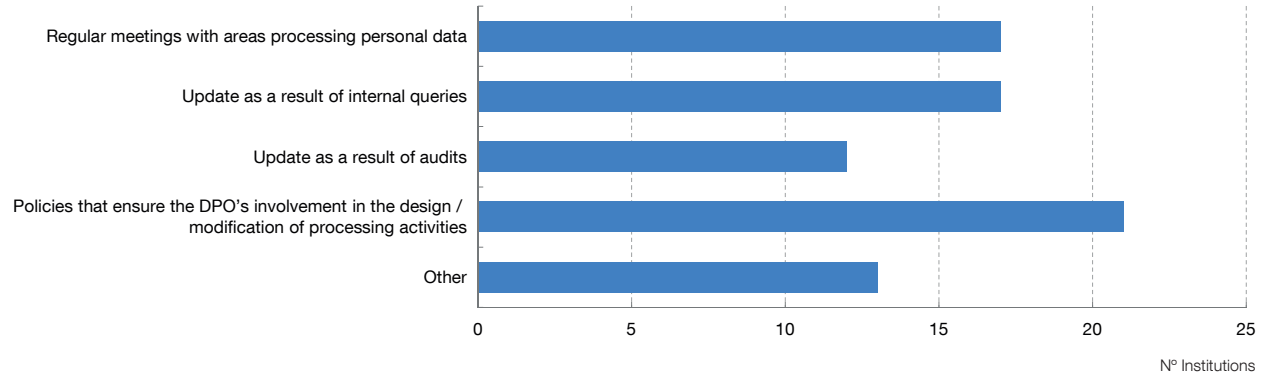
SOURCES: ESCB/SSM institutions (Annex 2).

3.4 Ways in which NCBs/NCAs ensure that records of processing activities are up to date

The most usual way whereby the NCBs/NCAs make sure the records of processing activities are up to date is by introducing policies that ensure that the DPO is involved in the design/modification of the processing activities. Other noteworthy ways involve using configuration management database (CMDB) monitoring, automatic alerts whenever a new processing activity is entered on the record

of processing activities, involvement of the DPO in projects, recurring monitoring carried out by the DPO, or alerts by first-line data privacy champions[9] (see Chart 5).

Chart 5
WAYS IN WHICH NCBs/NCAs MAKE SURE THE RECORDS OF PROCESSING ACTIVITIES ARE UP TO DATE



SOURCES: ESCB/SSM institutions (Annex 2).

3.5 Publishing records of processing activities

Only three NCBs/NCAs publish the records of processing activities:

— The Spanish NCB/NCA, as a public institution, is legally obliged to make the register accessible in electronic form, pursuant to Art. 31(2) of the Spanish Data Protection Act.[10] The online register can be consulted here: https://www.bde.es/bde/en/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de-acti/.

— The ECB, pursuant to Art. 31(5) EUDPR,[11] is obliged to make the central register recording its processing activities publicly accessible. It can be consulted here: https://www.ecb.europa.eu/ecb/access_to_documents/data_protection/html/index.en.html.

— The Latvian NCB publicly provides a general overview of the purposes and lawfulness of personal data processing; categories of personal data; personal data recipients; place of processing, data storage and protection; and data subject rights. This information is available here: https://www.bank.lv/en/about-us/useful/processing-of-personal-data.

9 The privacy champions are employees who act as point of contact for the DPO and centralise privacy and data protection concerns within the business areas.

10 https://www.boe.es/eli/es/lo/2018/12/05/3.

11 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552577087456&uri=CELEX:32018R1725.

4 Legal bases and special circumstances for data processing (Art. 6 - 11 GDPR)

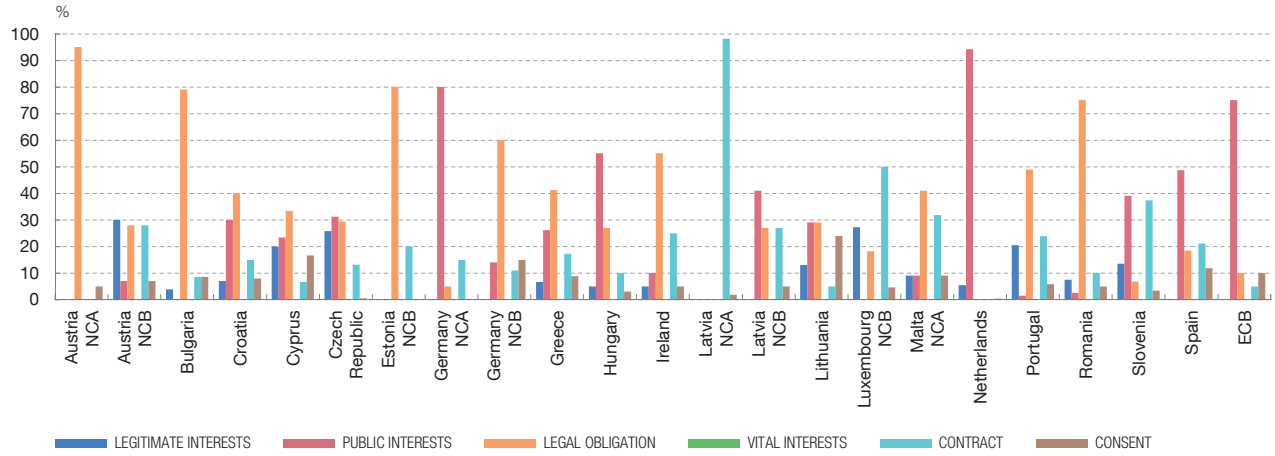
One of the cornerstone principles of the GDPR is that personal data shall be processed lawfully. Art. 6 GDPR presents the lawful bases for personal data processing. However, some aspects concerning legal bases have been regulated or interpreted differently in certain jurisdictions (e.g. some jurisdictions do not allow public institutions to base any processing activities on legitimate interests). As a result, even though the mandate of all participating NCBs/NCAs is essentially comparable – which a priori would lead any reader to conclude that the same legal bases should apply to analogous processing activities – in practice, substantial differences are observed.

4.1 Legal bases assigned by NCBs/NCAs

In order to be able to compare how legal bases are assigned, given the diverse grouping criteria and resulting number of processing activities, respondents were asked to provide the percentage of the legal bases to which they assign their processing activities. As is evident from Chart 6, there is no one way to decide on the legal basis for the processing activities performed by the NCBs/NCAs: some report having based almost all their activities on Art. 6(1)(b) GDPR (performance of a contract), Art. 6(1)(e) GDPR (public interest) or Art. 6(1)(c) GDPR (legal obligation), respectively, whereas others do not base any of their processing activities on these bases.

Nevertheless, there are two consistent trends: no NCBs/NCAs base their processing activities on Art.6(1)(d) GDPR (vital interests), and only four use Art. 6(1)(a) GDPR (consent) as the legal basis for more than 10% of their processing activities, whereas most NCBs/NCAs make only marginal use of this legal base.

Chart 6
LEGAL BASES



SOURCES: ESCB/SSM institutions (Annex 2).

4.2 Legitimate interests as a basis for processing activities of NCBs/NCAs

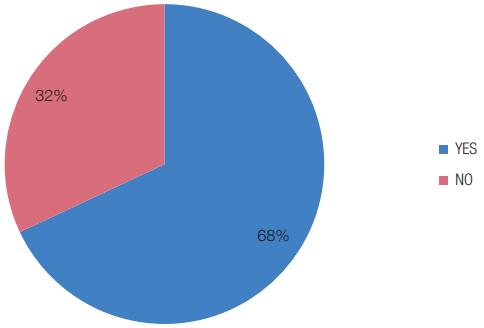
It is particularly noteworthy that approximately two-thirds of the NCBs/NCAs reported having processing activities based on Art. 6(1)(f) (legitimate interests), while the other third reported not

using that legal basis at all (see Chart 7). In most cases, the processing activities reported as being based on legitimate interest were connected with managing events (e.g. participants' lists, taking and posting pictures, travel arrangements) or monitoring and controlling working hours or employees' use of IT equipment and security (e.g. CCTV surveillance).

Among the reasons why some NCAs/NCBs refrain from using legitimate interests as a legal basis for processing, the ECB states that the EUDPR does not allow personal data processing on the basis of legitimate interests, while other NCBs/NCAs, such as the Spanish NCB/NCA, explain that their national DPA expressly discourages the use of legitimate interests as a legal basis for public institutions.

Chart 7

IS THERE ANY PROCESSING ACTIVITY BASED ON LEGITIMATE INTERESTS IN YOUR INSTITUTION?



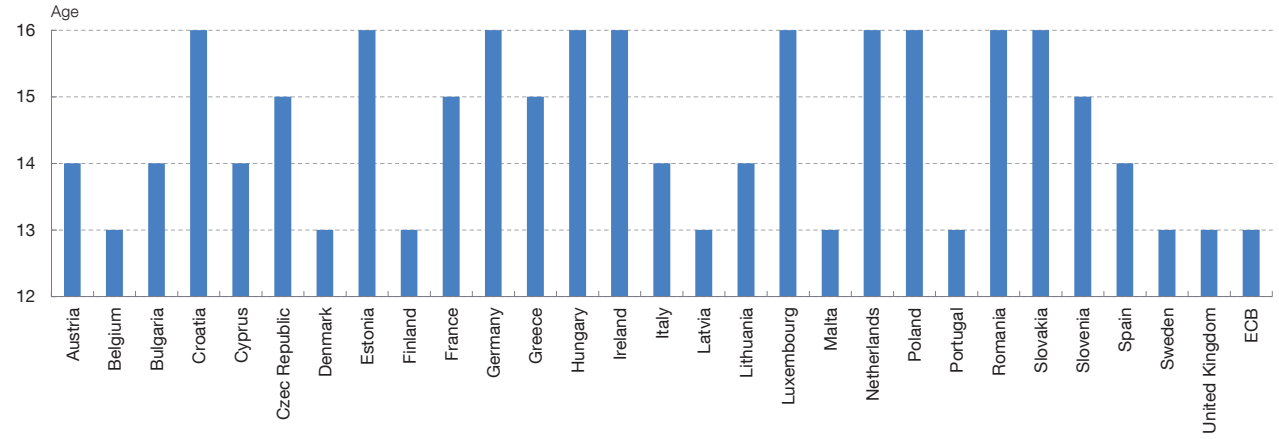
SOURCES: ESCB/SSM institutions (Annex 2).

4.3 Age at which national regulations consider processing of a child's data to be lawful without parental representation

As the GDPR grants certain discretion to Member States to establish the age of consent for data protection purposes between 13 and 16 years, respondents were asked to provide information on their national legislation in this regard (see Chart 8). The information for those jurisdictions for which none was provided was obtained from public sources.

Chart 8

NATIONAL AGE OF CONSENT WITHOUT PARENTAL REPRESENTATION



SOURCES: ESCB/SSM institutions (Annex 2).

4.4 Processing of special categories of personal data and data relating to criminal convictions

One NCB reported that it does not have any processing activities that include special categories of personal data or data relating to criminal convictions. All other NCBs/NCAs reported having at least one processing activity that includes these type of personal data (maximum number reported: 77).

Most NCBs/NCAs named processing activities that include special categories of personal data or data relating to criminal convictions, such as fit and proper (F&P) assessments, human resources (HR). matters and access control to buildings, special areas or server rooms. In particular, for F&P assessments, criminal record checks are carried out; in HR activity, in addition to pre-employment criminal record checks, occupational health, health insurance or membership data are processed; and in access control to buildings / special areas / server rooms, biometric data are processed.

4.5 Maximum retention periods

NCBs/NCAs indicated that national rules concerning maximum retention periods were in place in only three jurisdictions:

— The Cypriot NCB/NCA reported the need to *keep the personal data for former clients (including related parties/guarantors) for 10 years after the termination of contractual relationships. In the event of pending litigation or an investigation by a public authority of the Republic of Cyprus, the period shall start to run from the date of their final termination.*

— The French NCB and NCA pointed out that *in some case, French DPA (CNIL) can provide specific retention periods in its referentials.*

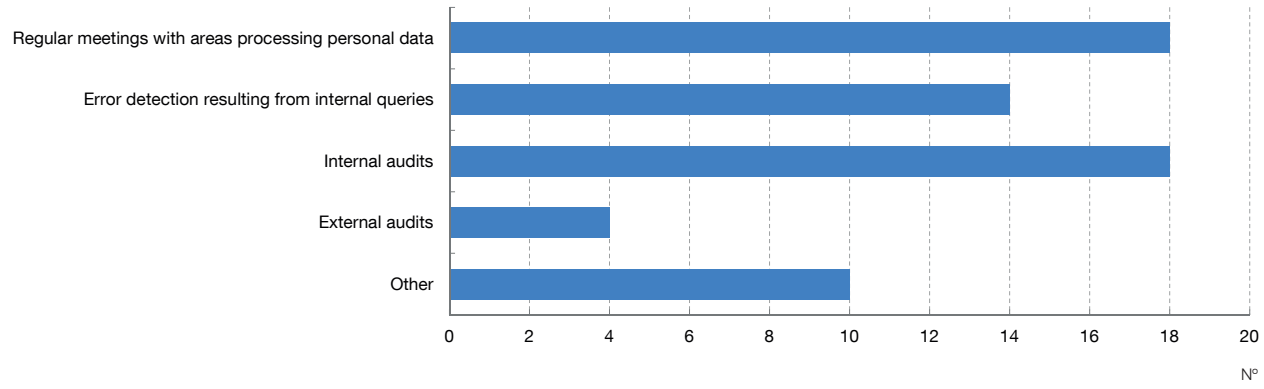
— In addition, both the Latvian NCB and NCA noted that national rules do not establish general maximum retention periods. However, they cited the following rules: *A data subject may receive information regarding recipients or categories of recipients of its data to which data have been disclosed over the last two years; and If an obligation is imposed on the controller to ensure storage of audit trails of the system, they shall be stored for not longer than one year after making of an entry, unless laws and regulations or nature of processing stipulates otherwise.*

5 Transparency (Arts. 13 and 14 GDPR)

Another key principle of the GDPR is transparency, enshrined in Arts. 13 and 14. In this section of the survey, the NCBs/NCAs responded to questions on the way they ensure that information clauses are duly recorded on forms: all institutions reported having at least one way to do so, while 19 NCBs/NCAs reported using multiple ways. The most common ways are regular meetings with areas processing personal data and internal audits (see Chart 9).

Chart 9

NUMBER OF NCBs/NCAs USING THE FOLLOWING WAYS TO ENSURE THAT INFORMATION CLAUSES ARE DULY RECORDED ON FORMS



SOURCES: ESCB/SSM institutions (Annex 2).

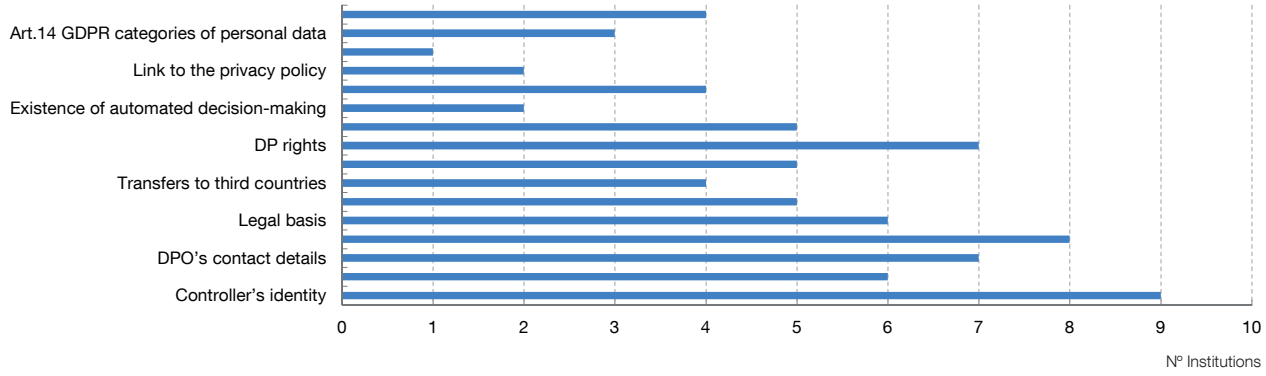
Other ways reported by the NCBs/NCAs to ensure that information clauses are duly recorded on forms are the following:

- template forms including information clauses;
- standard information clauses distributed to business units;
- monitoring by the DPO;
- occasional meetings with areas processing personal data;
- update as a result of internal queries;
- internal training and awareness campaigns;
- internal verification processing.

5.1 Summarising the information of Arts. 13 - 14 GDPR as a first layer

Eight NCBs/NCAs reported the possibility of summarising the information of Arts. 13 - 14 GDPR as a first layer. However, the mandatory content of the first layer is not consistent across jurisdictions (see Chart 10).

Chart 10
MANDATORY CONTENT FOR THE FIRST LAYER



SOURCES: ESCB/SSM institutions (Annex 2).

6 Exercise of rights requests (Arts. 12 and 15 – 23 GDPR)

The GDPR places much weight on the active accountability of the controller and stresses the need for data subjects to be able to exercise their rights properly. In this section, a closer look is taken at how NCBs/NCAs process the exercise of rights requests.

6.1 Public credit registries containing personal data

Of the participating NCBs, 15 report having public credit registries processing personal data. In six of those jurisdictions (i.e. Cyprus, France, Italy, Latvia, Portugal and Spain) personal data rights are subject to restrictions pursuant to Art. 23 GDPR. For example, the French NCB keeps a national register of household credit repayment incidents (FICP); data subjects cannot object to the processing or ask for data to be erased before the end of the retention period.

6.2 Number of requests processed in 2018-2019

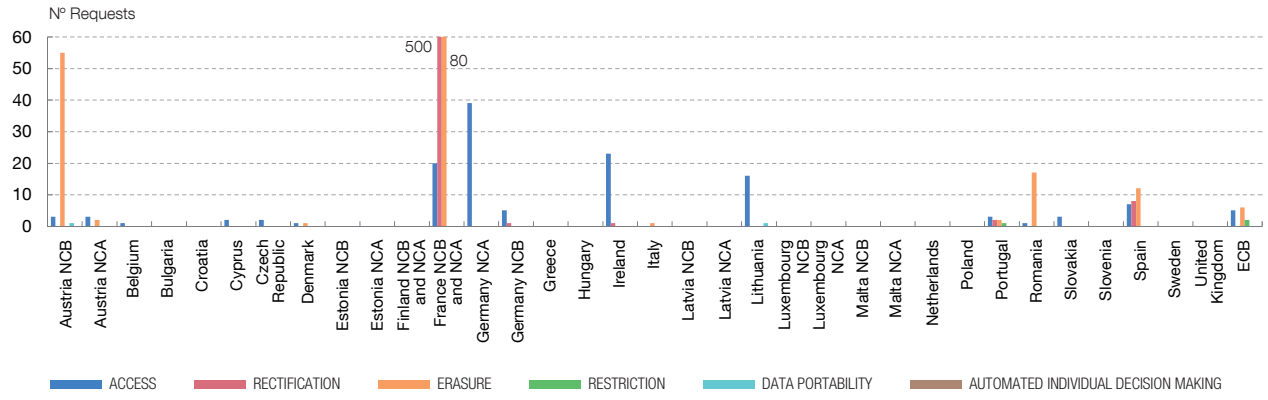
The overall number of requests per year reported by the NCBs/NCAs was rather low, with the exception of the French NCB and NCA which reported 500 rectification requests in 2018, relating to mailing lists and recruitment.

In addition, only the following NCBs/NCAs reported having received more than 25 requests per year, excluding those relating to public credit registries.

INSTITUTION	REQUESTS IN 2018	REQUESTS IN 2019
Austrian NCB	59	64
German NCA	39	48
Irish NCB/NCA	24	35
Portuguese NCB/NCA	8	26
Spanish NCB/NCA	27	54

The other NCBs/NCAs stated having received 25 or fewer requests per year excluding those relating to public credit registers (see Chart 11 and Chart 12).

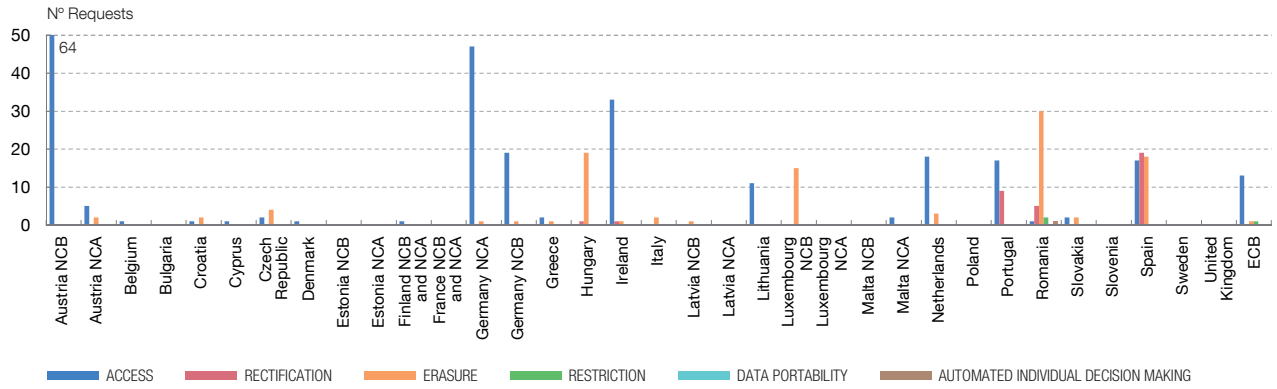
Chart 11
NUMBER OF REQUESTS IN 2018



SOURCES: ESCB/SSM institutions (Annex 2).

Chart 12

NUMBER OF REQUESTS IN 2019

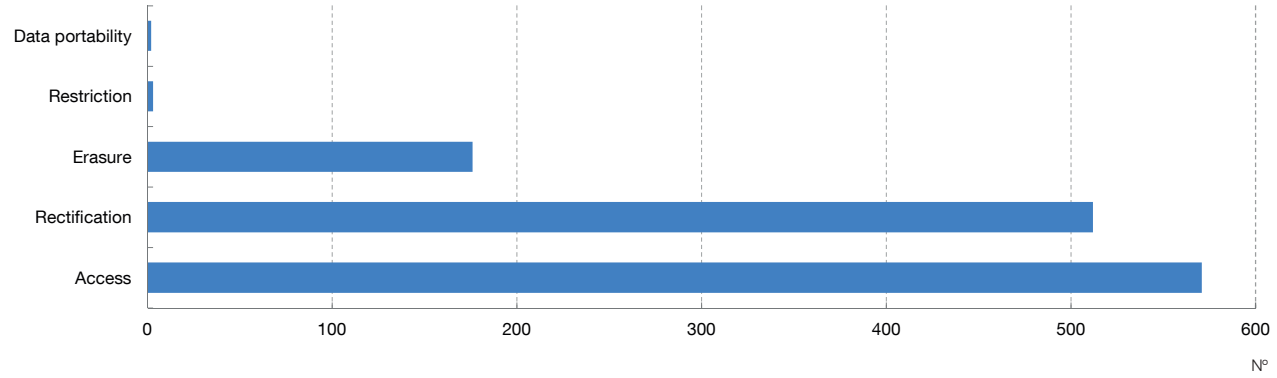


SOURCES: ESCB/SSM institutions (Annex 2).

As depicted in Chart 13 and Chart 14 below, most of the requests processed by the NCBs/NCAs concern access to personal information, rectification and erasure. The NCBs/NCAs received only a couple of single requests concerning restriction, data portability and automated individual decision-making.

Chart 13

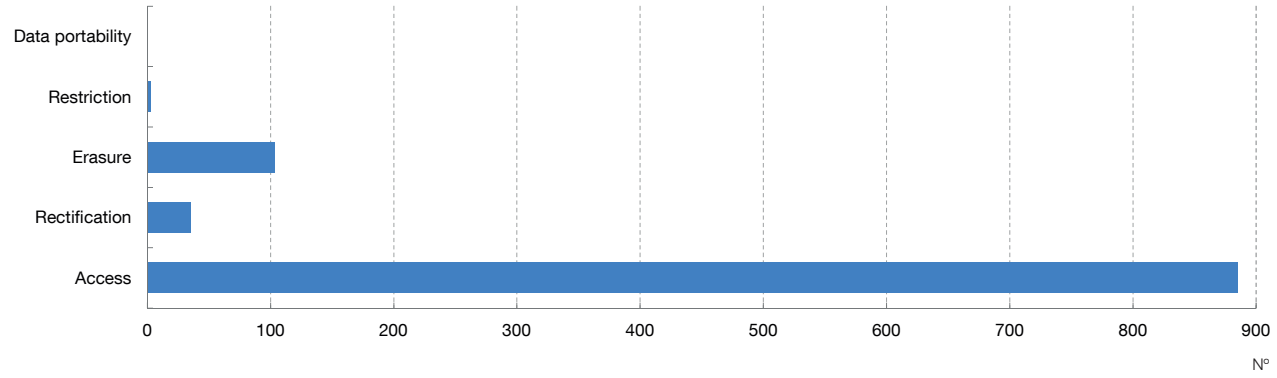
NUMBER OF REQUESTS PER TYPE IN 2018



SOURCES: ESCB/SSM institutions (Annex 2).

Chart 14

NUMBER OF REQUESTS PER TYPE IN 2019



SOURCES: ESCB/SSM institutions (Annex 2).

6.3 Possibility of requesting specification as to which processing activity a request relates

Of the participating NCBs/NCAs, 67% reported being entitled to request specification where it is not clear to which processing activity a request relates. However, most of the NCBs/NCAs[12] explained that no specific national legal provisions or guidelines regulate this possibility. In this regard, the ECB adopts, in its internal procedures, the following approach:

"Whilst an individual is entitled to access to any or all of their personal data, where a controller processes a large quantity of information concerning the individual, the controller should be able to request that the individual clarifies the request, by specifying the information or processing activities which they want access to or information on. This should only be done where reasonably necessary to clarify a request, and not to delay in responding to it. Where a controller asks an individual to clarify their request, they should let them know as soon as possible. If the individual refuses to clarify the request, the controller will still need to comply with the original request".

6.4 Activities in which NCBs/NCAs process the most requests

Most requests processed by NCBs that keep public credit registers relate to said register. As a result, in order to compare the practice of different NCBs/NCAs, it is important to filter out this category. The French NCB receives more than 800,000 access requests relating to the public credit register every year. In the case of the Irish NCB/NCA, the DPO noted that access to records held on the public credit register is facilitated through a separate mechanism.

Notwithstanding the above, the other areas where NCBs/NCAs process most requests are HR (i.e. job applications, employee relations), numismatic activity (e.g. online stores selling collector coins) and general requests from members of the public. The ECB was the only NCB/NCA that reported that most requests received related to banking supervision.

6.5 Rejected requests in 2018 and 2019

Most NCBs/NCAs report either not having rejected any requests or not having available data in this regard. Of the eleven NCBs/NCAs that reported having rejected requests, ten had rejected fewer than five requests in each year.

The main reason cited by the NCBs/NCAs for the rejections was a lack of evidence of the applicant's identity. Other reasons referred to by the NCBs/NCAs were:

- rejection of access on the grounds of supervisory confidentiality;
- rejection of data portability on the grounds that the data to be transferred were not submitted by the data subject;
- rejection of erasure where there is a legal obligation to keep the data or the data are kept for reasons of public interest.

12 The Spanish NCB/NCA reported that the Spanish Data Protection Act expressly entitles data controllers to request specification.

Concerning banking secrecy, 57% of the NCBs/NCAs reported that they do not provide access to personal data included in documents protected by banking supervisory secrecy. However, most of these NCBs/NCAs added comments clarifying that they provide only those (extracted) data relating to the requesting person and only if it is possible to pass over words and sentences protected by banking supervisory secrecy.

6.6 Data subject identification

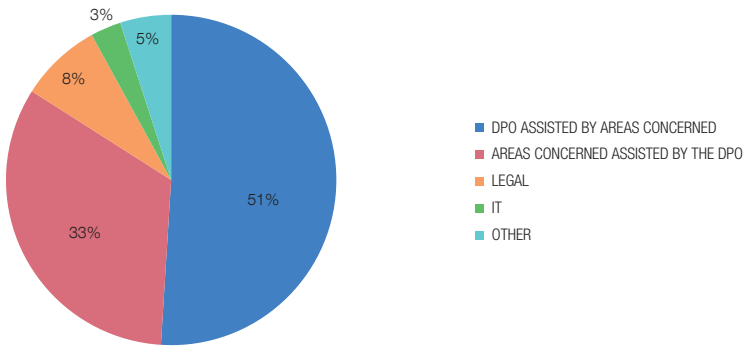
Practically all NCBs/NCAs identify the data subject by requesting a copy of the person's ID/passport or other official proof of identity (e.g. driver's licence) containing relevant information such as identification number, country of issue, period of validity, name, address and date of birth. All other information that is not required for identification purposes can be blacked out. Other means of identification mentioned by several NCBs/NCAs were a qualified electronic or authenticated signature and an employee's internal email address. The Latvian NCA noted that applicants identify themselves via an official system by connecting to the system using their internet banking credentials.

6.7 Right to object vs public interest

About 61% of the NCBs/NCAs report having processing activities where the right to object is overridden by reasons of public interest. These include processing activities where public interest is the legal basis, in particular: financial market supervision, including F&P assessments; data kept on public credit registers; data held for surveillance, anti-money laundering (AML), corruption prevention or national security purposes; data processed for statistical purposes, including central balance sheet offices; and administrative infringement and penalty procedures.

6.8 Areas handling requests

Chart 15
WHO PROCESSES REQUESTS?



SOURCES: ESCB/SSM institutions (Annex 2).

As depicted in Chart 15, in most NCBs/NCAs, requests are processed by either the DPO assisted by the business units concerned or the business units concerned assisted by the DPO. Only in very few cases are Legal and IT departments involved. In this regard, three NCBs/NCAs reported that

the Legal department is involved in handling requests, but only in Denmark does this department lead the assessment. One NCB/NCA reported that the IT department is involved alongside the DPO assisted by the business unit concerned and the Legal department. None of the NCBs/NCAs report that the Compliance department is involved.

6.9 Claims against the NCBs/NCAs for non-GDPR compliance

Eight NCBs/NCAs report having had to deal with claims submitted by data subjects to the DPA for alleged non-compliance with GDPR. The main reasons reported by the NCBs/NCAs are the following:

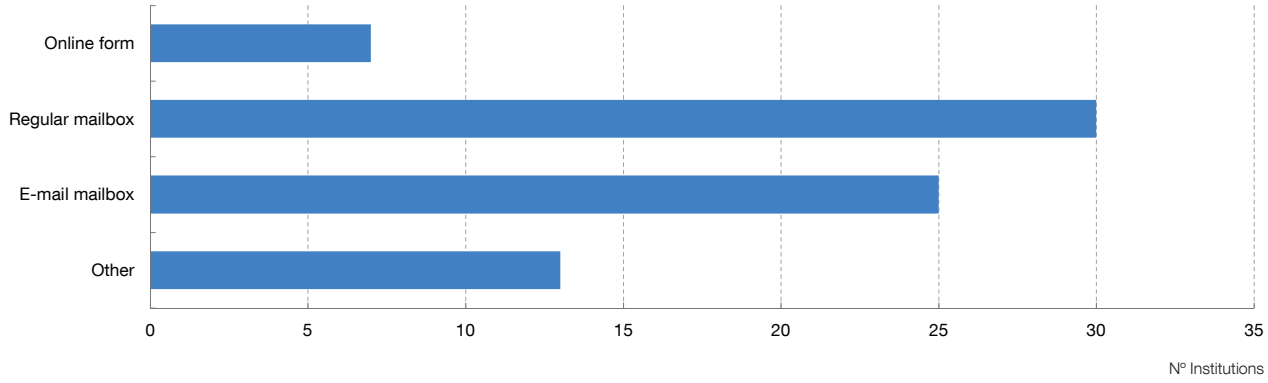
- lack of understanding of Art. 23 GDPR restrictions for public credit registers;
- alleged unlawful transmission of data;
- disagreement over legitimate interests;
- disagreement over data exchange between authorities;
- dissatisfaction caused by rejection of requests

Additionally, one NCB/NCA reports that the DPA initiated ex officio proceedings to assess the lawfulness of the processing activities based on public interest and legitimate interests.

6.10 Channels for exercise of data protection rights

As depicted in Chart 16, Most of the NCBs/NCAs provide multiple ways for data subjects to exercise their data protection rights. For the Czech NCB/NCA, it can be any conceivable channel (including by phone, in person at the Czech NCB/NCA or by delivery of the application to the Czech NCB/NCA mail/submissions room). All of the NCBs/NCAs provide an electronic channel, either an email mailbox or an online form. For 25 NCBs/NCAs, applicants can also submit their requests by regular mail. As regards, other channels for exercise of data protection rights, seven NCBs/NCAs report the possibility of filing requests in person at the NCB's/NCA's premises. Additionally, one NCB/NCA mentions an online portal for submitting requests.

Chart 16
CHANNELS TO EXERCISE DATA PROTECTION RIGHTS



SOURCES: ESCB/SSM institutions (Annex 2).

In the vast majority of cases reported by the NCBs/NCAs, the applicants use appropriate channels to submit requests. Most of the NCBs/NCAs mentioned that if an incorrect channel is used, requests are forwarded to the DPO internally. However, only two NCBs/NCAs report that many data subjects do not use appropriate channels to exercise data protection rights. In the extreme case of the Spanish NCB/NCA, 233 out of 253 requests forwarded related to the department in charge of the public credit register (CIRBE), as a result of persons basing their requests on GDPR rather than on the specific regime applicable under Art. 23 GDPR to the public credit register. A specific template reply has been prepared to address this scenario and has been sent to the team in charge of the CIRBE.

6.11 Processing and recording requests

Most of the participating NCBs/NCAs have set up a procedure to process and record requests where: first the requesting person's identity is verified; then the business unit in charge of the processing activity is involved; and subsequently the answer prepared is sent to the person who submitted the request and is filed in internal records. Some NCBs/NCAs note that the Legal department is also involved in drafting the reply. In addition, some NCBs/NCAs report certain noteworthy particularities:

- The Irish NCB/NCA records all incoming requests in a register log placed on a MS SharePoint platform, which tracks and provides a countdown to the time available for response.

- The Slovenian NCB/NCA reports that all requests relating to data kept on the public credit register are processed through an online application accessible via an official digital certificate whereby:

  - applicants may access the data recorded on the register free of charge;

  - records may be kept on when the data have been consulted and by whom;

- complaints may be submitted;

- reports may be exported in pdf format.

— Lastly, the Czech NCB/NCA sets out a detailed procedure for processing and recording requests. This may be useful for those NCBs/NCAs that are still fine-tuning their internal procedures. The procedure is structured as follows:

1 Receipt of the request by the DPO either directly or through other business units.

2 Verification of the applicant's identity by the DPO.

3 Assessment by the DPO of whether the request is standard or not (e.g. unreadable, unintelligible, confusing, etc.).

4 Assessment by the DPO of the eligibility of the request (pre-conditions for the possibility to make a request set out in the GDPR).

5 Assessment by the DPO of whether the request is manifestly unfounded or disproportionate (e.g. the request lacks justification or a large number of requests come from the same applicant).

6 Assessment by the DPO of whether an exclusion or restriction of rights is applicable (e.g. supervisory secrecy or public credit register restrictions; in general restrictions stemming from Art. 23 GDPR as adopted and refined in national legal instruments).

7 Exercise of the data subject's right. If the DPO is unable to ensure the exercise of the right directly, other business units are involved.

8 Assessment by the DPO of whether the exercise of the data subject's right does not adversely affect the rights and freedoms of others (Art. 15(4) GDPR).

9 Drafting by the DPO of the reply to the request (and dispatch of the reply).

Additionally, the following formalities are undertaken:

- Each request is assigned a registration number.

- All documents are kept by the DPO in an electronic folder dedicated to the request and located on a drive to which only the DPO has access.

- All communications relating to the request are recorded on the NCB/NCA's information system.

— If other business units are involved, a dedicated shared electronic folder is created on a drive to which the business units have access. Once the business unit's involvement is over, the DPO copies the dedicated electronic folder to the drive to which only the DPO has access and subsequently deletes the shared folder.

— Where the data subject's request is on paper, all hardcopy documents are kept in a locked cabinet to which only the DPO has keys.

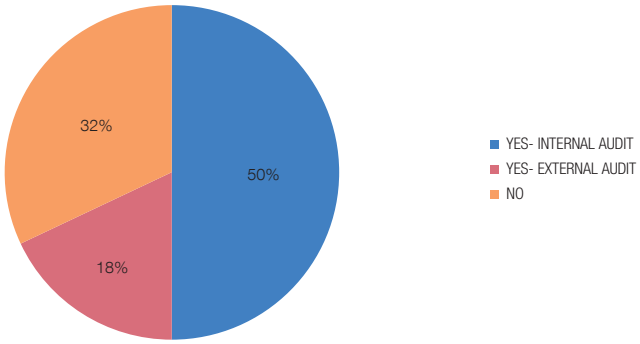
7 Privacy by design and by default (Art. 25 GDPR)

Through Art. 25, GDPR requires the controller to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This implies that privacy needs to be embedded by design and by default. As a result, in this section, NCBs/NCAs elaborated on how they have achieved or plan to achieve the privacy by design and default status.

7.1 GDPR compliance audits

Twenty NCBs/NCAs report having performed either an internal or an external audit to check their GDPR compliance, including three NCBs/NCAs that have performed both. However, 11 DPOs state that their NCBs/NCAs have not yet performed any GDPR compliance audit (see Chart 17). The scope of the audits reported varied from covering only single departments (e.g. HR) to covering the whole institution. Some NCBs/NCAs also commented that they either conduct an annual data protection exercise jointly with Internal Audit, where all data processing activities are analysed and corrective actions are taken, or recurring audits over a 3-year time frame.

Chart 17
HAS YOUR NCB/NCA PERFORMED ANY AUDIT TO MAKE SURE IT COMPLIES WITH THE GDPR?



SOURCES: ESCB/SSM institutions (Annex 2).

7.2 Application of proper technical and organisational security measures

As depicted in Chart 18, almost all the NCBs/NCAs use either assistance from the CISO or standard security measures elaborated in collaboration with the chief information security officer (CISO), or apply specific measures set out in national regulations/guidelines. However, there are some other interesting practices that have been reported to ensure that proper security measures are taken:

- standard security measures aligned with DPIA methodology;
- hardcopy documents locked in cabinets with restricted access;
- application of ESCB information security policies;

— interaction with SRM – WG;[13]

— ISO 27001 ISMS and ISO 27002/2017 criteria;

— common classification of IT risks.

Chart 18
HOW DO YOU ENSURE A PROPER LEVEL OF SECURITY WHEN PROCESSING PERSONAL DATA?

SOURCES: ESCB/SSM institutions (Annex 2).

7.3 Policies to ensure privacy is considered by default

Of 31 NCBs/NCAs, 24 confirm having polices to ensure that privacy is considered by default. Most cases cite internal polices/handbooks involving the DPO at early stages, but other interesting policies were reported, such as:

— oaths taken in court by all employees;

— records management policies;

— guidelines on management of ESCB/SSM confidential information;

— public credit register regulations;

— confidentiality policies;

— policies on prevention of abuse of insider information;

— codes of conduct;

— IT policies.

13 Storage Resource Management (SRM) Working Group: https://sdm.lbl.gov/srm-wg/.

In this regard, the Portuguese NCB/NCA reports having drafted both a general guide on personal data processing and a specific guide on privacy by design and by default. Additionally, the Dutch and Spanish NCBs/NCAs report that they are currently drafting specific privacy policies. In the case of the Spanish NCB/NCA, the policy will allocate specific responsibilities to business units taking part in the processing, the DPO and the CISO, as follows:

1 The business unit concerned will inform the DPO prior to starting/modifying a processing activity and will complete a questionnaire detailing the main aspects of the processing activity.

2 The DPO will provide guidance regarding which technical/organisational measures will be adopted to safeguard data protection by design and by default. These measures will be recorded in a report and drafted in collaboration with the CISO.

8 Data processors and joint controllers (Arts. 26 and 28 GDPR)

The GDPR places different requirements on parties to processing activities. This section sheds light on the types of processing activities performed by data processors or through joint controller arrangements.

8.1 Joint controller arrangements

Of 31 NCBs/NCAs, 12 report acting as joint controllers in activities beyond the scope of ESCB IT-shared services, SSM common procedures and FMIs, such as the following:

- the Austrian NCB and NCA, joint controllers over the processing of a joint database pursuant to the Austrian Banking Act;
- the Danish NCB and NCA, joint controllers over the processing of data from financial institutions;
- the Danish NCB and the Danish Business Authority, joint controllers over a 12week payment statistics project;
- the Greek NCB/NCA and the Greek Employees' Healthcare Fund, joint controller/data processing agreement;[14]
- the Irish NCB/NCA and an educational establishment, joint controllers over the processing of employees' personal data to provide specific training courses leading to a subsequent university qualification;
- the Latvian NCB and the Proxy Registry "Instant Links", joint controllers over the processing of an online database for linking mobile phone numbers and other identifiers to credit institution customer account numbers for instant payments;[15]
- the Slovak NCB/NCA, joint controller with certain providers (e.g. travel agencies, security services, photo or video recording services, external auditors);
- the Spanish NCB/NCA and the Spanish Stock Exchange Commission, joint controllers over processing of data to promote financial education.

8.2 Updating agreements with data processors

Only the Spanish Data Protection Act provides for a time frame to regularise agreements with data processors executed prior to application of the GDPR. Under this framework, agreements with

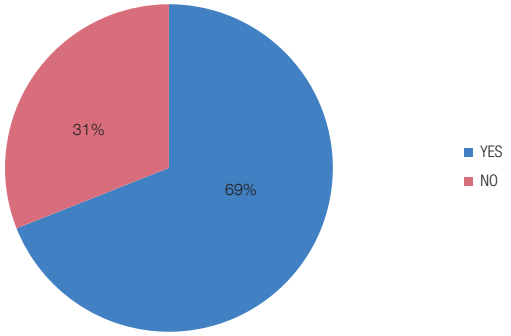
14 The agreement between the Greek NCB/NCA and the Greek Employees' Healthcare Fund provides that the NCB and the Fund are joint controllers with respect to specific processing activities, while they act as controller/processor with respect to other processing activities (specified in the agreement).

15 https://www.bank.lv/en/tasks/payment-systems/proxy-registry-instant-links.

data processors executed before 25 May 2018 will remain in force until their expiration date or, if subject to an indefinite term, until 25 May 2022, notwithstanding the right of any party to request the agreement to be adapted to Art. 28 GDPR provisions.

Chart 19

HAS YOUR INSTITUTION CHECKED ALL THE AGREEMENTS EXECUTED WITH DATA PROCESSORS PRIOR TO THE APPLICATION OF GDPR TO MAKE SURE THEY COMPLY WITH ARTICLE 28 GDPR?



SOURCES: ESCB/SSM institutions (Annex 2).

In terms of the status of their agreements with data processors, approximately two-thirds of the NCBs/NCAs have already updated all their agreements to comply with Art. 28 GDPR (see Chart 19). In this regard, the Austrian NCB indicates that the updating process started in 2016. In addition to drafting standardised amendments and templates for the purposes of Art. 28 GDPR, the Austrian NCB has also rolled out an enhancement of the ISO 27001supplier management process to ensure that all agreements with processors are GDPR compliant.

Apart from the Austrian NCB, other NCBs/NCAs also report standardised amendments for data processors. The Croatian NCB/NCA has also taken this opportunity to reconsider re-insourcing some outsourced activities (e.g. recruitment).

None of the institutions reported having any problems with data processors disagreeing with the Art. 28 GDPR related update.

Approximately one-third of the NCBs/NCAs have not yet checked all the agreements executed with data processors to ensure that they comply with Art. 28 GDPR. In this regard, one NCB/NCA reports prioritising critical agreements (e.g. IT and HR), two NCBs/NCAs update contracts when they are to be renewed and two NCBs/NCAs consider the updating of agreements as an ongoing process.

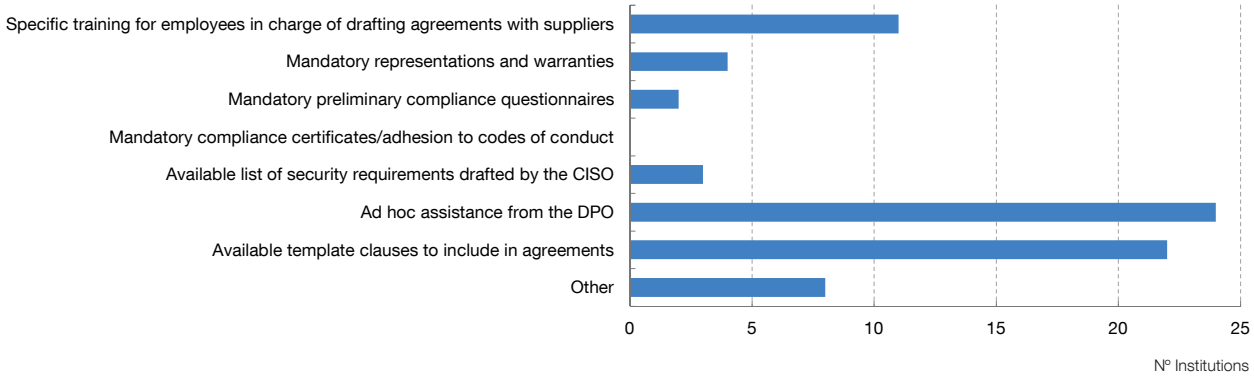
8.3 Detecting and documenting agreements with data processors

The main ways in which the NCBs/NCAs are detecting and documenting agreements with data processors are by ad hoc assistance of the DPO and the availability of template clauses. Additionally, 35% of the respondents report using specific training for employees in charge of processing agreements with suppliers as a way of ensuring compliance with Art. 28 GDPR.

Only a few institutions make use of lists of security requirements drafted by the CISO, mandatory representations and warranties or preliminary compliance questionnaires. None of the NCBs/NCAs reported requiring mandatory compliance certificates or adhesion to codes of conduct (see Chart 20).

Chart 20

HOW DOES YOUR NCB/NCA MAKE SURE AGREEMENTS WITH DATA PROCESSORS ARE DULY DETECTED AND DOCUMENTED PURSUANT TO ART. 28 GDPR?



SOURCES: ESCB/SSM institutions (Annex 2).

The measures listed as "Other" comprise ad hoc assistance from the business units concerned and setting up policies, which ensure that the Procurement and Legal departments check agreements with suppliers before entering into new agreements.

The Lithuanian NCB/NCA notes that all requirements to be included in agreements with data processors have been formalised in the general personal data processing regulations adopted by the institution. Additionally, it is currently in the process of specifying the regulations on security requirements to be demanded of partners and service providers. Nevertheless, to date, technical requirements also form part of the agreement.

8.4 Auditing data processors

Almost half of the NCBs/NCAs report carrying out audits on data processors based on specific audit clauses that provide for audits with a short notice period, and requiring that data processors make available, at the controller's request, information evidencing compliance with obligations set forth in the agreement. The scope and time frame of the audits usually vary and are assessed on a case-by-case basis, taking into account the risks associated with the processing activities concerned. One NCB/NCA notes that they perform annual audits on organisational and technical measures implemented by data processors.

NCBs/NCAs approach auditing data processors in several ways. Some use only audit reports, while others take a risk-based approach, carrying out on-site inspections on standard and higher risks and document-only checks for low-risk processing.

Additionally, some NCBs/NCAs prioritise auditing the information security of a small number of critical vendors who process sensitive data, or impose on the business units concerned the obligation to monitor annually that data processors are acting in accordance with the contract, with the assistance of the DPO and/or internal audit.

8.5 NCBs/NCAs acting as data processors

Almost half of the NCBs/NCAs report acting as data processors for certain processing activities, nevertheless noting that these circumstances are exceptional. The following processing activities were given as examples:

- the Austrian NCB provides IT services to its subsidiaries;
- the Belgian and the Dutch NCBs/NCAs act as joint data processors for the provision of services on a cash single-shared platform (SSP);
- the Bulgarian NCB/NCA maintains a nationwide online platform for information exchange among financial institutions;
- the Danish NCB acts as data processor providing IT services to associations and funds associated with the NCB;
- the Maltese NCA acts as data processor providing assistance to other NCAs or supervisory authorities;
- the Spanish NCB/NCA considers that SSM NCAs act as data processors for SSM supervision activities and F&P assessments of significant institutions;
- the Italian NCB/NCA acts as a data processor providing services to the Italian insurance market regulator;
- the Cyprus NCB/NCA acts as data processor providing services on behalf of competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and prevention of threats to public security.

9 Personal data breaches (Arts. 33 and 34 GDPR)

The GDPR requires that personal data breaches be notified without undue delay to the DPA, unless they are unlikely to result in a risk to the rights and freedoms of natural persons. Where they are likely to result in a high risk to the rights and freedoms of natural persons, they must be notified to the natural person concerned without undue delay.

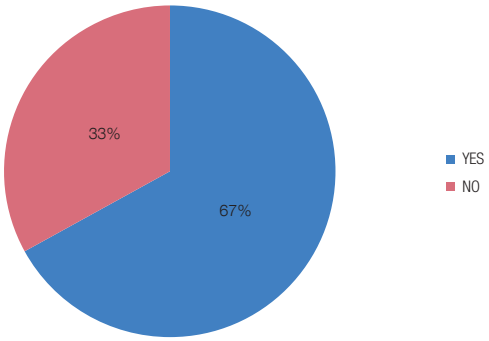
In this section of the report, a closer look is taken at how the NCBs/NCAs fulfil the above-mentioned GDPR notification requirements.

9.1 Personal data breaches and notifications

Approximately two-thirds of the NCBs/NCAs report having experienced personal data breaches (see Chart 21). In half of the cases these breaches were notified to the DPA and in a quarter of the cases the data subjects were also notified.

Chart 21

HAS THERE BEEN ANY PERSONAL DATA BREACH IN YOUR INSTITUTION SINCE THE APPLICATION OF GDPR?



SOURCES: ESCB/SSM institutions (Annex 2).

The institutions reported from one to 38 breaches, with the exception of one NCB/NCA which experienced 200 personal data breaches in 2019 due to incorrect reporting of details by lenders to the public credit register, according to initial guidelines provided by the national DPA in 2019. However, following discussion with the national DPA, a revised approach to the reporting of these errors will be adopted and the number of breaches is expected to decrease significantly in 2020.

In terms of types of data breaches, the institutions reported breaches caused by:

- software malfunctions;
- a large-scale DDoS attack, which made access to the corporate internet infrastructure temporarily unavailable;

— a breach experienced by an IT data processor that made leisure time benefits data in employees' profiles temporarily unavailable;

— loss of devices, data carriers and/or hardcopy documents including personal data;

— personal data sent or handed over to the wrong recipients;

— incorrect access permissions to IT systems;

— storage of counterparties' personal data on an employee's personal computer and mobile phone;

— unauthorised disclosure to the media of the employment status of two employees.

9.2 Mandatory notification of personal data breaches to the DPA and data subjects

Of the responding NCBs/NCAs, 55% report having a formula/risk matrix to assess whether the personal data breach notification obligation is triggered. In terms of assessment, several NCBs/NCAs report using ENISA methodology,[16] some adjusting it to their specific needs. Others reported using matrixes that take into account the impact of a personal data breach and its risk probability.

The ECB stated using the following criteria to assess the risk: (i) elements of the incident, (ii) categories and number of personal data affected, (iii) categories and number of persons affected, (iv) likelihood of the consequences, and (v) mitigation measures to address the incident.

The Finnish NCB and NCA both use a matrix provided by the Finnish DPA. Also, the Spanish NCB/NCB uses a formula provided by the Spanish DPA. This formula was shared with all the NCBs/NCAs at the 2019 Network meeting and was adopted by the Austrian NCB.[17]

In this regard, the Portuguese NCB/NCA notes that no formula/risk matrix has been approved and all data breaches need to be notified to the Portuguese DPA. In order to assess whether data subjects need to be notified, the Portuguese NCB/NCA may use the ENISA methodology. However, a first assessment is made by a data protection steering committee and/or the Board of Directors.

16 Recommendations for a methodology of the assessment of severity of personal data breaches, v1.0.

17 RISK = Volume x (Type x Impact) where:
If risk is higher than 20 OR two qualitative circumstances apply (in red), notification obligation to the DPA is triggered.
If risk is higher than 40 OR two qualitative circumstances apply (in red), notification obligation to the data subject is triggered.

VOLUME		TYPE OF DATA		DISCLOSURE	
< 100 records	1	No special categories	1	No disclosure	2
100 to 1,000 records	2			Internal (company)/controlled	4
1,000 to 100,000 records	3			External (suppliers, attackers)	6
> 100,000 records	4	Special categories	2	Public (internet)	8
> 1,000,000 records	6			Unknown	10

Please note that, in October 2020, the Spanish DPA launched a specific tool to assess the risks arising from personal data breaches and whether they need to be notified (https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd).

9.3 Internal reporting of personal data breaches to the DPO

All but two NCBs/NCAs report having internal policies to make sure that the DPO is informed when a personal data breach is detected. In some NCBs/NCAs internal policies require employees to report data breaches directly to the DPO. In other cases, specific data breach processes and support measures (e.g. data breach notification forms) automatically alert the DPO.

In this regard, a number of NCBs/NCAs also note the importance of raising awareness and of continuous employee training.

9.4 Documenting personal data breaches

In most NCBs/NCAs, DPOs keep record of personal data breaches. However, some NCBs/NCAs report that it is the Legal department that is in charge of keeping records.

The way in which breaches are documented varies between NCBs/NCAs. A number of NCBs/NCAs keep an internal incident register where they record breaches and hold internal databases for all relevant accompanying documentation. Other NCBs/NCAs use reporting templates to document breaches. Lastly, one NCB/NCA reports not having a centralised data breach documentation method.

10 DPIA (Arts. 35 and 36 GDPR)

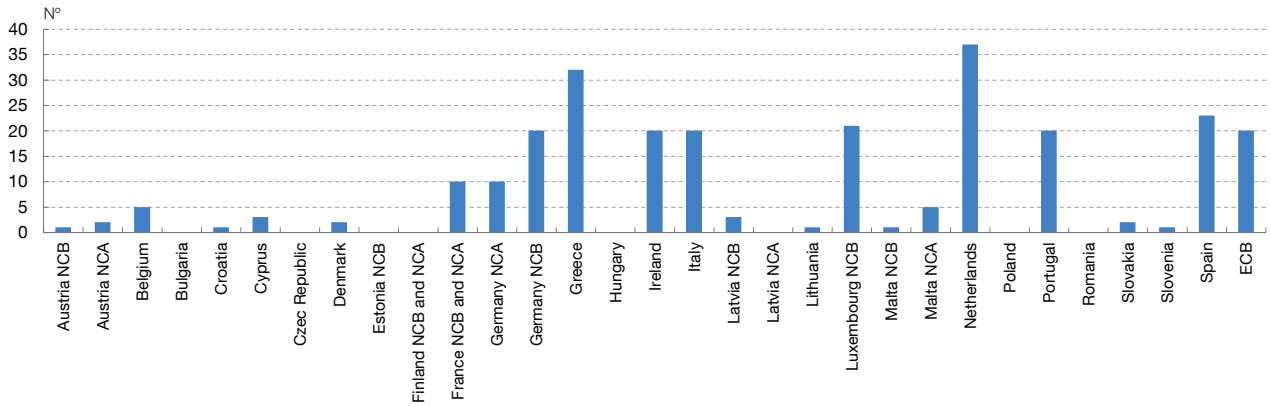
Under Art. 35 GDPR, data controllers must perform a data protection impact assessment (DPIA) on processing activities that are likely to result in high risk to the rights and freedoms of natural persons. Art. 36 GDPR requires that the controller consult the DPA prior to processing in cases where a DPIA indicated that this processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

This part of the report sets out the information reported by respondents on the DPIAs they have performed and whether they have consulted their national DPA pursuant to Art. 36 GDPR.

10.1 Processing activities subject to DPIAs: overall numbers

As depicted in Chart 22, the number of DPIAs reported by the NCBs/NCAs varies widely, ranging from none to 37, with the Dutch and Greek NCBs/NCAs having performed the most DPIAs (37 and 32, respectively). The Czech NCB/NCA reports not having conducted any DPIAs, while underlining that the Czech DPA's methodology on DPIAs is currently under public consultation.

Chart 22
HOW MANY DPIAS HAS YOUR INSTITUTION CARRIED OUT?



SOURCES: ESCB/SSM institutions (Annex 2).

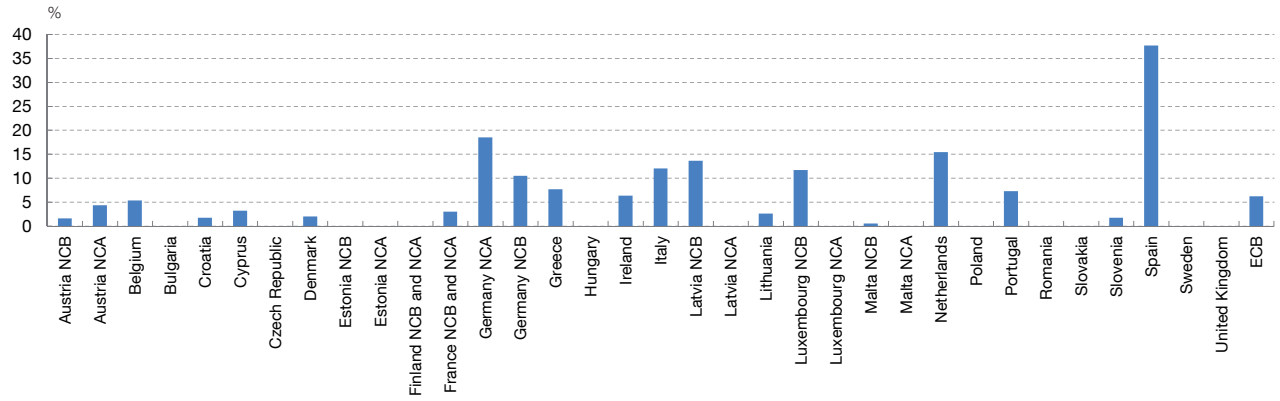
Annex 5 has a list of reported examples of processing activities subject to DPIAs. This may be a useful tool should a NCB/NCA wish to consult precedents on the need to conduct a DPIA under certain conditions.

Some NCBs/NCAs, such as the German NCB, report that most of the DPIAs carried out were due to the national DPA blacklist.

On the scope of the DPIAs, some NCBs/NCAs, such as the Slovenian NCB/NCA, report only conducting DPIAs for processing activities initiated after application of the GDPR, whereas other

NCBs/NCAs, such as the Spanish NCB/NCA, have been expressly instructed by their DPAs to also subject data processing activities that were in place prior to the GDPR to DPIAs. As a result of the above, the percentage of processing activities subject to DPIAs varies.[18] Nevertheless, most of the NCBs/NCAs conducted DPIAs on less than 10% of their processing activities (see Chart 23).

Chart 23
% OF DPIAs OVER TOTAL PROCESSING ACTIVITIES

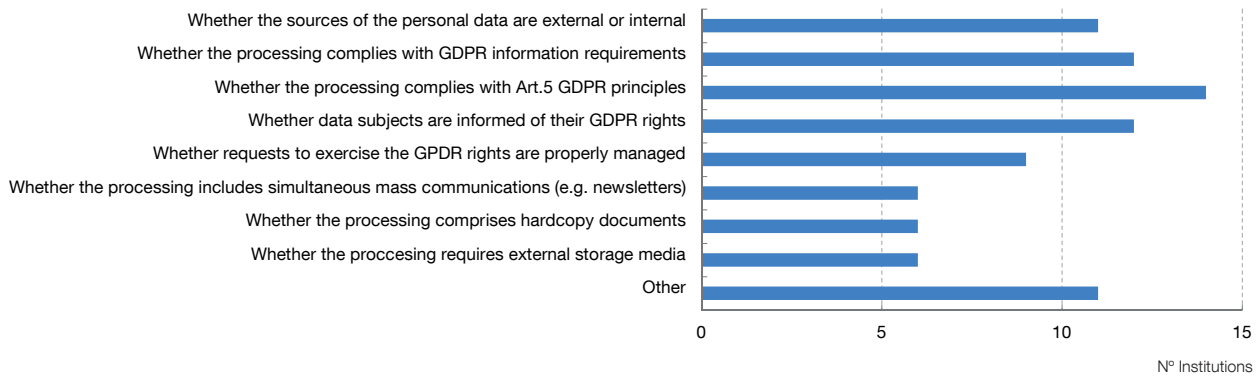


SOURCES: ESCB/SSM institutions (Annex 2).

10.2 Analysing risks for data subjects

Of the responding NCBs/NCAs, 79% declare having a policy to analyse risk for data subjects. The factors that they consider to assess inherent risk and whether a DPIA is required mostly focus on the aspects depicted in Chart 24:

Chart 24
FACTORS TAKEN INTO ACCOUNT TO ASSESS INHERENT RISK AND WHETHER DPIA IS REQUIRED



SOURCES: ESCB/SSM institutions (Annex 2).

18 Number of processing activities stated by the institutions in question 5 of the questionnaire (either pre- or post-grouping, whichever was reported).

Several NCBs/NCAs also report using other ways to assess inherent risk:

— the Bulgarian NCB/NCA uses a decree law, currently repealed, which contains guidelines for evaluation of risks according to the impact on the subjects in the event of a breach;

— the Czech NCB/NCA applies factors introduced in the Czech DPA's guidelines ('List of types of processing operations (not)subject to the data protection impact assessment');

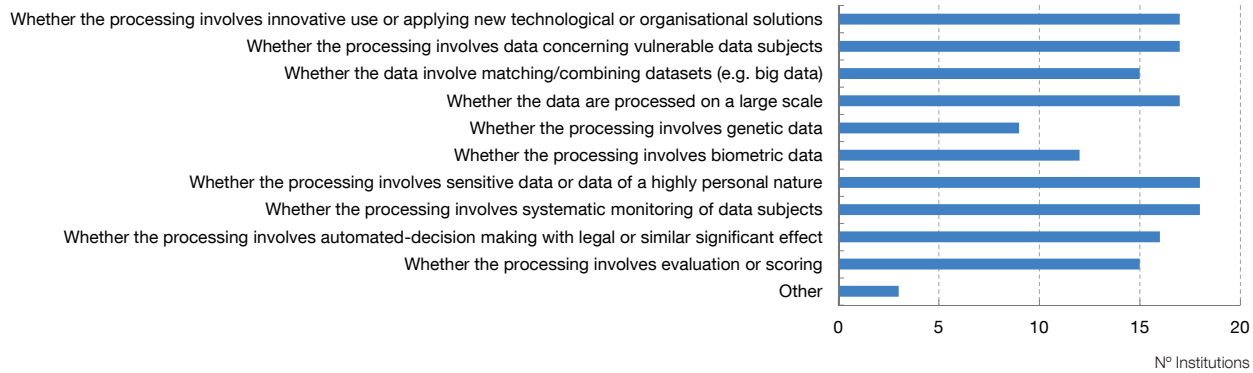
— the French NCB and NCA also check the personal data category and the DPIA blacklist issued by the French DPA;[19]

— the Irish NCB/NCA assesses the level of processed personal data and, also, if the data are being held by external vendors;

— the Lithuanian NCB/NCA examines network and technical resources, how the personal data will be processed, the data processing participants and the scope of the processing.

In this regard, when assessing the need to perform a DPIA, most of the NCBs/NCAs also take into account the criteria contained in the EDPB *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,*[20] and in particular the factors depicted in Chart 25.

Chart 25
EDPB DPIA FACTORS



SOURCES: ESCB/SSM institutions (Annex 2).

Among the factors listed as "Other" by the NCBs/NCAs:

— the Czech NCB/NCA assesses whether the data are sensitive but do not belong to a special category (e.g. financial data) and whether the data subject has reasonable expectations that the processing will take place;

19 https://www.cnil.fr/fr/listes-des-traitements-pour-lesquels-une-aipd-est-requise-ou-non.

20 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

— the Italian NCB/NCA assesses whether the data will be transferred to other controllers;

— the Lithuanian NCB/NCA also conducts DPIAs where:

  — notifying data recipients of personal data rectification, erasure or restriction of processing in accordance with Article 19 of the GDPR proves impossible or would involve a disproportionate effort;

  — personal data are processed for video surveillance in at least one of the following: (i) in premises and/or territories not owned by the controller or managed on other legal grounds; (ii) at healthcare, social care, detention establishments and other agencies where services are provided for vulnerable data subjects; or (iii) combined with sound recording;

  — telephone conversations are recorded;

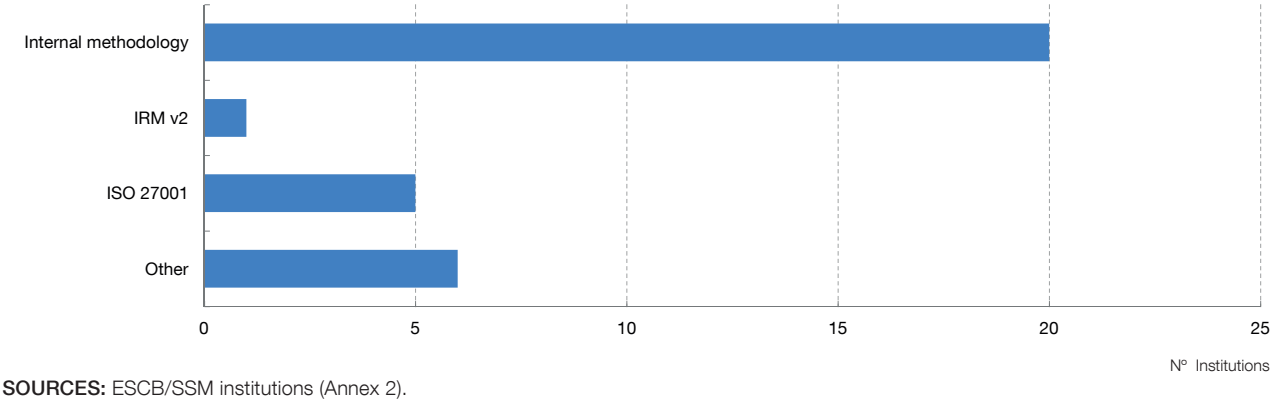
  — personal data of children are processed for direct marketing purposes, subject to automated-decision making, including profiling, or information society services are offered to children directly;

  — employees are being monitored for control purposes.

10.3 DPIA tools

Of the responding NCBs/NCAs, 77% stated that they have a specific questionnaire to perform DPIAs. Most of these questionnaires are based on internal methodologies. However, in some cases, they are supported by ISO 27001 guidelines and, in the case of one institution, the IRM v2. ISO 27001 standard was named as the sole basis of a questionnaire (see Chart 26).

Chart 26
DPIA QUESTIONNAIRE BASIS



SOURCES: ESCB/SSM institutions (Annex 2).

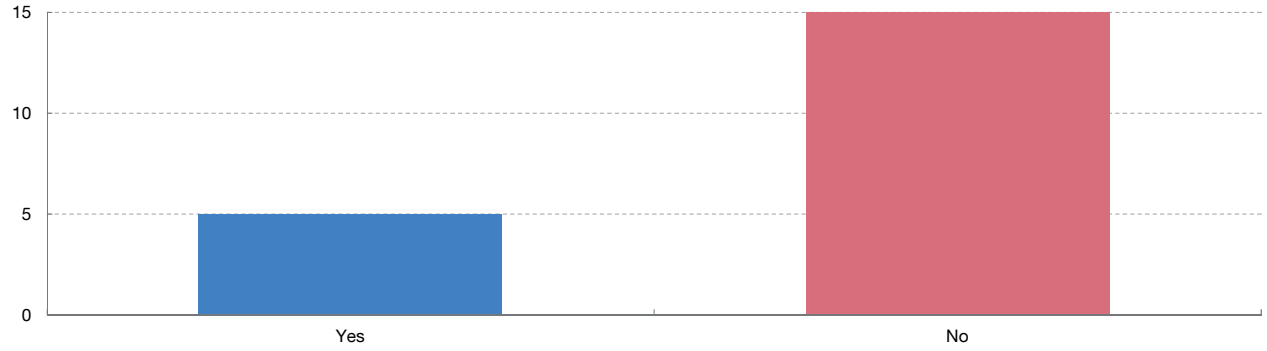
Six NCBs/NCAs report using other sources for their DPIA questionnaires, namely:

- the Czech NCB/NCA, although still waiting for the Czech DPA's methodology subject to public consultation, reports that the planned methodology will take into account internal methodologies (operational risks management, IT safety profiles), ISO 27000 and other external methodologies (e.g. ISO/IEC 29134);
- the French NCB and NCA use open source software provided by the French DPA;[21]
- the Luxembourg NCB based its questionnaire on methodology provided by an external consultant (EY);
- the Dutch NCB/NCA uses a simplification of the DPIA laid out by the Dutch government;
- the Slovak NCB/NCA takes into account the requirements stated in the National DPA regulation;
- the Spanish NCB/NCA uses the methodology provided by the Spanish DPA in its Guidelines on DPIAs.

Five NCBs/NCAs report using the same questionnaire to assess the risks related to personal data and those related to all other data managed by their institution (see Chart 27).

Chart 27

DOES YOUR INSTITUTION USE THE SAME METHODOLOGY TO ASSESS THE RISKS RELATED TO PERSONAL DATA AND THOSE RELATED TO THE REST OF THE DATA MANAGED BY YOUR INSTITUTIONS?



SOURCES: ESCB/SSM institutions (Annex 2).

10.4 Large-scale processing activities

When defining "large scale" for the purposes of Art. 35 GDPR, almost all of the NCBs/NCAs rely on a case-by-case estimation without specific thresholds. NCBs/NCAs mostly undertake this estimation

21 https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

guided by Article 29 WP – Guidelines on DPIA as adopted on 4 April 2017.[22] However, some of the NCBs/NCAs provide specific thresholds, criteria or formulas:

— The Bulgarian NCB/NCA reports considering large-scale processing only in the case of monitoring public areas, which they do not do.

— The Czech NCB/NCA points to the criteria to consider large-scale processing provided by the Czech DPA: *"from 10,001 data subjects or more than 1.0 ‰ of the population of the Czech Republic or the countries concerned; and/or over 20 persons/employees of the controller, who have access to personal data concerned; and/or more than 20 processing sites/branches; and at the same time the state level (NUTS = NUTS1) in terms of origin / location of subjects data".*

— The Polish NCB considers large-scale processing to be when it concerns over 100 persons.

— The Spanish NCB/NCA has designed the following formula on the basis of the Article 29 WP Guidelines:

If [average of basic factors + (∑ qualifying factors)] ≥ 2 Large scale

Where:

Basic factors

No. of data subjects	No. of data categories	Occasional vs recurring processing	Geographical scope
☐ 0 to 1,000 (0.5)	☐ 1 to 3 (1)	☐ occasional (1)	☐ Regional (1)
☐ 1,001 to 10,000 (1)	☐ 4 to 6 (2)	☐ recurring (2)	☐ National (2)
☐ 10,001 to 100,000 (2)	☐ 7 to 9 (3)		☐ International (3)
☐ More than 100,000 (3)			

Qualifying factors

☐ Special categories of data (0.5)
☐ Large-scale innovative tech (big data, AI...) (0.5)

— Additionally, the Slovenian NCB/NCA notes that in Slovenia large-scale processing activities would normally be defined by law and the assessments would have to be conducted by the legislator.

10.5 Consultation with the DPA under Art. 36 GDPR

Only 19% of the NCBs/NCAs consulted report having consulted their national DPA prior to processing where a DPIA performed under Article 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by these institutions to mitigate risk:

22 *"Factors, in particular, be considered when determining whether the processing is carried out on a large scale[15]:*
a the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b the volume of data and/or the range of different data items being processed;
c the duration, or permanence, of the data processing activity;
d the geographical extent of the processing activity".

— the Cypriot NCB/NCA;

— the Maltese NCB;

— the Portuguese NCB/NCA;

— the Romanian NCB/NCA;

— the ECB.

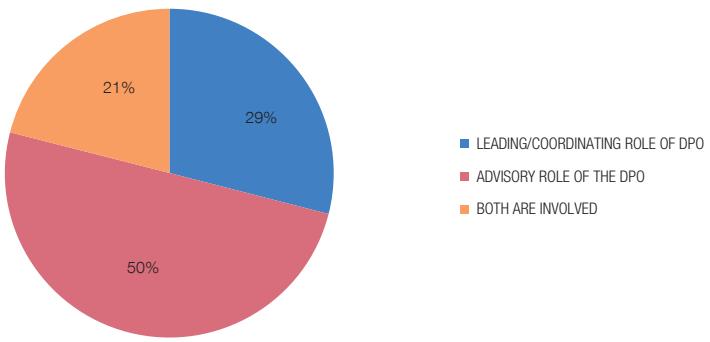
10.6 DPO and IT department involvement in DPIAs

As regards the involvement of the DPO and the IT department in conducting DPIAs (see Chart 28), most NCBs/NCAs report the DPO having an advisory role in providing guidance either on the drafting or the approval of DPIAs performed by the respective business units concerned. However, some NCBs/NCAs note, in particular, that the DPO will advise on mitigation measures and will validate the DPIA in order to assess the need for a prior consultation pursuant to Art. 36 GDPR and provide recommendations in this regard.

In eight cases, the NCBs/NCAs highlight a leading/coordinating role of the DPO, reporting either that DPIAs are carried out or coordinated by the DPO, or that the DPO provides a template and pre-completes forms after a first assessment together with the department responsible. These included the Dutch and the Spanish NCBs/NCAs which reported that, as the business areas concerned are not sufficiently proficient in GDPR matters to perform DPIAs, it is the DPO that takes the leading role.

In roughly one-fifth of cases, the NCBs/NCAs do not specify the roles of the DPO and the IT department in DPIAs, reporting that both parties are involved and work together.

Chart 28
WHAT IS THE INVOLVEMENT OF THE DPO AND OF THE IT DEPARTMENT?



SOURCES: ESCB/SSM institutions (Annex 2).

11 DPOs (Arts. 37 – 39 GDPR)

Arts. 37 to 39 GDPR set out the requirements concerning DPOs. Art. 37(1)(a) requires that public authorities processing personal data appoint a DPO. This encompasses all the EU NCBs/NCAs. Art. 38 establishes the requirements as to the position of the DPO in the institutions and Art. 39 concerns the tasks of the DPO.

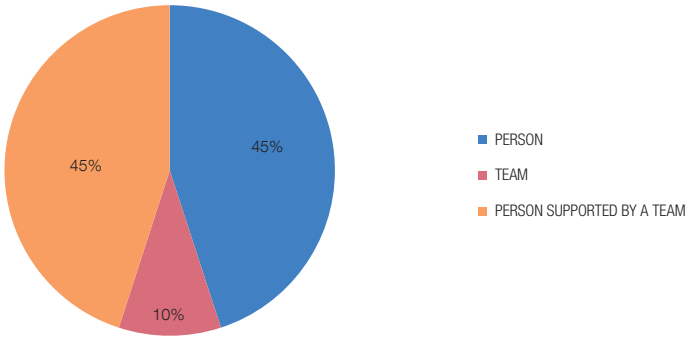
Following the GDPR, the questionnaire addresses the practical aspects that need to be taken into account by DPOs, such as their position in the structure of the NCBs/NCAs, the scope of their duties, professional background, certifications (if any), use of templates and IT support tools, their approach to GDPR compliance, training, awareness campaigns and handling of queries. This part also covers information on the networks to which DPOs belong.

11.1 DPOs: organisation and position in the NCBs'/NCAs' structure

In most NCBs/NCAs, the DPO is either a single person or a person supported by a team. Only four NCBs/NCAs structure the DPO as a joint team: the French NCB and NCA, which have a single DPO for both institutions, the Maltese NCB and the Spanish NCB/NCA (see Chart 29).

The teams supporting the DPOs vary in number from one to four persons, some full-time and some only part-time.

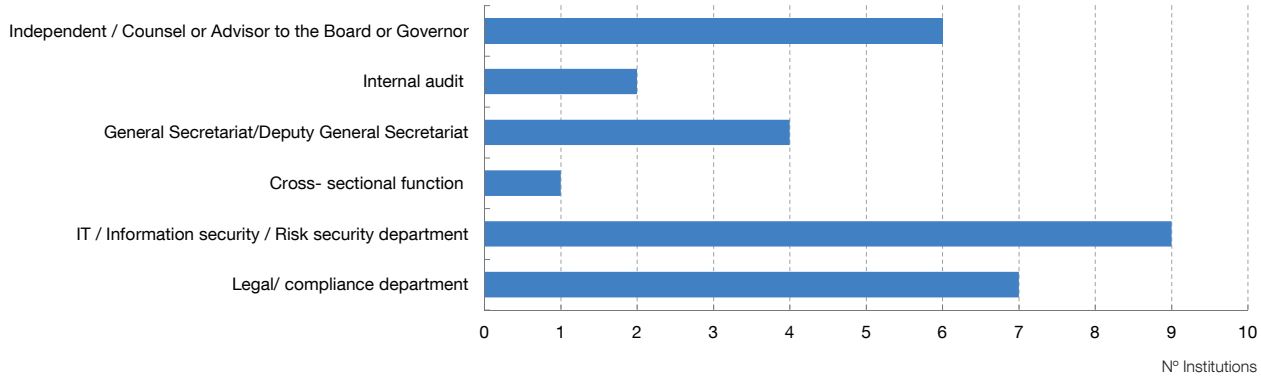
Chart 29
IS THE DPO A PERSON OR A TEAM OR A PERSON SUPPORTED BY A TEAM?



SOURCES: ESCB/SSM institutions (Annex 2).

In terms of where the DPO stands in the organisational structure, all but three DPOs have direct reporting lines to either the Governors or the highest management bodies. Two DPOs belong to the Legal Department and report to the Department Head. One DPO belongs to the Security Department and in practice reports to the Head of the Security Department, despite reporting theoretically to top management. Chart 30 summarises the areas where the DPO is situated in the NCB/NCA organisational chart.

Chart 30
DEPARTMENTS IN WHICH DPO IS SITUATED

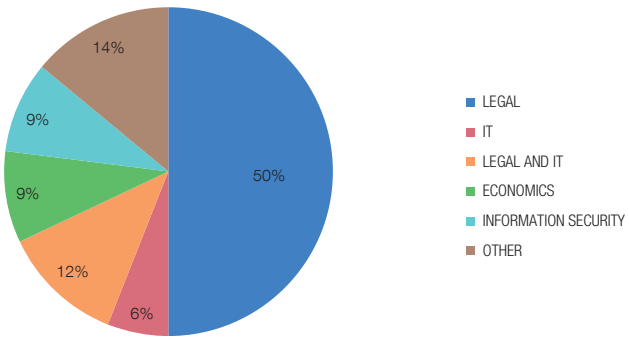


SOURCES: ESCB/SSM institutions (Annex 2).

11.2 DPO background and certifications

As depicted in Chart 31, even though most DPOs report having a legal background, four DPOs report having a dual background in IT and law. Other DPOs report having a background in IT, economics and information security, as shown in the chart below. The DPOs declaring a different background include an engineer, an auditor, a psychologist and a HR expert:

Chart 31
BACKGROUND OF THE DPO



SOURCES: ESCB/SSM institutions (Annex 2).

Only one-third of the DPOs report that they have been issued with certification either by their national DPAs (Belgian NCB/NCA and Latvian NCB) or through private certifications:

— Austrian NCB DPO: CIS-CERT;[23]

— Austrian NCA DPO: TUV Academy certification;[24]

23 https://at.cis-cert.com/.

24 https://www.tuv.com/world/en/data-protection.html?verbid=131.

— Czech NCB/NCA DPO: IAPP–CIPP/E, CIPM, CIPT, and EIPA certification for DPOs;

— Hungarian NCB/NCA DPO: System Media Kft. certification and Educational Centre of the Chamber of Hungarian Auditors;

— German NCA DPO: EIPA certification for DPOs;

— Latvian NCA DPO: EIPA certification for DPOs;

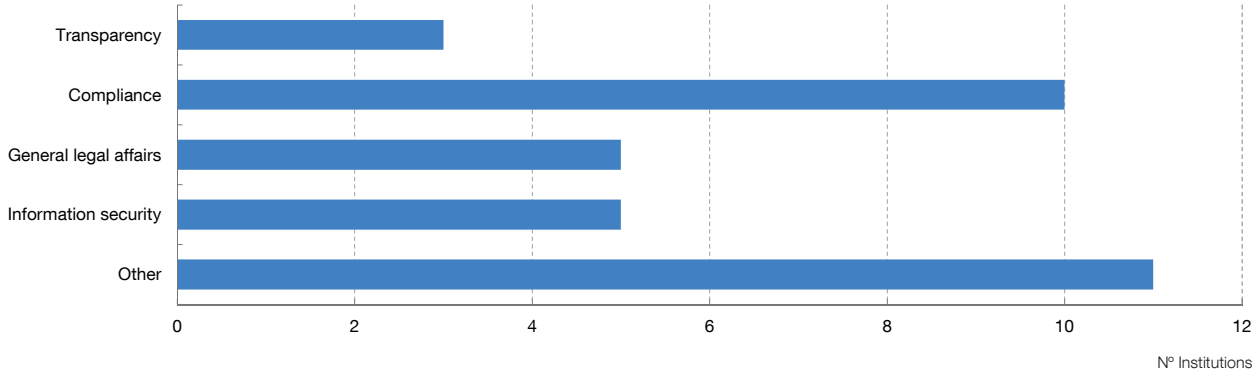
— Maltese NCB DPO: University of Malta DPO certification;

— Dutch NCB/NCA DPO: IAPP–CIPP certification.

11.3 DPO dedication

Only 32% of the DPOs report being dedicated exclusively to data protection matters. The most common other areas handled by DPOs are compliance, legal affairs, information security and transparency (see Chart 32).

Chart 32
OTHER AREAS HANDLED BY THE DPOs



SOURCES: ESCB/SSM institutions (Annex 2).

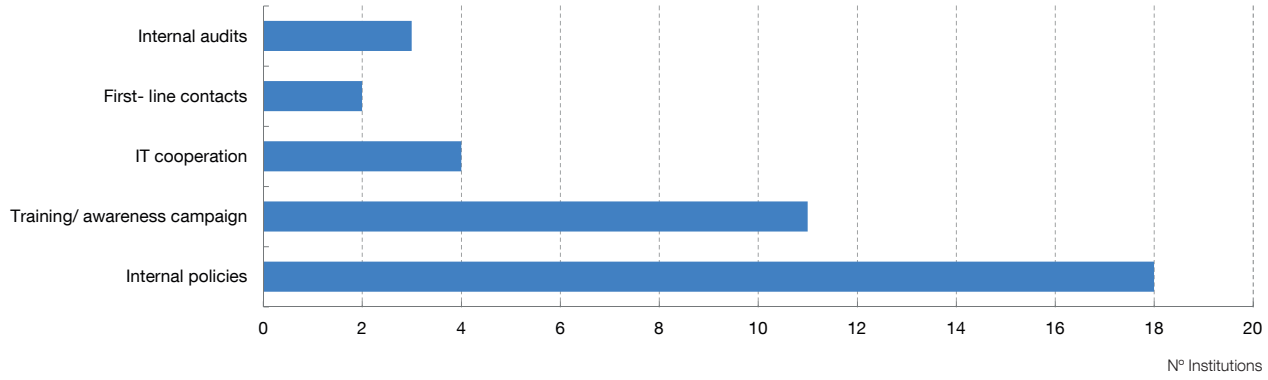
The "Other" areas in the chart comprise IT law, second line defence on banknotes, legal department budget, general risk, security and compliance, governance/ethics, employee safety, SSM coordination issues, HR matters, complaints against the institutions, registry of agreements executed with public institutions and whistleblowing channels.

11.4 DPO involvement

The main ways to ensure the proper and timely involvement of DPOs in all matters concerning data protection are through internal policies that oblige employees to inform the DPO about issues related to data protection and that require the DPO's opinion on projects that include

data protection matters, as well as information and awareness campaigns and training (see Chart 33).

Chart 33
DPO INVOLVEMENT



SOURCES: ESCB/SSM institutions (Annex 2).

As most of the DPOs rely on the employees to actively search for the DPO's opinion, it is important to constantly raise awareness and build trust in the help provided by the DPO on data protection matters. The Greek and Dutch DPOs underlined the importance of having specific liaison officers (first-line contacts) for data issues within each department of the bank, to alert the DPO to data protection issues.

Some DPOs pointed out that close cooperation between the DPO and the IT department is also important as most data are processed through IT systems. For example, the Czech DPO commented that all ICT projects must be submitted to the DPO for comments and that the DPO is also a member of the ICT Committee where every project is discussed and (ultimately) adopted.

Other DPOs added that internal audits help to ensure their proper and timely involvement in all personal data protection issues.

11.5 External IT support tools for DPOs

Only three DPOs report using external GDPR support tools, namely:

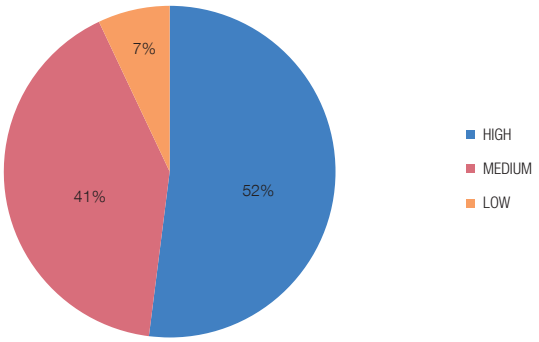
- the Austrian NCA: DataReg;
- the Danish NCB: ISMS system;
- the Portuguese NCB/NCA: GlobalSuite.

Additionally, the French NCB and NCA and the Greek NCB/NCA noted that they are planning to implement IT support tools soon.

11.6 Level of awareness about DPOs in institutions

Approximately half of the DPOs report a high level of awareness about their functions in the institution they represent. However, two DPOs report a low level of awareness (see Chart 34).

Chart 34
LEVEL OF AWARENESS ABOUT THE DPO



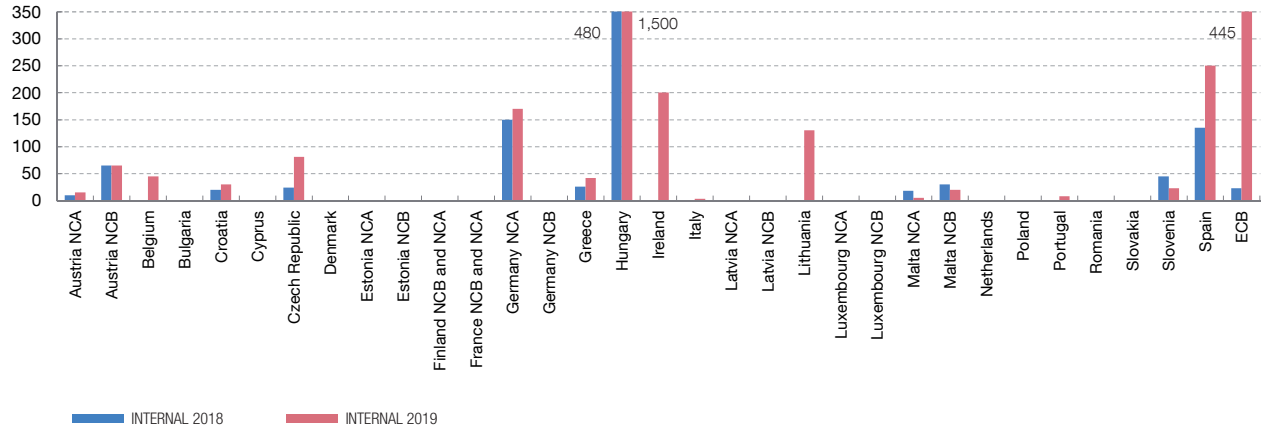
SOURCES: ESCB/SSM institutions (Annex 2).

The most common practices to raise awareness are internal training, publication of relevant content and videos on the intranet and provision of guidance to business units on queries. Some DPOs also mention raising awareness though involvement in different business projects and internal committees, where they provide recommendations and interact with other employees on specific business cases.

11.7 Queries handled by DPOs

In the case of internal queries, only some DPOs provide figures. Given that the GDPR came into force in mid-2018, FY2019 is more representative to detect trends in the volume of queries processed by the DPOs. Among the figures reported by the DPOs, as depicted in Chart 35, it is noteworthy that most of the NCBs/NCAs did not process more than 200 queries in either year, save for Hungary (1,500 queries in 2019), the ECB (445 in 2019), Spain (250 in 2019) and Ireland (200 in 2019).

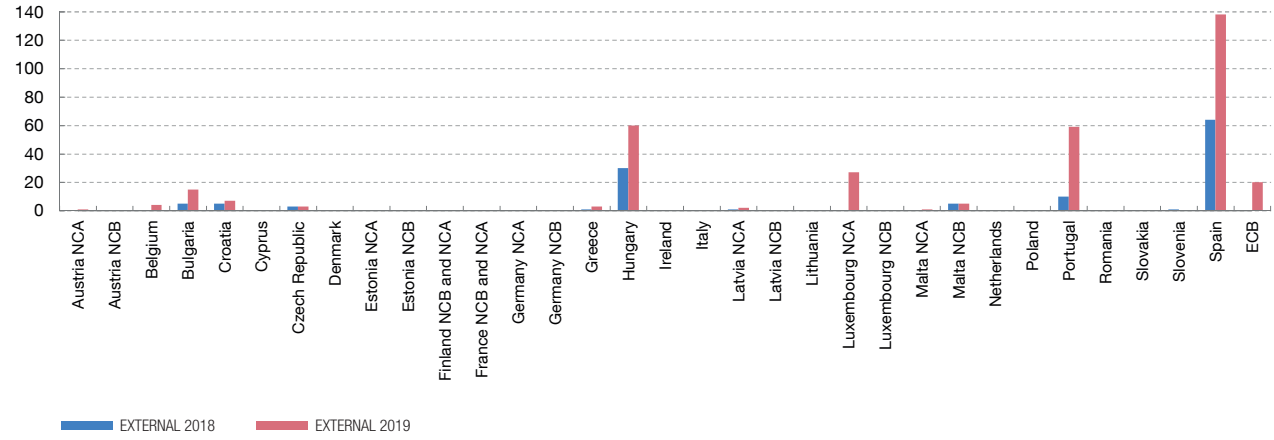
Chart 35
INTERNAL QUERIES 2018-2019



SOURCES: ESCB/SSM institutions (Annex 2).

Concerning external queries, as depicted in Chart 36, only three NCBs/NCAs have processed more than 50 queries: Spain (138 in 2019), Hungary (60 in 2019) and Portugal (59 in 2019):

Chart 36
EXTERNAL QUERIES 2018-2019



SOURCES: ESCB/SSM institutions (Annex 2).

Overall, NCBs/NCAs do not report a major increase in the number of queries between the two years adjusted for the date of the GDPR coming into force.

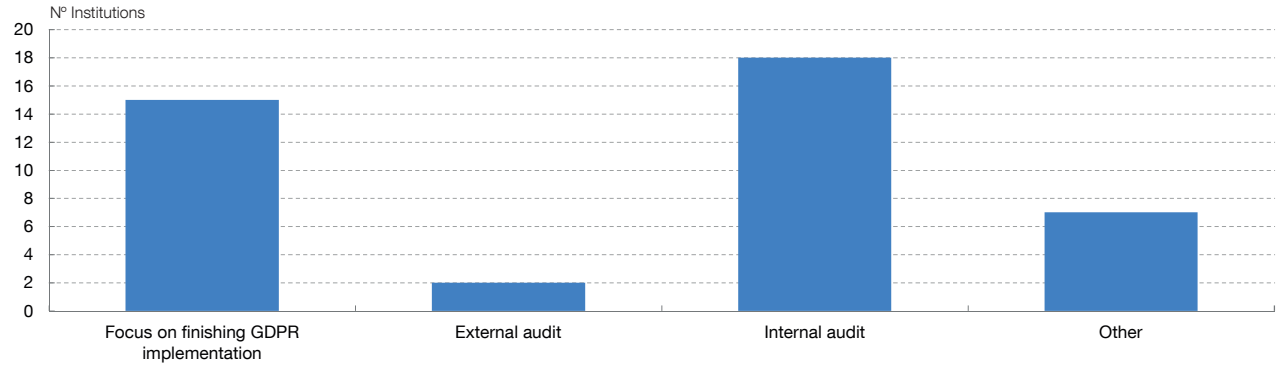
11.8 Monitoring GDPR compliance

As depicted in Chart 37, most of the DPOs report monitoring through internal audits, with the Czech DPO specifying that he takes part in the internal audits of the Audit Department and can also propose audit topics. The Cypriot NCB/NCA and the Maltese NCA have undertaken external audits

to check GDPR compliance. Among the respondents, 15 NCBs/NCAs report that their current focus is on finishing the implementation of the GDPR before shifting their focus to monitoring compliance.

The "Other" monitoring practices comprise interviews and questionnaires on recorded processing activities, ad hoc or regular verifications with business units and first-line contacts, private "investigations" triggered by queries or soft law (e.g. EDPB guidelines, case law, etc.) and attending meetings of IT committees.

Chart 37
MONITORING COMPLIANCE



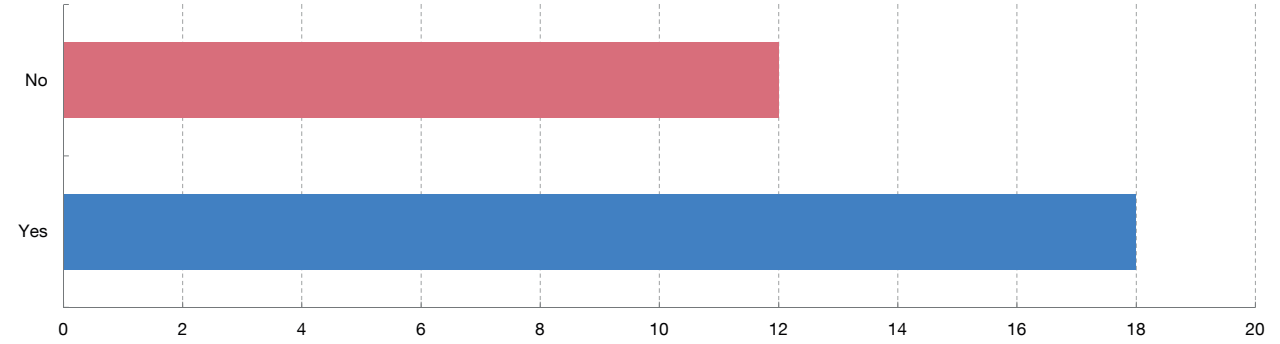
SOURCES: ESCB/SSM institutions (Annex 2).

The French DPO noted that the French NCB and NCA opted for a structure in which the DPO is not formally in charge of monitoring GDPR compliance. Even though the DPO is very actively involved, the Director of Risk Prevention acts as project manager and the Controller General as sponsor.

11.9 Personal data protection training

Almost all institutions provide some kind of training on data protection regulations, with 18 NCBs/NCAs providing mandatory training/information sessions (see Chart 38):

Chart 38
ARE TRAINING SESSIONS MANDATORY IN YOUR NCB/NCA?



SOURCES: ESCB/SSM institutions (Annex 2).

Additionally, three DPOs report providing online training to all employees (the Czech, Irish and Italian DPOs) and some DPOs report specific training sessions:

— the Cypriot DPO provides training to designated employees in business units that process personal data (e.g. DPIAs, notification of personal data breaches, etc.);

— the Czech DPO, apart from online training, provides training to all new employees in person to raise awareness;

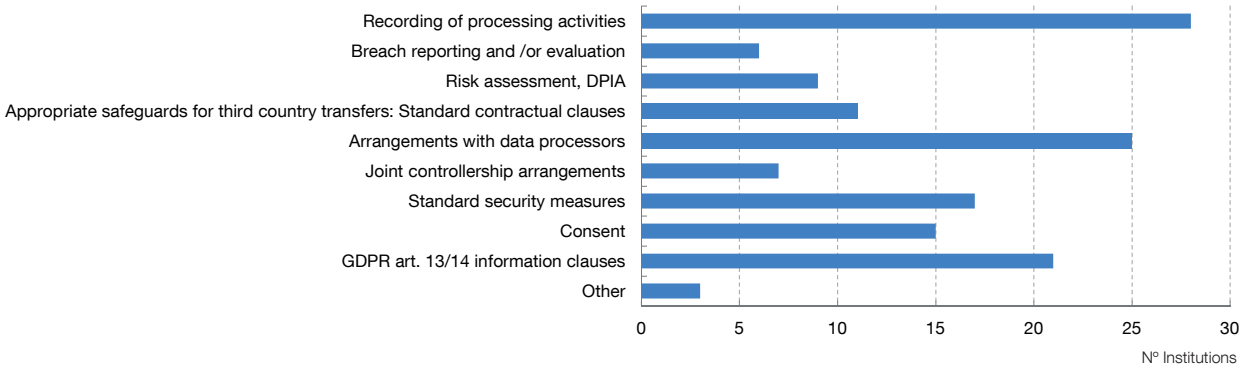
— the Irish and Spanish DPOs provide additional training sessions targeting the needs of specific areas, such as HR, regulatory supervision, employees dealing with data processor contracts, IT and market conduct.

The DPOs or DPO teams deliver 80% of the training sessions.

11.10 Personal data protection templates

All but one DPO report having at least one GDPR implementation template. The most broadly-used templates include those for recording processing activities and arrangements with data processors. Very few institutions report having templates for joint controller arrangements. This might be due to the fact that only a couple of NCBs/NCAs act as joint controllers beyond the scope of the ESCB and the SSM. Chart 39 illustrates other templates that were named:

Chart 39
AVAILABLE TEMPLATES



SOURCES: ESCB/SSM institutions (Annex 2).

The "Other" templates comprise reports to assess legitimate interests (Art. 6(1)(f) GDPR), in many cases in reply to questions on data subjects' rights, and reports on ITC incentives and preliminary studies, central banks' decrees, personal data destruction within IT systems and balancing tests.

11.11 Personal data protection networks

Nine DPOs report being members of networks/working groups aside from the ESCB/SSM:

- the Belgian DPO takes part in the Interfederal Statistical Institute (IIS) workgroup of DPOs;[25]
- the Cypriot DPO is a member of the Cyprus Privacy and Information Protection Association;
- the Danish DPO belongs to the EU GDPR Network Denmark;[26]
- the French DPO is a member of the French Association of Data Protection Officers (AFCDP);
- the German NCB DPO is a member of the German Association for Data Protection and Data Security (GDD) and attends regular meetings with DPOs of other federal public institutions and supervisory authorities;
- the Irish DPO belongs to the National Government Department DPO network;
- the Lithuanian DPO is a member of the Lithuanian DPO association;
- the Spanish DPO belongs to a DPO network of Spanish public institutions participated by the Spanish DPA and a DPO network organised by the Spanish Association for the Advancement of Information Security (ISMS Forum);[27]
- the ECB DPO belongs to the DPO Network of EU Institutions.

25 Collaboration between the different services of the federal state of Belgium and the federated entities in the production of public statistics.

26 https://www.eugdpr.institute/gdpr-network/.

27 https://www.ismsforum.es/index.php.

12 Transfers to third countries (Arts. 44 – 50 GDPR)

Given that the GDPR is binding within the EEA, personal data transferred to third countries could be at risk of abuse or misuse. To prevent that, the GDPR restricts transfers of personal data outside the EEA by putting in place requirements to ensure an equivalent level of protection to that granted by the GDPR. There are many ways in which such equivalence can be ensured, including an adequacy decision or proper administrative arrangements. The GDPR also introduces in Art. 49 a list of specific derogations that the transfer of personal data to third countries can be based on, where necessary.

This part of the report focuses on the list of the processing activities where personal data transfers to a third country take place, delving deeper to ascertain the grounds on which NCBs/NCAs base transfers where no adequacy decision has been adopted. Additionally, the NCBs/NCAs were asked to report on their interpretation of EC standard contractual clauses and the public interest derogation, to assess whether the approach adopted is consistent.

12.1 Processing activities involving transfers to a third country

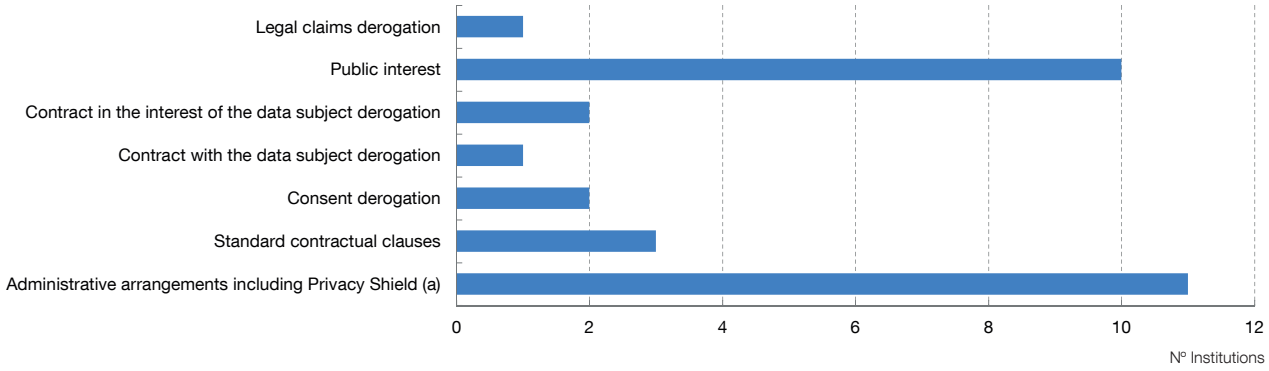
Most of the DPOs named their processing activities involving transfers to a third country, with only six NCBs/NCAs reporting that they do not transfer personal data to third countries or leaving the relevant section blank. The following processing activities were named by the DPOs as involving transfers to a third country in their respective institutions:

- HR (e.g. arrangements for mobility, certificates and reference letters, benefits and pensions to employees and families);
- international cooperation (e.g. business contacts, Christmas cards, international meetings and events such as ESMA, EBA, EIOPA);
- cooperation arrangements for supervision purposes (including F&P assessments and SSM common procedures);
- procurement (e.g. administration of receivables, contacts with foreign service providers);
- IT (equipment, user administration, cloud solutions, web portal management, newsletters);
- AML/CTF supervision;
- processing foreign payment transactions, depository services and banking operations (including government payments);
- market transparency supervision and consumer protection;
- household finance and consumption surveys.

12.2 Safeguards and derogations in the absence of adequacy decisions

In the absence of adequacy decisions, most NCBs/NCAs base transfers to a third country on the safeguards and/or derogations depicted in Chart 40.

Chart 40
IN THE ABSENCE OF ADEQUACY DECISIONS, MOST BROADLY-USED SAFEGUARDS AND DEROGATIONS

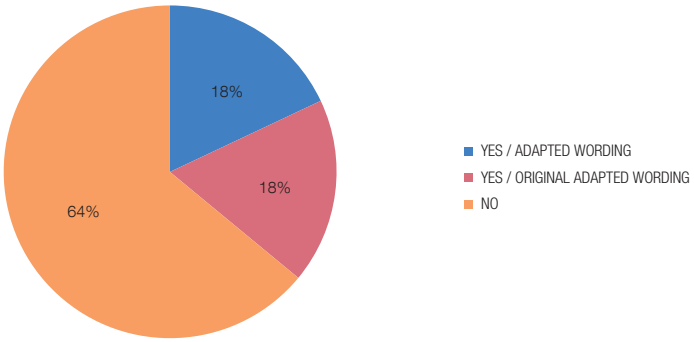


SOURCES: ESCB/SSM institutions (Annex 2).

a Privacy Shield was mentioned as an option by the ESCB/SSM participants prior to CJEU judgment C-311/18 (Schrems II).

Additionally, ten NCBs/NCAs report using EC model clauses. However, only half of the NCBs/NCAs have adapted the model clauses to the GDPR (see Chart 41).

Chart 41
DOES YOUR NCB/NCA USE EC MODEL CLAUSES?



SOURCES: ESCB/SSM institutions (Annex 2).

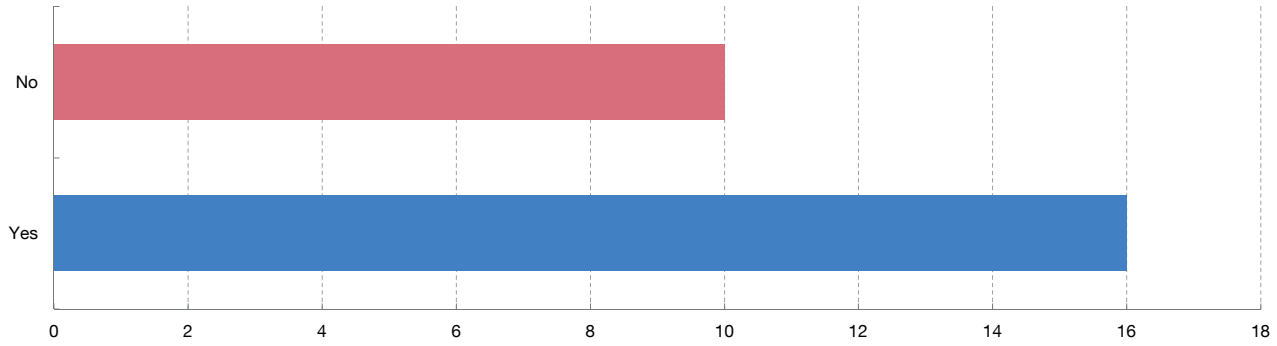
12.3 Transfers to third-country supervisors based on the public interest derogation

As depicted in Chart 42, sixteen of the institutions stated that they base transfers to third-country supervisors on the public interest derogation (Art. 49(1)(d) GDPR). It should be noted that the overall

number of answers given to this question was 26, as some institutions noted in previous questions that they do not make any international personal data transfers.

Chart 42

DOES YOUR INSTITUTION BASE TRANSFERS ON THE PUBLIC INTEREST DEROGATION?



SOURCEs: ESCB/SSM institutions (Annex 2).

13 Conclusions

The purpose of the survey that is the basis of this report was to learn more about the ways in which NCBs/NCAs meet the GDPR requirements. As this study shows, even though the business models of the ESCB central banks and SSM competent authorities are very similar, there are many different methods used to comply with the GDPR.

This study aims to help gather and share best practices among NCBs/NCAs. As many institutions are currently in the implementation phase, it should also help them discover possible ways to approach compliance with the GDPR provisions. Additionally, it can be a starting point for mutual discussion on the best and sure-fire ways to uphold higher standards of personal data protection in NCBs/NCAs.

It should be noted that in all but one jurisdiction national laws further detailing the GDPR have been passed. Even though the main purpose of the GDPR is to harmonise EU data protection regulations, some differences still remain among jurisdictions due to fragmented national regulations and DPA interpretations.

It is of paramount importance that controllers have an accurate and complete record of the processing activities under their responsibility. This not only provides a deep understanding of the types of processing activities undertaken by the institution, but also forms a solid basis for efficient and effective management of data privacy issues on a day-to-day basis. The number of processing activities reported by each institution ranged from 16 to 550 pre-grouping and from 22[28] to 417 post-grouping. Given that the institutions have similar business models, a deeper insight into the types of processing activities they perform and how institutions manage their registers could bring about improved solutions and ultimately enhance data flow governance at all institutions.

Understanding the different legal bases and choosing the correct one for a particular processing activity is not as straightforward as it might seem. As the information reported by the institutions shows, even though most of their processing activities are similar, the legal bases chosen as the grounds for processing differ enormously across institutions. Discussing different possible choices of legal bases and the reasons for those choices could help develop a common shared understanding of processing activities, which in turn would also help inform similar privacy notices.

The NCBs/NCAs noted many ways in which they ensure that information clauses are duly recorded on forms. Sharing their experience on the merits and flaws of each of those ways could generate better processes and, therefore, enhance transparency for data subjects.

The part of the report describing the exercise of rights requests offers a broad overview of the practical part of handling private data requests. The approaches reported by the institutions were largely similar. There were some differences noted in terms of the parties responsible for handling

28 The NCB/NCA that reported 16 processing activities pre-grouping did not state the number of processing activities post-grouping.

data requests, where not only the DPO and the business unit concerned but also both the Legal and the IT department are involved. Also in this section the institutions reported on claims that were directed against them to the national DPAs. Interestingly, one of the institutions reported that the DPA initiated ex officio proceedings to assess the lawfulness of the processing activities based on public interest and legitimate interests. Sharing valuable information on the outcome would help prevent more such cases arising in other jurisdictions.

The institutions shared the ways in which they have embedded the privacy by design and by default requirements in their implementation of GDPR requirements. Given that roughly one-third of the NCAs/NCBs do not yet undertake a GDPR-themed audit, they would benefit from knowing the outcome of the audit performed by other institutions. Additionally, the NCAs/NCBs reported the types of proper technical and organisational security measures that they apply as well as the policies they have in place to make sure privacy is considered by default. All this information could serve as reference for those institutions that do not yet have privacy by design and by default embedded in their privacy management structures.

The next part of the report looked into the relations NCBs/NBAs have with data processors. The institutions shared information on their progress in updating agreements with data processors and the ways in which they detect and document those agreements. Given that about one-third of the institutions do not yet update all the agreements, information on how other NCAs/NCBs approached this requirement would be useful for them. Additionally, information on audit clauses should be useful for updating agreements with data processors. NCBs/NCAs also shared examples of arrangements in which they themselves act as joint controllers or data processors. This list is a valuable resource for benchmarking each NCB's/NCA's own arrangements.

In terms of personal data breaches, the NCAs/NCBs shared both the number and types of breaches that occurred, and also whether there was a need to notify the DPA or the data subjects. Given that personal data breaches are part and parcel of today's information society, it is important to learn how to handle such cases from one another. The NCBs/NCAs share the formulas they use to determine whether or not a data breach need be notified, as well as the way they document it internally; this would merit a deeper insight into the efficiency and effectiveness of the breach reporting systems the NCBs/NCAs have in place.

Under the GDPR, processing activities that are likely to result in a high risk to the rights and freedoms of natural persons should be subject to a data protection impact assessment (DPIA). The number of DPIAs reported by the NCBs/NCAs varied significantly, ranging from none to 37. The analysis of risks performed for each of the processing activities also varied, as the institutions arrived at different conclusions considering the level of the risks posed by the processing activities. The insight given by the institutions regarding the tools they use for assessment and how they define large-scale processing might offer a partial explanation of the difference in the number of DPIAs. The information provided on the consultations that the NCBs/NCAs have undertaken with

their national DPAs pursuant to Art. 36 GDPR is also valuable, as understanding the reason for these consultations and their outcome may help other institutions to implement such processes smoothly.

When it comes to the part of the report concerning DPOs, there are many issues that could enrich the best practices currently in place at NCBs/NCAs. The DPOs surveyed include single person DPOs, team DPOs and single person DPOs supported by a team. Discussing the merits and drawbacks of each such structure should bring about a deeper understanding of each and prompt an informed choice in favour of one or the other. There is also a wide range of solutions as to the DPO's place in the structure of the institutions, which when discussed from a first-hand perspective can also help understand the strong and weak points of each. All of these different solutions are GDPR compliant.

The last part of the report illustrates the many and diverse processing activities that involve transfers to a third country. Given that almost all institutions have such processing activities and are in the same or similar international relations with many counterparts, sharing their experiences and contract clauses safeguarding the proper transfer of personal data would be of benefit to all.

Each NCB/NCA needs to create their own personalised way to implement the GDPR requirements. Nevertheless, learning from other NCBs/NCAs and sharing their own experience with chosen implementation methods can help improve the treatment of privacy matters across all ESCB institutions and SSM competent authorities and beyond.

Finally, we would like to thank all the participating NCBs/NCAs for their cooperation and support, without which this report would not have been possible.

Annex 1 Data Protection Schuman Questionnaire

General provisions		
1	In your country, is there a national regulation that further details GDPR provisions? (national DP regulation)	☐ Yes ☐ No
		If yes, please provide name and link below:
2	Has your DP authority issued any guidelines interpreting GPDR?	☐ Yes ☐ No
		If yes, please provide a list and links below:
Records of processing activities (Art. 30 GDPR)		
3	Have the areas involved in personal data processing appointed a contact person to deal with the DPO on personal data matters?	☐ Yes ☐ No
4	Do you record additional information to that required by Art. 30 GDPR?	☐ Yes ☐ No
		If yes, please list the additional information your Institution records:
5	How many processing activities are contained in your record prior to and post grouping? Which criteria do you use to group processing activities?	Initial number prior to grouping: _____ Resulting number post grouping: _____
		Grouping criteria: ☐ Related purposes ☐ Same area/department ☐ Similar processing mechanics ☐ Others (please specify below):
6	In what way does your Institution make sure the records of processing activities are up to date?	☐ Regular meetings with areas processing personal data ☐ Update as a result of internal queries ☐ Update as a result of audits ☐ Policies to ensure the involvement of the DPO in the design/ modification of processing activities ☐ Others (please specify below):
7	Does your Institution publish the record of processing activities?	☐ Yes, it is mandatory under national DP regulation ☐ Yes, it is not mandatory but it is published as a best practice ☐ No
		If yes, please provide below a link to the published record:

<table>
<tr><th colspan="3">Legal bases and special circumstances for data processing (Art. 6-11 GDPR)</th></tr>
<tr><td>8</td><td>Under your jurisdiction, is it possible for public institutions to base processing activities on the controller's legitimate interests (Art. 6.1(f))?</td><td>☐ Yes
☐ No</td></tr>
<tr><td rowspan="2">9</td><td rowspan="2">Is there any processing activity based on legitimate interests in your Institution?</td><td>☐ Yes
☐ No</td></tr>
<tr><td>If yes, please name below the processing activity:</td></tr>
<tr><td>10</td><td>Please provide an approximate percentage and total number of the processing activities based on:</td><td>
<table>
<tr><th>Legal basis</th><th>No.</th><th>%</th></tr>
<tr><td>Consent</td><td></td><td></td></tr>
<tr><td>Contract</td><td></td><td></td></tr>
<tr><td>Legal obligation</td><td></td><td></td></tr>
<tr><td>Vital interests</td><td></td><td></td></tr>
<tr><td>Public interest</td><td></td><td></td></tr>
<tr><td>Legitimate interests</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>11</td><td>Which is the age your national DP regulation considers processing of a child's data to be lawful without parental consent?</td><td></td></tr>
<tr><td>12</td><td>Which of your processing activities include special categories of personal data/data relating to criminal convictions? (e.g. Fit and Proper)</td><td></td></tr>
<tr><td rowspan="2">13</td><td rowspan="2">Does your national DP regulation or DP authority specify maximum retention periods for personal data?</td><td>☐ Yes
☐ No</td></tr>
<tr><td>If yes, please provide a list of the retention periods:</td></tr>
<tr><th colspan="3">Transparency (Art. 13 and 14 GDPR)</th></tr>
<tr><td>14</td><td>In what way does your Institution make sure information clauses are duly recorded on forms?</td><td>☐ Regular meetings with areas processing personal data
☐ Error detection resulting from internal queries
☐ Internal audits
☐ External audits
☐ Others (please specify below):</td></tr>
</table>

<table>
<tr><td rowspan="3">15</td><td rowspan="3">Does your national DP regulation allow the information of Art. 13-14 GDPR to be summarised as a first layer?</td><td>☐ Yes
☐ No</td></tr>
<tr><td>If yes, please tick below the mandatory content for the first layer:

☐ Controller’s identity
☐ Controller’s contact details
☐ DPO’s contact details
☐ Purposes of the processing
☐ Legal basis
☐ Recipients
☐ Transfers to third countries
☐ Retention period/criteria
☐ DP rights
☐ Right to lodge a complaint with the DP authority
☐ Existence of automated decision-making
☐ Whether the provision of the personal data is required
☐ Link to the privacy policy
☐ Link to the records of processing activities</td></tr>
<tr><td>Only when Art. 14 GDPR is applicable:

☐ Categories of personal data
☐ Source of personal data</td></tr>
<tr><td colspan="3">Exercise of rights requests (Art. 12 and 15-23 GDPR)</td></tr>
<tr><td rowspan="2">16</td><td rowspan="2">Do you have a public credit registry containing personal data?</td><td>☐ Yes
☐ No</td></tr>
<tr><td>If yes, are rights over personal data subject to any restrictions pursuant to Art 23 GDPR?

☐ Yes
☐ No</td></tr>
<tr><td>17</td><td>How many requests to exercise rights over personal data (excluding requests relating to personal data included in credit registries) has your Institution received since GDPR became applicable?</td><td>Number of requests per right excluding requests relating to credit registries:

<table>
<tr><th>Right over personal data</th><th>2018 requests</th><th>2019 requests</th></tr>
<tr><td>Access</td><td></td><td></td></tr>
<tr><td>Rectification</td><td></td><td></td></tr>
<tr><td>Erasure</td><td></td><td></td></tr>
<tr><td>Restriction of processing</td><td></td><td></td></tr>
<tr><td>Data portability</td><td></td><td></td></tr>
<tr><td>Automated individual decision making</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>18</td><td>If a request does not specify to which processing activity it relates to, does your national law allow you to request specification?</td><td>☐ Yes
☐ No</td></tr>
<tr><td>19</td><td>Which are the processing activities for which you receive the most requests? (e.g. credit registries, human resources…)</td><td></td></tr>
</table>

20	How many requests has your Institution rejected and on what grounds?	<table><tr><td></td><td>2018</td><td>2019</td></tr><tr><td>Rejected requests</td><td></td><td></td></tr></table> Brief description of the grounds:
21	Do you provide access to personal data included on documents protected by banking supervisory secrecy?	☐ Yes ☐ No Comments:
22	In what way does your Institution make sure the applicant is the data subject?	
23	Do you have processing activities where the right to object is overridden by the reasons of public interest?	☐ Yes ☐ No If yes, please briefly describe below the processing activities concerned:
24	Are requests addressed by the DPO team or are they handled by other areas?	☐ DPO assisted by areas involved in the processing activities concerned ☐ Areas involved in the processing activity concerned assisted by the DPO ☐ Legal ☐ IT ☐ Compliance ☐ Others (please specify below):
25	Have any data subjects submitted claims against the DP authority for non-compliance with GDPR?	☐ Yes ☐ No If yes, please provide below a number and a brief description of the main reasons behind the claim: (e.g. lack of understanding of Art. 23 restrictions, rejection of requests…)
26	Which channels do you provide to allow data subjects to exercise data protection rights?	☐ Online form ☐ Email mailbox ☐ Postal mailbox ☐ Others (please specify below):
27	Do data subjects mostly use the appropriate channels to exercise data protection rights? What do you do when a request is received through a different channel? Please elaborate in the comments section.	☐ Yes ☐ No Comments:
28	Please provide a brief description of how your Institution processes and records requests.	

Privacy by design and by default (Art. 25 GDPR)		
29	Have you performed any audit to make sure your organization complies with the GDPR?	☐ Yes. It was an internal audit ☐ Yes. It was an external audit ☐ No
		If yes, please include below a brief description of the scope:
30	In what way does your Institution make sure that proper technical and organizational security measures apply to ensure a proper level of security when processing personal data?	☐ Ad hoc assistance from the CISO ☐ List of standard security measures elaborated in collaboration with the CISO ☐ Application of specific measures set out in national regulations/ guidelines ☐ Others (please specify below):
31	Does your Institution have any policies to make sure privacy is considered by default? Please name these policies in the comments section.	☐ Yes ☐ No
		Comments:
Data processors and joint controllers (Art 26 and 28 GDPR)		
32	Does your Institution have any joint controllership arrangements besides the IT-Shared Services, SSM common procedures and FMIs?	☐ Yes ☐ No
		If yes, please provide a brief description:
33	Does your national law provide for a timeframe to regularise agreements with data processors executed prior to the application of GDPR?	☐ Yes ☐ No
		If yes, please provide a brief description:
34	Has your Institution checked all the agreements executed with data processors prior to the application of GDPR to make sure they comply with requirements set forth in Article 28 GDPR?	☐ Yes ☐ No
		If yes, please briefly describe the process of regularisation:
35	How does your Institution make sure that agreements with data processors are duly detected and documented in compliance with Article 28 GDPR?	☐ Specific training for employees in charge of drafting agreements with suppliers ☐ Available template clauses to include in agreements ☐ Ad hoc assistance from the DPO ☐ Available list of security requirements drafted by the CISO ☐ Mandatory compliance certificates/adhesion to codes of conduct ☐ Mandatory preliminary compliance questionnaires ☐ Mandatory representations and warranties ☐ Others (please specify below):

36	Does your Institution audit data processors? If yes, please briefly describe the scope and timing in the comments section.	☐ Yes ☐ No
		Comments:
37	Does your Institution act as a data processor?	☐ Yes ☐ No
		If yes, please briefly describe below:
	Personal data breaches (Art. 33-34)	
38	Has there been any personal data breach in your Institution since the application of GDPR?	☐ Yes ☐ No
		If yes, please provide the number and very brief description of the grounds:
39	If your Institution has experienced personal data breaches, were notification obligations triggered?	☐ Yes. Notification to the DP authority ☐ Yes. Notification to the data subjects ☐ No notification obligation was triggered
40	Do you have any formula/risk matrix to assess whether the obligation for notification is triggered?	☐ Yes ☐ No
		If yes, please provide a brief description of the assessment formula/ risk matrix:
41	Does your Institution have any policy to make sure the DPO is notified when a personal data breach is detected?	☐ Yes ☐ No
		If yes, please provide a brief description:
42	How does your Institution document personal data breaches?	

DPIA (Art.35-36 GDPR)		
43	How many DPIAs has your Institution carried out?	Number of DPIAs: _____
		List of processing activities subject to DPIAs:
44	Does your Institution have a policy to analyse risks for data subjects?	☐ Yes ☐ No
		If yes, which factors do you take into account to assess inherent risk and whether a DPIA is required? ☐ whether the processing is occasional or ongoing ☐ whether the sources of the personal data are external or internal ☐ whether the processing complies with GDPR information requirements ☐ whether the processing complies with GDPR Art. 5 principles ☐ whether data subjects are informed of their GDPR rights ☐ whether requests to exercise the GDPR rights are properly managed ☐ whether the processing includes simultaneous mass communications (e.g. newsletters) ☐ whether the processing comprises hardcopy documents ☐ whether the processing requires external storage media ☐ others: please specify below
		EDPB DPIA factors: ☐ whether the processing involves evaluation or scoring ☐ whether the processing involves automated-decision making with legal or similar significant effect ☐ whether the processing involves systematic monitoring of data subjects ☐ whether the processing involves sensitive data or data of a highly personal nature. If yes, do you take into account separately…? ☐ whether the processing involves biometric data ☐ whether the processing involves genetic data ☐ whether the data is processed on a large scale ☐ whether the data involves matching/combining datasets (e.g. big data) ☐ whether the processing involves data concerning vulnerable data subjects ☐ whether the processing involves innovative use or applying new technological or organisational solutions ☐ whether the processing prevents data subjects from exercising a right or using a service/contract ☐ others: please specify

45	Does your Institution have a specific questionnaire to perform DPIAs?	☐ Yes ☐ No
		If yes, is the questionnaire based on any specific methodology? ☐ Internal methodology ☐ ISO27001 ☐ IRM v3 ☐ Other external methodologies: please specify below
		If yes, does your Institution use the same methodology to assess the risks related to personal data and those related to the rest of the data managed by your Institution? ☐ Yes ☐ No
46	How does your Institution define large scale processing activities (see recital 91 GDPR)? If your Institution considers large scale processing solely based on a specific number of data subjects, please provide the figure.	
47	Has your Institution had to make any consultation with the DP supervisor pursuant to Article 36 GDPR?	☐ Yes ☐ No
48	Concerning DPIAs, which is the involvement of the DPO and of the IT services, respectively?	
DPO (Art. 37-39 GDPR)		
49	Is the DPO a person or a team?	☐ Person ☐ Team ☐ Person supported by a team
		If the DPO is a team or a person supported by a team… Number of people in the DPO team (excluding the DPO if he/she is a person): ____
		Is the team exclusively dedicated to support the DPO? ☐ Yes ☐ No
50	Where is the DPO situated in the structure of your Institution? Does the DPO report directly to top management?	
51	What is the background of the DPO?	☐ Legal ☐ IT ☐ Others (please specify below)

<table>
<tr><td>52</td><td>Has the DPO been issued with certification?</td><td>☐ Yes
☐ No</td></tr>
<tr><td></td><td></td><td>If yes, was the certification issued by…?

☐ National DP authority certification
☐ Private certification (please specify the name of the private certifying association/university)</td></tr>
<tr><td>53</td><td>Is the DPO exclusively dedicated to data protection matters?</td><td>☐ Yes
☐ No</td></tr>
<tr><td></td><td></td><td>If no, which other areas are handled by the DPO?

☐ Transparency
☐ Information security
☐ General legal affaires
☐ Compliance
☐ Others (please elaborate below)</td></tr>
<tr><td>54</td><td>How does your Institution ensure that the DPO is involved, properly and in a timely manner, in all issues relating to the protection of personal data?</td><td></td></tr>
<tr><td>55</td><td>Does your DPO use any external supporting IT products?</td><td>☐ Yes
☐ No</td></tr>
<tr><td></td><td></td><td>If yes, please provide name below (e.g. Onetrust):</td></tr>
<tr><td>56</td><td>What is the level of awareness about the DPO and his/her functions in your Institution and how do you raise it?</td><td>☐ high
☐ medium
☐ low</td></tr>
<tr><td></td><td></td><td>Comments:</td></tr>
<tr><td>57</td><td>Approximately, how many external and internal queries has the DPO addressed since the application of GDPR? If possible, please provide figures for 2018 and 2019.</td><td><table><tr><td>queries</td><td>2018</td><td>2019</td></tr><tr><td>Internal</td><td></td><td></td></tr><tr><td>external</td><td></td><td></td></tr></table></td></tr>
<tr><td></td><td></td><td>Comments:</td></tr>
<tr><td>58</td><td>In what way does the DPO in your Institution monitor compliance with the GDPR?</td><td>☐ Internal audits
☐ External audits
☐ As of today, the Institution is more focused on finishing the implementation of GDPR prior to monitoring compliance
☐ Others (please specify below)</td></tr>
</table>

59	Does your DPO provide data protection training programmes for employees?	☐ Yes ☐ No
		If yes, are training programmes usually mandatory? ☐ Yes ☐ No
		Are they usually provided by the DPO team or outsourced? ☐ Usually provided by the DPO team ☐ Usually outsourced
		Which is the scope (e.g. all employees, employees from certain areas)?
60	Does the DPO have templates on the following…?	☐ Recording of processing activities ☐ GDPR Art. 13/14 information clauses ☐ Consent ☐ Standard security measures ☐ Joint controllership arrangements ☐ Arrangements with data processors ☐ Appropriate safeguards for third country transfers ☐ Others (please specify)
61	Beside the ESCB/SSM Network, is your Institution a member of any data protection working groups or other international fora?	☐ Yes ☐ No
		If yes, please provide the name below:
Transfers to third countries (Art. 44-50 GDPR)		
62	Which of your Institution's processing activities involve third country transfers?	
63	In the absence of adequacy decisions, on what guarantee does your Institution usually base third country transfers?	
64	Does your Institution use EC model clauses?	☐ Yes ☐ No
		If yes, has it adapted the wording to GDPR? ☐ Yes ☐ No
65	Does your Institution base transfers to third-country supervisors on the public interest derogation (Article 49.1(d))?	☐ Yes ☐ No

Annex 2 List of authorities to which the questionnaire was distributed[29]

Table A2.1

CB/CA	Name
Austrian NCB	Oesterreichische Nationalbank
Austrian NCA	Finanzmarktaufsicht (FMA)
Belgian NCB/NCA	National Bank of Belgium
Bulgarian NCB/NCA	Българска народна банка (Bulgarian National Bank)
Croatian NCB/NCA	Hrvatska narodna banka
Cypriot NCB/NCA	Κεντρικη Τραπεζα της Κυπρου (Central Bank of Cyprus)
Czech NCB/NCA	Czech National Bank
Danish NCB/NCA	Danmarks Nationalbank
Estonian NCB	Eesti Pank
Estonian NCA	Finantsinspektsioon
Finnish NCB	Suomen Pankki
Finnish NCA	Finanssivalvonta
French NCB	Banque de France
French NCA	Autorité de contrôle prudentiel et de résolution (ACPR)
German NCA	Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin)
German NCB	Deutsche Bundesbank
Greek NCB/NCA	Τράπεζα της Ελλάδος (Bank of Greece)
Hungarian NCB/NCA	Magyar Nemzeti Bank
Irish NCB/NCA	Central Bank of Ireland
Italian NCB/NCA	Banca d'Italia
Latvian NCB	Latvijas Banka
Latvian NCA	Financial and Capital Market Commission (FCMC)
Lithuanian NCB/NCA	Lietuvos bankas
Luxembourg NCB	Banque centrale du Luxembourg
Luxembourg NCA	Commission de Surveillance du Secteur Financier (CSSF)
Maltese NCB	Central Bank of Malta
Maltese NCA	Malta Financial Services Authority
Dutch NCB/NCA	De Nederlandsche Bank N. V.
Polish NCB	Narodowy Bank Polski
Portuguese NCB/NCA	Banco de Portugal
Romanian NCB/NCA	National Bank of Romania
Slovak NCB/NCA	Národná banka Slovenska
Slovenian NCB/NCA	Banka Slovenije
Spanish NCB/NCA	Banco de España
Swedish NCB	Sveriges Riksbank
BoE	Bank of England
ECB	European Central Bank (ECB)

SOURCE: Own elaboration.

29 No response was received from Finantsinspektsioon (Estonian NCA), Commission de Surveillance du Secteur Financier (CSSF) (Luxembourg NCA), Sveriges Riksbank (Swedish NCB) and the Bank of England (UK NCB). As a result, the information concerning the UK and Sweden on Annex 3 and Annex 4 has been obtained from public sources.

Annex 3 List of national regulations detailing GDPR

Table A3.1

Country	National regulation detailing GDPR provisions
Austria	Datenschutzgesetz (Austrian Data Protection Act) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597
Belgium	Law of 30 July 2018 (Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel) https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018073046&table_name=loi
Bulgaria	Personal Data Protection Act https://www.cpdp.bg/en/index.php?p=element&aid=1194
Croatia	Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine br. 42/2018) https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
Cyprus	Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3b_en/page3b_en?opendocument
Czech Republic	Act No. 110/2019 Coll., on personal data processing https://www.uoou.cz/en/assets/File.ashx?id_org=200156&id_dokumenty=1837
Denmark	Databeskyttelsesloven https://www.retsinformation.dk/Forms/R0710.aspx?id=201319
Estonia	Personal Data Protection Act https://www.riigiteataja.ee/akt/104012019011
Finland	Data Protection Act (1050/2018) https://www.finlex.fi/fi/laki/kaannokset/2018/en20181050.pdf
France	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite «loi informatique et libertés», modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 Décret d'application n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037277401&categorieLien=id Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037800506&categorieLien=id Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038396526&fastPos=6&fastReqId=1970200897&categorieLien=cid&oldAction=rechTexte Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038528420&categorieLien=id
Germany	Bundesdatenschutzgesetz (BDSG) https://www.gesetze-im-internet.de/bdsg_2018/
Greece	Law 4624/2019, "Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 and transposition of Directive (EU) 2016/680" https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=66,121,83,229,125,127,247,242 HDPA Opinion 1/2020 on Law 4624/2019 https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=182,151,200,123,234,153,149,126
Hungary	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information https://www.naih.hu/act-cxii-of-2011---privacy-act--.html
Ireland	Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

SOURCES: ESCB/SSM institutions and public sources.

Table A3.1 (cont.)

Country	National regulation detailing GDPR provisions
Italy	Legislative decree No. 101 dated August 10th, 2018 (which amended Legislative decree No. 196 dated June 30th, 2003) https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true
Latvia	Personal Data Processing Law, in force from 05.07.2018 https://likumi.lv/ta/en/en/id/300099
Lithuania	State Data Protection Inspectorate https://vdai.lrv.lt/en/legislation
Luxembourg	Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679, portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo
Malta	Data Protection Act - Chapter 586 of the Laws of Malta https://legislation.mt/eli/cap/586/eng/pdf Other relevant data protection regulations: https://legislation.mt by running a search with the term "Data Protection Act"
Netherlands	UAVG https://wetten.overheid.nl/BWBR0040940/2018-05-25
Poland	The Act of 10 May 2018 on the Protection of Personal Data https://uodo.gov.pl/en/594
Portugal	Lei n.º 58/2019, de 8 de agosto https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized
Romania	Law no. 190/2018 https://www.dataprotection.ro/servlet/ViewDocument?id=1520
Slovakia	Act no. 18/2018 on personal data protection and amending and supplementing certain Acts https://dataprotection.gov.sk/uoou/sites/default/files/2019_10_03_act_18_2018_on_personal_data_protection_and_amending_and_supplementing_certain_acts.pdf#overlay-context=sk/content/182018#overlay-context=sk/content/182018%22
Slovenia	Slovenia has not passed yet a national law further detailing GDPR. Thus, GDPR and the Personal Data Protection Act passed prior to GDPR are applicable http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906
Spain	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales https://www.boe.es/eli/es/lo/2018/12/05/3
Sweden	Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218
United Kingdom	Data Protection Act 2018 (DPA 2018) http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
EU	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 Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552577087456&uri=CELEX:32018R1725

SOURCES: ESCB/SSM institutions and public sources.

Annex 4 List of competent DPAs and DPA guidelines

Table A4.1

Country	Competent DPA	Access to DPA guidelines
Austria	Österreichische Datenschutzbehörde	https://www.dsb.gv.at/documents/22758/116802/dsgvo_leitfaden.pdf/640015cb-eb90-4702-bf29-ca4fa2d32aca
Belgium	Commission de la protection de la vie privée	https://www.dataprotectionauthority.be/
Bulgaria	Commission for Personal Data Protection	https://www.cpdp.bg/en/index.php?p=rubric&aid=54 https://www.cpdp.bg/en/index.php?p=pages&aid=55 https://www.cpdp.bg/index.php?p=home&aid=0
Croatia	Croatian Personal Data Protection Agency	https://azop.hr/ (a) https://azop.hr/misljenja-agencije/
Cyprus	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3f_gr/page3f_gr?opendocument
Czech Republic	The Office for Personal Data Protection	https://www.uoou.cz/en/ (b)
Denmark	Datatilsynet	https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger/
Estonia	Estonian Data Protection Inspectorate	https://www.aki.ee/et/koik-juhised-loetelus
Finland	Office of the Data Protection Ombudsman	https://finlex.fi/fi/viranomaiset/tsv/ http://www.tietosuoja.fi/en/
France	Commission Nationale de l'Informatique et des Libertés – CNIL	https://www.cnil.fr/fr/recherche/lignes%20directrices%20CNIL https://www.cnil.fr/fr/recherche/r%C3%A9f%C3%A9rentiels https://www.cnil.fr/fr/biometrie-sur-les-lieux-de-travail-publication-dun-reglement-type
Germany	Die Bundes-beauftragte für den Datenschutz und die Informationsfreiheit	https://www.datenschutzkonferenz-online.de/kurzpapiere.html https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/DSGVO_in_der_Bundesverwaltung.html
Greece	Hellenic Data Protection Authority	https://www.dpa.gr/portal/page?_pageid=33,43290&_dad=portal&_schema=PORTAL (c) https://www.dpa.gr/portal/page?_pageid=33,239286&_dad=portal&_schema=PORTAL (d) https://www.dpa.gr/portal/page?_pageid=33,209418&_dad=portal&_schema=PORTAL (e)
Hungary	Data Protection Commissioner of Hungary	https://www.naih.hu/ajanlasok.html
Ireland	Data Protection Commissioner	http://www.dataprotection.ie/en/dpc-guidance
Italy	Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/provvedimenti-normativa (f)
Latvia	Data State Inspectorate	https://www.dvi.gov.lv/en/legal-acts/recommendations-and-guidelines/
Lithuania	State Data Protection	https://vdai.lrv.lt/lt/naudinga-informacija/rekomendacijos-gaires-ir-kt/valstybines-duomenu-apsaugos-inspekcijos-metodine-informacija (in Lithuanian only) (g)
Luxembourg	Commission Nationale pour la Protection des Données	http://www.cnpd.lu/
Malta	Office of the Data Protection Commissioner	http://www.idpc.org.mt

SOURCES: ESCB/SSM institutions and public sources.

a Interpretations of the GDPR by the Croatian DPA in response to individual queries.
b Guidelines on DPIAs for legislative proposals and DPIAs for controllers, personal data breach notification forms and GDPR FAQs.
c Guidelines on data subjects' rights in English.
d Guidelines on DPIAs.
e GDPR compliance (in Greek only).
f Doc. web num. 9069653, 9215890, 9124510, 9124510, 9058979, 9119868, 9141941, 9068972, 9069677, 9069637, 9096716.
g Designation of DPOs in the public sectors, unfounded claims, video recording, data processing during elections, security measures, GDPR for small and medium-sized companies, DPIA forms, reporting of personal data breaches, recording of data processing activities, GDPR for the public sector, safe internet browsing, processing of biometric data by electronic means, healthcare data security, security using wifi networks, protection of personal data on Android devices, depersonalisation methods.

Table A4.1 (cont.)

Country	Competent DPA	Access to DPA guidelines
Netherlands	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
Poland	The Bureau of the Inspector General for the Protection of Personal Data – GIODO	http://www.giodo.gov.pl/
Portugal	Comissão Nacional de Protecção de Dados – CNPD	https://www.cnpd.pt/home/decisoes/regulamentos/regulamentos.htm https://www.cnpd.pt/home/decisoes/diretrizes/diretrizes.htm https://www.cnpd.pt/home/decisoes/decide_sumarios.htm (h)
Romania	The National Supervisory Authority for Personal Data Processing	https://www.dataprotection.ro/
Slovakia	Office for Personal Data Protection of the Slovak Republic	https://dataprotection.gov.sk/uoou/en/taxonomy/term/139 (in Slovak only)
Slovenia	Information Commissioner	https://www.ip-rs.si/
Spain	Agencia Española de Protección de Datos	https://www.aepd.es/es/guias-y-herramientas/guias (Spanish) (i) https://www.aepd.es/en/guias-y-herramientas/guias (English)
Sweden	Datainspektionen	http://www.datainspektionen.se/
United Kingdom	The Information Commissioner's Office	https://ico.org.uk/
EU	European Data Protection Supervisor	https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

SOURCES: ESCB/SSM institutions and public sources.

h Guidelines on DPIAs and other aspects such as sanctioning public institutions (deliberaçao 495/2019) or the implementation of certain provisions (deliberaçao 494/2019).
i Guidelines on, among others, personal data breach reporting, DPIAs, risk assessment, privacy by design, cookies. Most guidelines are available in English.

Annex 5 DPIAs reported by NCBs-NCAs

The following processing activities were listed as being subject to DPIAs by some NCBs/NCAs:

Table A5.1

Processing activity subject to DPIA
Mobile device apps (i.e. WhatsApp & Co)
Market Monitoring and Administrative Penalty Proceedings
F&P and authorisations (Cloud Based NLP for F&P Questionnaires)
Consumer credit granted by credit institutions, where the personal identification number of the individual is processed
Surveillance and access control (CCTV, biometric data, Video analytics tool-Briefcam)
Use of biometric data
Prices and transactions on the real estate market based on data from real estate purchase agreements
IT monitoring
IT log files for operating systems monitoring
Social media web monitoring
IT field
IT management and support and
E-signature
Credit Claims assigned as collateral for Additional Credit Claims (ACCs)
HR: processing of employees' data, recruitment, analytics, social benefits
Processing relating to severely disabled data subjects
Perception of rights of the persons affected
Health management and medical schemes
Social work and psychosocial support
Disciplinary proceedings
Ethical Code
Household finance and consumption survey
Monitoring of incoming and outgoing payment orders
Extraction of data concerning payments processed via TARGET2 and transfer to recipients
Conduct of statistical analysis and research using data relevant to loans received by physical persons and enterprises
Monitoring of transactions for AML purposes
Processing queries submitted by legal authorities, e. g. police
Evaluation of supervised institutions' liquidity risk via a list of major depositors
Evaluation of supervised institutions' credit risk
Operation of central bank's historical archive
Deposit Guarantee Scheme
Mutilated notes/collector coins
Protected disclosures
Payment System
Whistleblowing channels
Digital LBCOIN e-shop
Procurement
Prudential supervision and inspections

SOURCE: ESCB/SSM Institutions.