FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

GDPR IN PRACTICE

EXPERIENCES OF DATA PROTECTION AUTHORITIES

REPORT



Contents

About this publication 4

Key findings and FRA opinions 5

Inadequate resources risk undermining the implementation of data protection authorities' mandate and their independence 7

FRA opinion 1 8

Supervision is key, but would be more effective if supported by additional tools 9

FRA opinion 2 10

Large numbers of complaints are a major challenge and should be addressed by data protection authorities as a priority 10

FRA opinion 3 10

Awareness among the general public of the existence of data protection laws does not necessarily mean that they actually understand these laws 11

FRA opinion 4 11

Providing scientific researchers with advice is a challenge for some data protection authorities 11

FRA opinion 5 12

Advising and supervising public bodies acting as data controllers remains a challenge due to mistrust and misunderstanding of data protection authorities' competencies 12

FRA opinion 6 13

The general data protection regulation is perceived as insufficient when it comes to concretely addressing the challenges posed by new technologies 13

FRA opinion 7 14

Strengthening cooperation between data protection authorities may require strengthening the European Data Protection Board 14

FRA opinion 8 15

Introduction 16

Why this report? 16

What does this report cover? 18

Scope and methodology 20

1. Data protection authorities' complete independence as a fundamental guarantee 22

1.1. Adequate resources – A safeguard for independence and effectiveness 23

1.1.1. Adequacy of funding 28

1.1.2. Adequacy of staffing 29

1.1.3. Consequences of a lack of resources 34

1.2. Freedom from external influence 40

1.2.1. Financial control must not compromise independence 41

1.2.2. Government, parliament and other public body control 42

1.2.3. Appointment of data protection authorities' leadership: ensuring independence and transparency 45

2. Data protection authorities as supervisory authorities **46**
2.1. Investigatory techniques 47
2.1.1. Lack of diversity of investigatory techniques 49
2.1.2. Extending the scope of investigations 50
2.1.3. Enhanced involvement of data controllers 51
2.2. Handling complaints 55
2.2.1. Large number of complaints 55
2.2.2. Complaints against public administrations 57
2.2.3. Joint operations involving several data protection authorities 58
2.3. Ex officio investigations 63

3. Data protection authorities as advisory authorities **65**
3.1. Advising the general public 67
3.2. Advising data controllers 69
3.3. Focus – advising researchers is challenging 72
3.4. Advising on legislative initiatives 77
3.5. Data protection officers: privileged partners for data protection authorities 83
3.6. Lack of expertise to for responding to challenges related to new technologies 84

4. Data protection authorities as cooperating authorities **91**
4.1. The European Data Protection Board's added value 92
4.2. Concerns about the European Data Protection Board 94
4.3. Looking ahead: the European Data Protection Board's development 96

Annex: Methodology **98**

Abbreviations **101**

Endnotes **102**

About this publication

© European Union Agency for Fundamental Rights, 2024

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Union Agency for Fundamental Rights copyright, permission must be sought directly from the copyright holders.

Neither the European Union Agency for Fundamental Rights nor any person acting on behalf of the Agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2024

HTML

- ISBN 978-92-9489-398-7
- doi:10.2811/62250
- TK-05-24-233-EN-Q

PDF

- ISBN 978-92-9489-397-0
- doi:10.2811/768473
- TK-05-24-233-EN-N

Photo credits (cover):

- Cover: © Miha Creative/Adobe Stock

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria

T +43 158030-0 – F +43 158030-699

- Website
- Facebook
- X
- LinkedIn

Key findings and FRA opinions

In 2024, the general data protection regulation (GDPR) is in its sixth year of implementation. This regulation, adopted in 2016 as a key part of the EU's data protection reform, amended the legal framework that had been in place since the 1995 data protection directive entered into force. It has enhanced data subjects' rights, redefined the scope and application of the fundamental right of data protection and harmonised further national legal frameworks across the European Union. It has strengthened the mandate, tasks and powers of supervisory authorities. Supervisory authorities are referred to in this report as 'data protection authorities' (DPAs), as key enforcers of the fundamental right of protection of personal data.

Article 97 of the GDPR provides for regular evaluation reports by the European Commission. The first evaluation report was published in June 2020 and will be superseded by evaluation reports every 4 years. The first report noted, among other things, a significant increase in the amount of work for DPAs, with the number of complaints, notifications of data breaches, investigations and cross-border cases increasing during the reporting period. Discrepancies in terms of DPAs' resources (human, technical and financial), affecting DPAs' ability to exercise their role, across Member States were also highlighted. The European Union Agency for Fundamental Rights (FRA) provided specific insights to the European Commission, focusing on the experiences of civil society organisations with applying the GDPR.

The Commission is due to publish its second evaluation report in 2024. The evaluation is taking place in a context where the processing of data is at the core of several EU legal initiatives. The additional requirements stemming from these initiatives and recently adopted legislation have increased or will increase the roles and responsibilities of DPAs. In April 2021, the European Commission presented an artificial intelligence (AI) package, including a proposal for regulating AI. In November 2022, the Digital Services Act and the Digital Markets Act entered into force, which aim to, among other things, reinforce the fundamental rights of users of digital services. In November 2023, the EU Data Act, which provides rules on access to and use of data, for example by users of smart devices, was adopted. Similarly, the Data Governance Act, which entered into force in June 2023, strengthened mechanisms for increasing data availability and overcoming technical obstacles to the reuse of data. In addition, duties contained in the EU's new pact on migration and asylum will add to DPAs' responsibilities.

Ahead of the second evaluation, the European Commission requested that FRA collect data on the experiences, challenges and practices identified by DPAs in implementing the GDPR.

In response to this request, between June 2022 and June 2023, FRA undertook 70 qualitative interviews with DPA representatives from all 27 EU Member States. Three staff members were interviewed separately at each DPA, with the exception of five DPAs, where fewer staff members were interviewed. The three staff members were the head of the DPA, an official in charge of international cooperation and an official in charge of processing complaints, investigations

and/or sanctions at the DPA. Interviewees were questioned on their experiences in the following areas: DPAs' independence; the institutional capacity of DPAs; modern technological challenges; raising public awareness; the investigatory powers of DPAs; sanctioning GDPR violations; cooperation between EU DPAs and the GDPR consistency mechanism; cooperation with other national regulators; and the protection of personal data and competing fundamental rights.

This report discusses some of the challenges and promising practices identified and highlighted by DPA staff. It does not provide any comparative legal analysis, nor does it provide an in-depth analysis of DPA work based on qualitative data, such as DPAs' annual budgets, the number of complaints received or the number of investigations conducted. The aim of the report is to complement such data – available in DPA, European Data Protection Board (EDPB) and European Commission reports – with concrete and detailed examples of practices developed and difficulties faced by DPAs.

From the fieldwork data, FRA identified four key areas related to the challenges faced by DPAs when implementing the GDPR. These are covered by the report as follows. Chapter 1 focuses on independence. Here, FRA analyses what DPAs perceive as challenging in terms of maintaining their independence, looking at both the adequacy of their resources and their freedom from external influence. Chapters 2 and 3 look at the two pillars of the DPAs' mandate: their supervisory powers and advisory powers, respectively. Finally, Chapter 4 looks into the cooperation established by DPAs with other regulators at the national level and with other DPAs and the EDPB at the EU level.

All these areas are affected, directly or indirectly, by the DPAs' availability of human, financial and technical resources. While several reports at the national and EU levels have already pointed out that DPAs are lacking resources across the EU, FRA's research provides a practical understanding of the diverse and multilayered difficulties that DPAs face in the day-to-day management of fulfilling their mandate and in enforcing the right of data protection in the EU. The research also identifies solutions developed to mitigate these challenges. In addition, it gathers details on promising practices that DPAs have developed to mitigate the challenges they face in implementing the GDPR.

The findings of this report should be interpreted in the context of findings from previous FRA publications on DPAs' role, effectiveness, functioning and independence. Trends in the data can be seen when comparing the findings of the current research with FRA findings published in 2010 and 2014. In particular, this report shows that, 14 years on, gaps in DPAs' financial and human resources remain, while the number of tasks that DPAs are responsible for has increased.

The research is intended to complement the evidence gathered by the European Commission, and the studies and reports prepared by the European Parliament, the Council of the European Union and the EDPB. Therefore, to avoid any duplication with the European Commission's data collection, this report provides input focused on the role and circumstances of DPAs, drawing on their practical experiences, without conducting a comprehensive assessment of GDPR enforcement by DPAs.

Inadequate resources risk undermining the implementation of data protection authorities' mandate and their independence

With the GDPR's entry into force, DPAs have been assigned more tasks and their powers have been strengthened. Article 57 of the GDPR lists a number of tasks that DPAs must carry out, such as providing advice to different stakeholders, raising awareness, handling complaints and investigating data protection breaches on their own initiative and when requested.

This research confirms FRA's findings on the role of DPAs published in 2010 and 2014, and findings published as part of the 2020 and 2021 Fundamental Rights Reports, which emphasised that DPAs face difficulties in fulfilling the entirety of their mandate due to a lack of resources.

This research acknowledges Member States' efforts to increase DPAs' overall budgets and staffing when the GDPR entered into force. Nonetheless, an overwhelming majority of interviewees stated that DPAs' workloads also increased significantly with the introduction of the GDPR. They repeatedly highlighted the mounting workloads that DPAs need to manage with limited staff and inadequate funding.

Concerns expressed by interviewees relate mainly to the extremely large and growing number of individual complaints being submitted, including minor complaints, which DPAs are obliged to handle within a reasonable time under Article 57(1)(f) of the GDPR. This report shows that, because DPAs find themselves underfunded and understaffed, many are obliged to prioritise complaints handling over other regulatory tasks that the GDPR has entrusted to them – such as promoting awareness among public administration bodies and the private sector of their obligations under the GDPR, raising people's awareness on the right of data protection and providing high-quality advice to public institutions on legislative proposals. Some interviewees pointed out that, due to a lack of resources, their DPA was not able to undertake on its own initiative investigations of data processing operations that could pose risks for data subjects. This limitation would appear to hinder DPAs' ability to provide independent oversight, including oversight of public institutions and other bodies. Moreover, insufficient resources have been reported to undermine DPAs' ability to contribute effectively to the EDPB's increasing volume of activities and to take part in external cooperation mechanisms established under Chapter VII of the GDPR.

In addition, several respondents emphasised that new EU legislation, adopted after the GDPR entered into force, has tasked DPAs with additional duties and responsibilities, extending their workload further, even though the level of resources remains the same. Some interviewees mentioned that EU law requires DPAs to supervise the implementation of new, large-scale EU information technology (IT) systems in the area of migration and border control. These include the Entry/Exit System, which will process the biometric data of hundreds of millions of people at borders coming to the EU for short-term visits as of the end of 2024. Some respondents indicated that new supervisory roles may also arise in the context of the development of AI-driven technologies, with the pending adoption of the Artificial Intelligence Act.

To effectively carry out their duties in evolving and complex technical areas, DPAs need qualified legal and IT professionals with data protection knowledge. However, several interviewees indicated that recruiting professionals with the appropriate legal and technical expertise is a challenge, especially given that DPAs have to compete with the private sector. Some respondents also emphasised that, in their Member State, the recruitment process is conducted through public service competitions, which tend to attract generalists. This has limited DPAs' autonomy to select and recruit qualified staff, meaning that training on the job has been required, negatively affecting the quality and timeliness of DPAs' work.

Hence, a large majority of interviewees emphasised that inadequate financial and human resources are a major obstacle to their DPA carrying out the full extent of the tasks required under the GDPR under Article 52 and recital 121 of the GDPR.

Article 52 of the GDPR stipulates elements of DPAs' independence that Member States should safeguard. These elements include freedom from external influence and enabling them to ensure that their human, financial and technical resources are adequate for performing their mandatory tasks. FRA research published in 2010 and 2014, as well as FRA's Fundamental Rights Report – 2021 and FRA's Bulletin 2 on the fundamental rights implications of the COVID-19 pandemic, found that external political pressure was exerted on some DPAs, particularly during the COVID-19 pandemic. This was reported less often during the current fieldwork research. A few interviewees suggested that a DPA's independence might be at risk if that DPA's budgetary proposal has to be approved by a ministry that manages a large number of databases that process personal data in various fields. Under-resourcing may also negatively affect DPAs' perceived independence, by limiting their ability to conduct investigations on their own initiative and to duly oversee governments and public authorities when acting as data controllers.

FRA opinion 1

EU Member States should secure the necessary financial, suitably qualified human and appropriate technical resources for DPAs, in light of obligations contained in Article 52 of the GDPR. As a key element of independence, DPAs should be provided with the means to adequately perform the entirety of their regulatory tasks, as defined in Article 57 of the GDPR. This especially concerns tasks where DPAs can act on their own initiative, which includes the timely provision of advice and opinions on draft legislation and conducting their own investigations of public authorities.

When allocating budgets, Member States should consider that DPAs have been entrusted with additional roles and responsibilities, many of which flow from new requirements under recently adopted EU law. As DPAs' role expands, so must their resources. An assessment of the adequacy of their resources should be made with reference to all tasks and powers of DPAs.

Member States should consider funding DPAs under a separate and independent budget line from the state budget, to make their budget visible. Where budgets are authorised at the government

level, DPAs should be free to determine the allocation and prioritisation of the resources allocated to them, in line with Article 52(6) of the GDPR.

While ensuring core funding for DPAs in the public budget, national budgetary authorities could consider stepping up funding for DPAs in relevant sectoral budgetary lines, in areas where DPAs' expertise is required, for example asylum, migration, digitalisation of services and internal security.

Member States should support independent and objective reviews of DPAs' workload to assess whether current budgets and human resources permit them to cope with their mandates and tasks.

The EDPB could consider facilitating exchanges of promising practices of national DPAs, as regards managing available resources to carry out tasks defined in the GDPR.

Member States should ensure that DPAs have the autonomy to recruit competent staff, including IT experts and specialist lawyers, and offer adequate remuneration to prevent frequent staff turnover.

Supervision is key, but would be more effective if supported by additional tools

Interviewees highlighted that supervision is their core task. Supervision includes all mandatory tasks aimed at investigating potential GDPR breaches (Article 58 of the GDPR), either on the DPA's own initiative or following a complaint. A thorough investigation is a precondition for effective supervision. For some DPAs, these investigatory and supervisory tasks should take precedence over any other function (notably in relation to advising), as investigating GDPR breaches is an obligation established in the GDPR. However, several interviewees highlighted various challenges that prevent DPAs from conducting their supervisory and investigatory tasks effectively. Several respondents explained that investigatory measures listed in the GDPR are appropriate but could be complemented with other tools to reinforce their supervisory capacity, such as concrete techniques to identify data controllers of digital services, or investigatory measures allowing for undercover investigations. These should be complemented by more in-depth and technical tools. Interviewees discussed difficulties in launching *ex officio* investigations, the importance of being able to expand the scope of an investigation based on preliminary findings and the difficulty in assessing electronic evidence collected during investigations. Another recurring challenge mentioned by interviewees relates to the difficulties some may face regarding data controllers' cooperation with the DPA during the investigation, as such cooperation is not mandatory in many Member States.

In addition, as highlighted above, human resource shortages may force DPAs to concentrate resources on complaints, not leaving enough time for *ex officio* investigations. Moreover, in most interviews, DPA staff highlighted that they are still adapting to the broadened mandate DPAs were

entrusted with by the GDPR, identifying the most efficient way to deal with the high number of complaints.

FRA opinion 2

The European Commission should assess, with the support of the EDPB, which technical and procedural tools – required to fully implement the investigatory tasks and powers prescribed under Article 57(1)(h) and Article 58(1) of the GDPR – DPAs lack. Notably, DPAs should be able, with appropriate safeguards, to collect information under a secret or concealed identity, and extend the scope of the investigation based on their findings, if further potential GDPR violations are discovered during the investigation. Any proposed amendment to the GDPR could also clarify the conditions for the admissibility of electronic evidence.

The European Commission should consider introducing reforms to enhance DPAs' ability to conduct both *ex officio* and complaints-related investigations in an adequate, effective and timely manner. Any proposed reform should reinforce the legal framework so that data controllers under investigation have an obligation to cooperate with DPAs.

Large numbers of complaints are a major challenge and should be addressed by data protection authorities as a priority

Most interviewees highlighted that the GDPR requires them to respond to every complaint that has been lodged but that they lack the time and human resources to do so. Complaints concern issues of unequal gravity and some can be petty and repetitive. DPAs have developed a wealth of practices to address complaints more effectively, through prioritisation, grouping, templates, automation or standard replies. However, FRA findings show that there is still no harmonisation and no sufficient exchange of such practices among DPAs to effectively tackle such challenges.

Furthermore, some respondents emphasised that, 5 years after the entry into force of the GDPR, DPAs' decisions in GDPR investigations and lack of timely response to complaints are increasingly challenged in courts at the EU and national levels. Defending themselves against these challenges is costly and resource intensive for DPAs.

FRA opinion 3

The EDPB could consider strengthening the exchange of national practices and experiences, specifically on improving handling large numbers of complaints. Notably, the issues of prioritisation and grouping of complaints would benefit from further guidance from the EDPB, namely guidance on which criteria and safeguards to implement in order to ensure each complaint is properly addressed.

Awareness among the general public of the existence of data protection laws does not necessarily mean that they actually understand these laws

While the majority (69 %) of people in the EU-27 have heard about the GDPR, as FRA's Fundamental Rights Survey on data protection and privacy showed in 2020, the large number of trivial or unfounded complaints received by DPAs indicates that a proper understanding of what the right to personal data entails is lacking. However, for most DPAs, despite their wish to provide advice and raise awareness among data subjects and the general public, doing so is challenging given their lack of resources.

As reported to FRA, DPAs receive very few requests for prior consultation from data controllers based on Article 36 of the GDPR, which requires data controllers to consult their DPA when the result of a data protection impact assessment (DPIA) shows that the risk to the protection of personal data is high. The limited number of prior consultation requests and of DPIAs gives rise to concerns about the actual understanding of the data protection implications of processing operations among data controllers. The low number of prior consultation requests and the low number of DPIAs suggests, according to interviewees, that, even if data controllers are aware of data protection risks, they do not fully understand what these risks entail or what they should do to identify and prevent them. Interviewees considered the lack of knowledge of data controllers on the application of data protection provisions especially striking when it comes to the development of AI systems.

FRA opinion 4

EU institutions and Member States should further support and promote awareness and understanding of data subjects' rights and data controllers' obligations among the general public. This is particularly important for tackling the currently low number of DPIAs, as identified by DPAs.

To increase the understanding of data protection implications in complex fields, notably, but not only, when it comes to the use of new technologies, the EDPB could develop further specific guidance on data processing involving new technologies or related to complex fields.

Providing scientific researchers with advice is a challenge for some data protection authorities

Most of the respondents interviewed by FRA did not recall any practical experience of providing advice to researchers in the field of scientific research, apart from during the COVID-19 pandemic.

Those interviewees who did recall giving advice identified three main challenges that DPAs face when advising researchers. First, some DPAs reported that researchers found Article 89 of the GDPR – which provides for safeguards and derogations when data are processed for research purposes (including statistical, scientific or historical purposes) – to be a complex provision. This is reinforced by the fact that researchers also reported to DPAs that the number of applicable EU and national laws confuses them when attempting to identify the correct legal basis for processing data for scientific and statistical purposes, and DPAs would welcome further field-specific guidance to enable them to properly advise researchers.

Second, some data controllers tend to be unwilling to provide access to data for research-related purposes. Lastly, several interviewees emphasised how the shift to an accountability system (from the pre-GDPR authorisation scheme) has affected their ability to advise researchers. These respondents indicated that they did not appreciate that DPAs are no longer responsible for authorising the processing of sensitive data. While general guidance has been developed by the EDPB and the European Data Protection Supervisor (EDPS), most interviewees emphasised that what they are lacking is field- and technology-specific guidance to enable them to appropriately advise researchers.

FRA opinion 5

The EDPB should consider developing further specific guidance on processing personal data for research purposes, including processing of sensitive data. More guidance, and, where relevant and feasible, more tools, should be provided to clarify the application of derogations prescribed in Article 89 of the GDPR. This guidance should address both researchers and the data controllers that researchers may contact to access specific databases. The guidance should clarify that granting or refusing access to data for research purposes is only based on Article 89 of the GDPR and that the GDPR should not be used as a justification to deny access to data for research purposes. The EDPB could also consider collecting and promoting relevant promising practices identified at the national level.

Advising and supervising public bodies acting as data controllers remains a challenge due to mistrust and misunderstanding of data protection authorities' competencies

According to Article 57(1)(c) of the GDPR, DPAs shall provide advice to national institutions and bodies on legislative measures that relate to the protection of personal data. Some interviewees reported specific difficulties concerning advising public bodies acting as data controllers. Interviewees indicated cases where, due to either fear or distrust of the DPA, public bodies did not consult with the authority before launching a data processing operation.

Similarly, several interviewees noted both mistrust and misunderstandings from the executive

when it comes to consulting with the DPA, although lawmakers agreed on the importance of providing adequate comments on draft laws to ensure effective implementation of data protection principles, which is prescribed by Article 57(1)(c) of the GDPR. In some instances, DPAs' opinions were not considered in final draft legislation, while in other instances DPAs were not consulted or were given tight deadlines. Some interviewees also highlighted how staff shortages can negatively impact DPAs' ability to advise public institutions, as DPAs lack the expert knowledge in-house needed to provide administrative bodies with exhaustive and detailed analysis on questions that are sometimes very technical or sector specific. Several interviewees reported to FRA that mistrust of data protection principles (often perceived as globally hampering the effectiveness of proposed legislation), combined with a misunderstanding of DPAs' competencies, were the main reasons for not consulting DPAs on draft legislation.

Several interviewees reported difficulties when investigating public administrations because some institutions competent in human rights or national security issues are sometimes granted a general derogation from certain obligations contained in the GDPR under national law, under Article 23 of the GDPR.

FRA opinion 6

Member States should ensure that data protection principles and requirements are mainstreamed in the work and procedures of public bodies and public authorities. They should promote the principle of data protection by default for all data processing, provide public officials with adequate guidance and regular training, and encourage a more systematic consultation of public institutions via their data protection officers (DPOs).

Member States should ensure that any restrictions allowed to public entities under Article 23 of the GDPR are granted on a restrictive basis.

Member States should guarantee that DPAs are equipped with the necessary resources to enable them to provide high-quality and specialist advice to public bodies, in line with Article 57(1)(c) of the GDPR. This includes both technological resources and human expertise, which implies granting DPAs additional resources for recruiting experts and developing in-house training.

Member States should ensure that data protection principles are taken into account when drafting legislative proposals, by consulting with DPAs and seeking their advice in advance. Member States should ensure that sufficient time is given to DPAs to provide detailed, relevant and exhaustive advice.

The general data protection regulation is perceived as insufficient when it comes to concretely addressing the challenges posed by new technologies

FRA research shows that, while the majority of interviewees believe that the requirements and tools provided in the GDPR are, in theory, adequate, most interviewees also highlighted that in practice the GDPR remains insufficient to regulate new technologies. Several interviewees said that DPAs are mostly unprepared when it comes to understanding and supervising new technologies (e.g. the implementation of AI-based systems). Some respondents emphasised the importance of dedicating more time and resources to the development of regulatory approaches for testing technologies, such as sandboxes (schemes used to test innovations in a controlled environment). Several interviewees expressed concern over the lack of clarity on the role their authority may have to play in the enforcement of data-related EU acts that have been proposed or adopted since the entry into force of the GDPR, in particular the proposed Artificial Intelligence Act.

FRA opinion 7

The EDPB should consider providing DPAs with further guidance on the application of the GDPR to new technologies. Specifically, the EDPB is invited to collect information from DPAs to identify specific technology-related areas where further explanation is needed to apply the GDPR to data processing. Member States should ensure that DPAs can further engage in research – for example using sandboxes – to identify challenges and have potential solutions ready with respect to new fields where data protection oversight is required. To avoid duplication of work, DPAs are encouraged to foster cooperation with other DPAs and share knowledge and expertise on specific data processing involving new or complex technologies.

The EU legislator should ensure that the competencies of supervisory authorities envisaged in new data-related acts (notably, the draft Artificial Intelligence Act) do not conflict with the competencies of DPAs. Should DPAs be entrusted with any additional tasks and competencies, Member States should ensure that this is accompanied by the provision of relevant additional financial, human, and technological resources.

Strengthening cooperation between data protection authorities may require strengthening the European Data Protection Board

FRA interviews confirmed that strong cooperation between DPAs will ensure swift enforcement and a harmonised interpretation of the GDPR. According to recital 123 of the GDPR, reinforced and harmonised cooperation between DPAs is a key objective of the GDPR, and the EDPB was provided with a broader mandate than its predecessor to fulfil this objective. The EDPB's broad mandate described in Article 70 of the GDPR can greatly support DPAs and reduce their workload by ensuring cooperation and consistency and by developing guidance. Interviewees were mostly positive about the EDPB, recognising the quantity of work performed by an institution that many recognise to be understaffed. However, interviewees did identify room for improvement. Some

interviewees argued that, although the work of the EDPB is welcome, it has led to significant additional work for DPAs, notably in their participation in working groups and numerous meetings. In this context, several DPAs identified a need to restructure the way in which the EDPB operates and its internal procedures.

FRA opinion 8

EU institutions should provide the EDPB with sufficient human and financial resources to allow it to fully fulfil its mandate and, as appropriate, support the work of EDPB members, including, where relevant, by developing appropriate tools. In turn, the EDPB should consider reflecting on its working procedures to ensure they do not create unnecessary burdens for DPAs.

Introduction

> **Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.**
>
> *Article 51(1) of the general data protection regulation*

Why this report?

The general data protection regulation (GDPR) [1] entered into force on 25 May 2018. Its objectives are twofold: to ensure harmonisation in the protection of personal data processing across the European Union and to provide a general legal framework that is adapted to a technology-oriented society where data processing has become more extensive and more complex. To achieve these objectives, the GDPR has created additional rights for data subjects, additional responsibilities for data controllers and data processors, and additional tasks for supervisory authorities. Supervisory authorities are referred to in this report as 'data protection authorities' (DPAs). The key role of DPAs and the importance of their independence was highlighted by FRA in 2010, in a report on the role of the DPAs [2], and in 2014, in a report on access to data protection remedies in EU Member States [3].

Article 97 of the GDPR provides that 'by 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council'. In June 2020, the European Commission published its first review [4]. This 2020 report identified both positive trends and challenges associated with the implementation of the GDPR. With regard to positive trends, the Commission highlighted an increase in the level of awareness of individuals' rights to the protection of their personal data and of their private life. FRA also identified this positive trend in its 2020 Fundamental Rights Survey, as reported in Your Rights Matter: Data protection and privacy, which showed that 69 % of people in the EU-27 had heard about the GDPR.

The European Commission's 2020 report focused on the essential role of and essential activities

performed by DPAs in relation to data protection legal frameworks. The mandate and tasks of DPAs are detailed in Chapter VI of the GDPR [5]. The report emphasised that the entry into force of the GDPR resulted in a significant increase in the amount of work for DPAs. The number of complaints, notifications of data breaches, investigations and cross-border cases increased [6]. The report also highlighted discrepancies in terms of resources (human, technical and financial) across national DPAs [7].

The 2020 report highlighted that there was not a harmonised understanding and application of the GDPR among Member States, despite the use of consistency mechanisms introduced by the regulation. The report stated that 'developing a truly common European data protection culture between data protection authorities is still an on-going process' [8]. DPAs have worked with the European Data Protection Board (EDPB) on harmonising the interpretation of the regulation. The board has produced a corpus of guidelines to reinforce a common approach in the application of the GDPR principles.

To inform the Commission's 2020 report, in 2019 FRA distributed an online questionnaire among members of the agency's Fundamental Rights Platform to assess how well civil society organisations understand EU data protection requirements, their interactions with DPAs, their implementation efforts, their experiences with GDPR-based complaints, and whether they found compliance a challenge. While the findings showed a good understanding of the main principles of the GDPR, a number of challenges were identified [9].

For the second evaluation of the GDPR, due to be published in 2024, the European Commission invited FRA to conduct qualitative research, collecting the experiences, challenges and best practices identified by DPAs in implementing the GDPR. This report analyses the fieldwork data collected in response to this invitation. It aims to complement the data collection performed by the European Commission, and the reports prepared by the European Parliament and the Council of the European Union.

This report provides specific input and is not a comprehensive overview of the GDPR. It provides DPAs and national and EU institutions with a detailed overview of practical challenges staff members working within DPAs are facing when implementing the tasks assigned to them in the GDPR. The report is a collection of experiences reported to FRA during interviews with individual staff members. It does not, and does not aim to, present an exhaustive list of all challenges that DPAs may be facing. However, it provides insight into the most pressing challenges raised by staff members working within DPAs. FRA identified common trends among these, notably DPAs' insufficient resources, lack of capacity to conduct research and lack of necessary investigatory tools. FRA also found that DPAs in the EU-27 fall into roughly two groups, with more recently established DPAs and/or DPAs that are located in smaller Member States generally more affected by a lack of financial, human and technical resources. Interviewees from these DPAs highlighted repeatedly throughout the discussions the differences they have identified between their DPA and other (more established and better resourced) DPAs.

What does this report cover?

In this report, FRA explores some of the challenges that DPAs may face when implementing the GDPR. Challenges discussed in this report are a reflection of the difficulties that staff members, as well as the heads of DPAs, have identified and reported to FRA. The responses provided by 70 interviewees from DPAs in all 27 Member States were analysed to identify trends in the challenges DPAs face and in promising practices when enforcing the GDPR.

FRA identified several common challenges that DPAs face when implementing the GDPR. The majority of them relate, directly or indirectly, to insufficient and inadequate resources.

While several reports at the national and EU levels have already pointed out DPAs' lack of resources across the EU [10], FRA's findings provide a practical understanding of how the lack of resources affects DPAs on different levels and in different sectors of their work – and ultimately affects the performance of several of their tasks.

Comparing the findings of the current research with findings from FRA reports on the role of DPAs published in 2010 and 2014 (see FRA activity: strengthening DPAs' role in the EU), this report shows that gaps in DPAs' financial and human resources have not sufficiently reduced in the past 10–15 years. This is despite Article 52(4) of the GDPR requiring Member States to provide DPAs 'with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers', as a key guarantee of their independence.

FRA activity: strengthening DPAs' role in the EU

FRA has published several reports on the role of DPAs and their effectiveness, functioning and independence in EU Member States.

In 2010, FRA found that normative and practical obstacles hindered DPAs' capacity to act fully independently of governments. These obstacles included lack of financial control over some DPAs' budgets, insufficient and inadequate human, technical and financial resources to perform functions, non-transparent appointment procedures of staff members and interference in the performance of certain duties (*).

In 2014, FRA research on access to data protection remedies (**) noted that the lack of financial and human resources had a negative impact on the quality and quantity of most DPAs' work and limited their ability to control and sanction data protection violations.

In 2018, FRA published an updated version of the *Handbook on European Data Protection Law (***)*, produced in cooperation with the Council of Europe and the

European Data Protection Supervisor (EDPS). The handbook highlights novelties brought by EU data protection reform and the modernisation of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Chapter V of the handbook describes the competence, powers and tasks of DPAs.

In 2020, FRA data (collected as part of FRA's *Fundamental Rights Report – 2020* (****)) showed persistent staffing and funding shortages affecting several DPAs. This is despite the strengthened legal mandate provided by the GDPR and its requirement that Member States provide DPAs with adequate resources to carry out their mandatory tasks under Article 52(4).

In June 2020, FRA published a report on people's opinions on and experiences of data protection and technology (*****), extracted from its larger Fundamental Rights Survey. The report focused on two main aspects: how people to share data about themselves and their willingness to do so, and their awareness of the EU data protection legal framework. FRA research found that 69 % of people in the EU-27 have heard about the GDPR and 71 % of people in the EU-27 have heard about their national DPA.

Sources:

(*) FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010;

(**) FRA, Access to data protection remedies in EU Member States, 2014, Chapter 4.2;

(***) FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, 2018;

(****) FRA, Fundamental Rights Report – 2020, Publications Office of the European Union, Luxembourg, 2020;

(*****) FRA, Your Rights Matter: Data protection and privacy – Fundamental Rights Survey, Publications Office of the European Union, Luxembourg, 2020.

FRA's findings are presented in four chapters. Chapter 1 focuses on a key aspect of any authority's effectiveness: its independence. In this chapter, FRA reports what DPAs perceive as challenging in terms of maintaining their independence, looking at both the adequacy of their resources and their freedom from external influence. Chapters 2 and 3 look at the two pillars of the DPAs' mandate: their supervisory and advisory powers, respectively. Finally, Chapter 4 looks into the cooperation established by DPAs with other regulators at the national level and with other

DPAs and the EDPB at the EU level.

Scope and methodology

This section presents a summary of the research methodology. The Annex: Methodology provides a more detailed description of the methodology.

The report draws on the findings of qualitative research conducted in 2022 and 2023. It is based on face-to-face, semi-structured interviews carried out with DPA representatives from the 27 EU Member States.

FRA developed a questionnaire in consultation with the European Commission to avoid any duplication with the data collection conducted by the Commission and ensure that relevant information was collected. The questionnaire addressed the tasks of the DPAs listed in Article 57 of the GDPR. The aim of this research was not to present an exhaustive report on the work of the DPAs or the challenges they may face. The objective was to collect information on **practical experiences** to illustrate the challenges DPAs face and the promising practices DPAs have experimented with to respond to these challenges.

During the interviews, FRA asked respondents if they had any examples of good or promising practice they believe are useful in their daily activities, or help address any challenges their DPA faces when implementing the tasks outlined in the GDPR.

FRA collected many practices that differ in their scope, specificity and applicability. These practices were not analysed or tested by FRA. These practices are presented in this report to encourage their dissemination and the exchange of experiences among national DPAs.

All practices were mentioned during the interviews. FRA contacted the interviewees to verify the accuracy of the practices and, eventually, to add information and contextualise them. Where available, an official source was added to the practice.

Up to three staff members from each DPA were interviewed. To ensure a variety of views and experiences were captured, interviews were carried out with:

- the head of the DPA (e.g. president, chair);
- an official in charge of national or international cooperation work at the DPA;
- an official in charge of processing complaints, investigations and/or sanctions at the DPA.

The questionnaire covered nine areas:

- the institutional capacity of DPAs;
- modern technological challenges;
- the independence of DPAs;

- raising public awareness;
- the investigatory powers of DPAs;
- sanctioning GDPR violations;
- cooperation between EU DPAs, the GDPR consistency mechanism and collaboration with the EDPB;
- cooperation with other national regulators;
- the protection of personal data and competing fundamental rights.

Due to overlaps in the responses and the trends identified by FRA, the report does not follow the structure of the questionnaire. The challenges identified by the respondents are presented based on their relevance to DPAs' independence, their supervisory powers, their advisory tasks, and their cooperation at the national and EU levels. Furthermore, interviewees did not identify any relevant challenges under the ninth area, the protection of personal data and competing fundamental rights. This does not mean that there have no challenges related to the protection of personal data and competing fundamental rights, but that interviewees were not aware of any specific challenges. This does not necessarily mean that there have not been any challenges related to the protection of personal data and competing fundamental rights, and should not be understood as a finding in itself.

FRA did not fact-check the statements made during the interviews. The purpose of these interviews is to provide the reader with an insight into the experiences of DPA staff members in their daily work, based on the testimonies provided to FRA during confidential interviews.

All interviews were conducted under conditions of strict confidentiality. For this reason, discussions of trends in this report do not identify the interviewees or their country or authority. All quotes are anonymous. Member States are identified only in promising practices, to support their dissemination.

1. Data protection authorities' complete independence as a fundamental guarantee

> **Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.**
>
> *Article 52(1) of the GDPR*

EU law safeguards DPAs' complete independence. The latter is enshrined in the EU Charter of Fundamental Rights [11] and the Treaty on the Functioning of the European Union [12] as a fundamental guarantee for ensuring enforcement of the right to data protection. The 1995 directive on data protection stated that DPAs 'shall act with complete independence when exercising the functions entrusted to them' [13], but it did not define this concept. The GDPR seeks to strengthen this essential requirement and sets out guarantees for the independent of DPAs [14], building on the jurisprudence of the Court of Justice of the European Union (CJEU) [15]. According to Articles 52 and 53 of the GDPR, DPAs should be granted [16]:

- **freedom from external influence on their leaders**, whether direct or indirect, for example freedom from governments' or other third parties' influence;
- **the opportunity to ensure the integrity and impartiality of their leadership**,meaning that DPA members should not engage in any actions or occupations that are incompatible with their duties;
- **the financial, human and technical resources**, premises and infrastructure necessary for the effective performance of their tasks and exercising of their powers, including in the context of mutual assistance, cooperation and participation in the EDPB;
- **their own staff** chosen by and under the sole supervision of the DPA member(s);
- **financial control** that doesnot affect their independence;
- **separate annual public budgets**, which may be part of Member States' budgets;
- **transparency** in thenomination of DPA members [17].

Member States must ensure that each DPA is endowed with the above elements to enable them to work completely independently. DPAs' independence has been a central focus of FRA research over the years, as an essential aspect of the enforcement of the fundamental right of protection of

personal data [18]. In 2010, FRA found that normative and practical obstacles hindered DPAs' capacity to act fully independent of governments, before the adoption of the GDPR [19]. These obstacles included governments' financial control over DPAs' budgets, insufficient and inadequate human, technical and financial resources to perform functions, non-transparent member appointment procedures and interference in the performance of certain duties. In 2014, FRA's research looking into access to data protection remedies found that these findings were still relevant for the large majority of DPAs [20]. Most DPAs covered by the 2014 research stated that they were underfunded and understaffed [21]. Their budget did not allow for high-quality specialists to be hired and new, cutting-edge technology to be acquired for the collection and analysis of evidence. The lack of financial and human resources had a negative impact on the quality and quantity of their work and limited their ability to control and sanction data protection violations [22], ultimately affecting their independence.

> **The independence of the supervisory authority and its members, as well as of staff, from direct or indirect external influences, is fundamental in guaranteeing full objectivity when deciding on data protection matters.**
>
> *FRA, Council of Europe and EDPS (2018), Handbook on Data Protection Law, pp. 191–194.*

This chapter presents the challenges that most interviewees stated regarding the implementation of the GDPR's guarantees of independence. Section 1.1 focuses on Member States' requirement to adequately resource DPAs (Article 52(4), GDPR). It examines whether respondents consider that their DPA has sufficient financial and human capacities to perform the tasks set out in Article 57 of the GDPR effectively and fully independent from external influence. Section 1.1.1 looks into adequacy of financial resources, while Section 1.1.2 examines the adequacy of staffing. Section 1.2 discusses the external influence of governments or parliaments, or other external control reported to FRA in this research, including in the allocation of budgets.

1.1. Adequate resources – A safeguard for independence and effectiveness

> **Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.**

Article 52(4) of the GDPR

Article 52 of the GDPR sets out guarantees for the independence of DPAs. Among those guarantees, adequate financial, human and technical resources are critically important for DPAs to be able to perform their tasks effectively and fully independent of external influence. The first European Commission evaluation of the GDPR identified a positive trend in DPAs' financial and human resources, with 'an overall increase of 42 % in staff and 49 % in budget for DPAs taken together in the EEA' [23] . Nonetheless, the Commission emphasised that differences between DPAs remained, and that the resource situation was 'not satisfactory overall' [24] .

> **Data protection authorities play an essential role in ensuring that the GDPR is enforced at the national level and that the cooperation and consistency mechanisms within the Board function effectively, including, in particular, the one-stop-shop mechanism for cross-border cases. Member States are therefore called upon to provide them with adequate resources as required by the GDPR.**

Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final)

Definition: resources

For the purpose of this report, the term ‘resources’ covers financial resources and technological assets (such as information technology assets) allocated to DPAs, as well as human resources (employees working at DPAs and their expertise).

Following the Commission’s first evaluation, the European Parliament issued a resolution calling upon ‘… Member States to comply with their legal obligation under Article 52(4) of the GDPR to allocate sufficient funds to their DPAs to allow them to carry out their work in the best way possible and to ensure a European level playing field for the enforcement of the GDPR’ [25].

The EDPB has gathered data on the availability of resources of DPAs over the years, showing that they are generally inadequate [26]. In its contribution to the forthcoming European Commission evaluation of the GDPR, the EDPB showed that, while budgets and numbers of staff have generally increased in percentage terms for almost all DPAs [27], most DPAs consider that they are ‘insufficient, from a human, technical and financial perspective’ [28] to perform the tasks listed under Article 57 of the GDPR [29].

> **… the EDPB and supervisory authorities (SAs)are facing a rapidly evolving technological and legal landscape that not only requires the performance of the tasks envisaged in the GDPR, but also of new tasks at national and EU level, more cooperation among the SAs and more involvement of the EDPB. … most of the SAs and the EDPB consider that their resources are insufficient, from a human, technical and financial perspective. In this respect, very specialised technical knowledge is required, in particular with regard to new and emerging technologies, while the financial resources available to SAs and the EDPB cannot compete with those of the private sectors. Therefore, it is of the utmost importance that all SAs are provided with sufficient resources by the Member States to carry out their tasks effectively.**

The overwhelming majority of DPA representatives participating in this research confirmed the overall inadequacy of DPAs' financial, human and technical resources to perform the entirety of the tasks that the GDPR requests of the DPAs. Despite nominal increases, most respondents claimed that funding and staff were insufficient to cope with an increased workload and growing demands in multiple areas of their work. Interviewees referred to three areas that their DPA found particularly challenging to handle within its existing capacity.

First, the most frequently cited concern was the substantial increase in workload resulting from managing a significant volume of complaints and data breach notifications, encompassing minor issues, following the implementation of the GDPR. This was previously identified as an issue in FRA's 2020 and 2021 Fundamental Rights Reports [30]. Some interviewees linked this surge in workload to the GDPR's requirement that DPAs have to respond to every complaint submitted, even if trivial [31]. Respondents from a large number of DPAs variously referred to complaint backlogs and long processing times as a consequence of a lack of resources to handle them. In two cases, respondents stated that their DPA was unable to comply with the GDPR's requirement to address each and every individual complaint within its current capacity [32]. Section 2.2 will examine this aspect in more detail.

> **In my view, it is evident that we lack the necessary financial and human resources. Over the last 2 years, claims have increased by 80 %. This year only, 37 % more complaints were lodged compared to the previous year. Investigations are also getting more complex for the DPA to carry out. The total number of claims will most likely exceed 20 000, which is the highest record ever reached at the DPA.**
>
> *An EU DPA staff member*

> **Our main problem is the lack of resources, which leads to enormous backlogs. Anyone can file a complaint under the GDPR easily, which is good for the data subjects but complicated for DPAs. We cannot handle hundreds of complaints each year, in a timely and appropriate manner.**
>
> *An EU DPA staff member*

Second, according to several interviewees, the fast growth of online digital platforms and the development of increasingly complex data-processing technologies require DPAs to be well resourced and technically equipped to properly and in a timely manner monitor the risks that such digital and technological advancements might pose to the protection of personal data, as discussed further in Section 3.5. Several respondents stated that this is a highly resource-intensive area, requiring technical expertise and adequate information technology (IT) equipment, which underfunded DPAs are unable to properly ensure within their current capacity. Some DPA staff also emphasised the influence of online digital platforms on their workload. Data subjects or groups of data subjects have been increasingly turning to social media to voice data protection concerns related to public policies or emerging technologies in areas such as health, security and education. Monitoring and responding to such queries takes resources and time away from other tasks, interviewees said.

> **… the GDPR places an obligation on Member States to provide their national authorities with sufficient resources to carry out their duties. It's not only a question of numbers, staff and budget, it is about meeting our ambitions for the regulation of the digital ecosystems. Effective enforcement in the digital world means independent authorities are provided with effective means to achieve this goal. For several years now the CNIL has seen its resources increasing, we are on the right track, but it needs to be amplified given the many challenges ahead. And this is certainly true for all EU DPAs; we count on the European Commission to ensure that all Member States comply with their obligations in this regard.**

> *Marie-Laure Denis, Chair of the National Commission on Informatics and Liberty, The Future of Data Protection – Effective enforcement in the digital world, keynote speech at the European Data Protection Supervisor conference, 17 June 2022*

Third, several respondents mentioned that EU or national legislation has tasked DPAs with additional work in several areas, without increasing their budget accordingly. For example, in the area of migration and border control, EU law extended the oversight role of DPAs to new EU IT systems [33], such as the Entry/Exit System [34], which is expected to collect and process the biometric data of millions of people entering the EU for short-term visits from the second half of 2024. In the area of communication and technology, the Digital Services Act regulating online intermediary services [35], including very large online platforms and search engines with more than 45 million users per month in the EU, may create new responsibilities for DPAs in some Member States [36]. Similarly, EU legislation under negotiation at the time of the research is also expected to task DPAs with further roles. Interviewees mostly referred to the proposal for an Artificial Intelligence Act [37], which may task DPAs with submitting annual reports on the use of real-time remote biometric identification systems used in public spheres for law enforcement purposes [38]. In addition, DPAs might also be responsible for the supervision of artificial intelligence (AI) regulatory sandboxes, which will be used to test the use of AI technologies [39]. Furthermore, the new pact on migration and asylum contains several pieces of legislation, in relation to which DPAs will have to provide supervision and advice. For example, in light of Article 44 of the Eurodac regulation adopted on 14 May 2024, DPAs will need advice from people with sufficient knowledge of biometric data to be able to perform their supervisory role [40]. Under Article 10 of the screening regulation adopted on 14 May 2024, DPAs will also need to support national independent mechanisms, which Member States will have to set up to monitor compliance when screening new arrivals and when examining their asylum requests at borders [41].

The following sections describe how respondents believe that resource constraints affect DPAs' ability to perform their regulatory tasks in an effective and independent manner.

1.1.1. Adequacy of funding

In 2023, 20 DPAs considered their funding to be insufficient, according to data gathered by the EDPB [42]. Other studies and reports have also documented the inadequacy of DPAs' financial resources to be able to perform their tasks over the years [43].

A large majority of interviewees stated that, overall, DPAs' budgets were increased after the entry into force of the GDPR. Nonetheless, this increase has not enabled DPAs to expand their institutional capacity sufficiently to carry out all the tasks and exercise all the powers set out in Articles 57 and 58 of the GDPR [44]. This was mentioned repeatedly during the interviews,

including by interviewees working in DPAs that have received significant increases in budget and staff in the last few years. In two DPAs, respondents had diverging views on this issue: while legal officers stated that they were unable to initiate certain investigations on their own initiative due to lack of resources, their managers considered that resources were sufficient.

Insufficient funding was the main cause of staffing shortages (as Section 1.1.2 further explains) and lack of adequate technical equipment. However, the latter is necessary to conduct investigations and supervise innovative technologies. Some interviewees illustrated this by highlighting that, currently, they cannot step up the digitalisation of complaint forms, overhaul their databases or purchase portable forensics devices to carry out on-site investigations.

Some respondents considered national resource audits a valuable tool to assess whether DPAs are equipped with the resources they need to function according to their tasks and mandate, as the box Promising practice: audits and external evaluations assessing adequacy of resources and needs explains.



Promising practice: audits and external evaluations assessing adequacy of resources and needs

In some Member States, the government has commissioned resource audits to assess whether its DPA has the necessary resources to perform its tasks under the GDPR. In the Netherlands, the Ministry of Justice commissioned three studies, which confirmed the financial challenges that the Dutch DPA was facing. Similarly, in Lithuania, the Ministry of Justice carried out a staff audit in 2021, which revealed that the DPA would need to double its number of personnel to fulfil its mandate and perform the tasks assigned by the GDPR. In Cyprus, several studies have documented the increased work volume of the DPA. This was attributed not only to the GDPR but also to increased awareness of data protection issues among the public, who increasingly contact the DPA.

Sources: Interviews with staff of the Dutch, Lithuanian and Cypriot DPAs. Publicly available source (the Netherlands): KPMG, Research Tasks and Financial Resources at AP (Onderzoek taken en financiële middelen bij AP), 2020.

1.1.2. Adequacy of staffing

The GDPR requires that DPAs are adequately staffed [45] and that 'each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned'

(Article 52(5), GDPR) [46] .The extent to which DPAs are able to exercise and enjoy independence regarding all aspects of their staff is also critical to their ability to carry out their functions effectively and independently. In 2012, in *European Commission* v *Republic of Austria*, the European Court of Justice clarified that '… the attribution of the necessary equipment and staff to such authorities must not prevent them [DPAs] from acting "with complete independence" in exercising the functions entrusted to them within the meaning of … Directive 95/46' [47] .

Since 2010 [48] , FRA has documented inadequate staffing levels at most EU DPAs. The EDPB has also reported over the years that an overwhelming majority of DPAs do not possess the necessary human resources to carry out mandatory activities under the GDPR – with 24 DPAs stating that they were understaffed in 2022 and 23 DPAs stating the same in 2023 [49] .

Most respondents stressed the unavailability of sufficiently qualified personnel to perform DPAs' functions properly. Interviewees from DPAs in only six Member States considered that their DPA had the necessary staffing level to effectively carry out its mandatory functions.

Several challenges related to securing an adequate number of qualified staff were mentioned to FRA. Understaffing was often linked to underfunding by the state. In a couple of Member States, respondents noted with concern that other national agencies and bodies with a supervision mandate were better staffed than the DPA.

Inadequate staffing also results in gaps in technical and legal expertise. This expertise is crucial to addressing challenges stemming from the use of new technologies to perform complex data processing – such as data-intensive online platforms. In almost 10 Member States, interviewees stressed that there were too few information and communications technology (ICT) experts.

> **Specialised expertise was necessary, for example, when analysing the proposal for transferring public administration data into the cloud. Analysing this governmental ordinance required a thorough understanding of the regulated aspects from a technical perspective.**
>
> *An EU DPA staff member*

In at least eight Member States, interviewees reported that it is difficult to hire qualified professionals with adequate data protection knowledge and ICT expertise, particularly if recruitment is carried out through general public administration competitions, which several DPAs have to rely on when selecting new staff. Insufficient legal expertise affects DPAs' ability to deliver on their advisory function, to the point that, in one Member State, the DPA referred data

controllers to EDPB guidelines when providing advice on new technological developments in almost every case. Chapter 3 of this report further explores the impact of inadequate staffing levels on DPAs' advisory role, while Chapter 4 looks in more detail at DPAs' capacity to effectively contribute to EDPB activities.

> **These data protection topics are very specific and are not widely known. It is not like hiring professionals in the area of accounting or human resources; there is not a broad availability.**
>
> *An EU DPA staff member*

Recruitment and retention of qualified staff was found to be a major challenge which was repeated by multiple interviewees. Low remuneration and less advantageous working conditions were often cited as the main reasons. In some cases, DPAs are limited by national recruitment rules from offering competitive remuneration. In at least eight DPAs, interviewees stressed that ICT specialists with high salary expectations would move to the private sector after being trained at the DPA. Attracting and retaining competent staff in this field was highlighted as a key issue in Member States with an overall shortage of ICT experts. One interviewee lamented the fact that specialist staff working at the DPA were not allowed to receive higher wages, as staff working for some other public agencies did.

> **The main issue we have faced is the low pay of staff over the last 4–5 years. We experienced high personnel turnover in the complaints and investigations unit. Only two colleagues have been in the DPA for more than 6 years. In the past 2 years, we have seen a 30 % increase in staff, but some colleagues have left within a year of employment. The main reason, that they share informally, relates solely to remuneration, which is too low for the expected expertise and workload.**
>
> *An EU DPA staff member*

> **The DPA makes great effort to attract skilled workers. The DPA competes for experts with the private sector – during both recruitment and retaining processes. The DPA's experts are highly valued employees for private companies. The DPA has two IT experts, which is insufficient.**

An EU DPA staff member

> **The DPA often hires personnel without previous experience. They receive training, and they are in demand in the private sector within 3–4 years and often leave, especially lawyers.**

An EU DPA staff member

In a few Member States, it was observed that staff recruited from the public administration pool seek to move to other public institutions shortly after their recruitment. They often move to services that better match their education and professional backgrounds. In general, the extreme workload affects staff performance and mental well-being in some Member States, it was reported to FRA. Legal experts often struggle to handle the high number of complaints and carry out investigations in complex areas of law. Often, backup systems to cover absences are not in place; as a consequence, many professionals leave.

> **To address insufficient human resources, staff are obliged to optimise performance and invest more time beyond regular working hours. This, however, is not necessarily a good practice.**

An EU DPA staff member

> **Several staff members from the DPA fell sick with burnout, which peaked last year, leading to long-term absences. The colleagues, who remained in service, experienced stress-related consequences (such as weight gain).**
>
> *An EU DPA staff member*

Constant changes in personnel hinders DPAs' ability to develop a consistent approach to exercising their mandate. Staff turnover may also affect their overall autonomy, objectivity and coherence when exercising their powers. For example, several interviewees mentioned that regular participation in EDPB activities was disrupted by frequent staff changes. Others said that this issue limits their ability to supervise evolving technological developments. Finally, the regular transfer of DPA employees to other public services or the private sector may also affect DPAs' perceived independence.

> **It is hard to find a data protection specialist without any links with some stakeholders in the field and who would not be in a conflict of interest.**
>
> *An EU DPA staff member*

> **Adequacy of human resources is the major shortcoming. The recruitment system publishes the posts and recruits the staff, and a few months later, after investing in his/her training, the officer moves to another post in the civil service. The only solution is to republish the vacancy and reinvest in a new officer. The DPA's performance is not negatively impacted, but, with more permanent, experienced officers, the authority could have a greater role in the EDPB subgroups.**

An EU DPA staff member

1.1.3. Consequences of a lack of resources

Several DPAs were forced to prioritise certain tasks over others and were not able to fulfil their entire mandate as a result of resource constraints. Complaints handling is usually prioritised, according to many interviewees [50]. Interviewees said that a lack of resources meant that it was difficult to perform certain tasks, such as carrying out rights-awareness campaigns; providing advice on GDPR compliance to legislators; and providing information to data subjects about their rights and to private bodies about their obligations. Chapter 3 of the report examines this in more detail. Interviewees in several Member States also highlighted that limited time and reduced capacity adversely affected the number of *ex officio* investigations that their DPA could undertake into the proper application of the GDPR, putting at risk their oversight function, as Section 2.3 further explains.

> **There is a fundamental problem with the tasks entrusted to the DPA by the GDPR. To be able to fulfil all the responsibilities listed under Article 57 of the GDPR, considerably more personnel would be required. Therefore, mandatory tasks are prioritised while secondary tasks are handled with remaining resources. Complaints handling is a high-priority task … .**

An EU DPA staff member

> **What the DPA would really like to do is to provide unsolicited advice, but, due to capacity problems, we don't manage to do so.**
>
> *An EU DPA staff member*

A shortage of resources also jeopardises DPAs' capacity to effectively cooperate with their counterparts in cross-border cases, as discussed in Section 4.2. Interviewees from at least five DPAs said cross-border cases were too complex and resource intensive. In addition, several DPAs were precluded from actively participating in EDPB working groups and activities because of a lack of resources – either a lack of financial resources to cover the cost of travel, or a lack of qualified staff. Section 4.2 examines DPAs' involvement in the EDPB in more detail.

> **The DPA received additional staff after the GDPR, but it would need many more to properly fulfil its mandate. We must persistently remind the budget ministry about the GDPR's requirement to cooperate with other DPAs in cross-border cases or in the EDPB, for example. The EU Digital Package will involve similar cooperation. Enhancing resources is imperative when entrusting competencies to DPAs. Otherwise, they will be overwhelmed and unable to properly enforce those duties.**
>
> *An EU DPA staff member*

Promising practice: balancing in-person and virtual EDPB meetings

The COVID-19 pandemic enabled DPAs to explore the effectiveness of virtual meetings, and EDPB group meetings in particular. Online meetings helped reduce DPAs' travel and personnel costs. Interviewees, who expressed concerns about

the cost of attending face-to-face meetings, were keen to continue the practice of remote participation, while stressing the importance of in-person meetings for discussing the most critical issues and for networking.

Source: Interviews with staff of several EU DPAs.

Lack of sufficient funding means that DPAs are not sufficiently technically equipped to be able to supervise and advise on the growing developments in AI-based technologies and the internet of things, according to interviewees in two Member States. Funding is also essential to ensure DPAs' activities are able to cover a wide geographical area. DPAs were restricted to conducting investigations in the capital city in two Member States due to high travel costs.



Promising practice: improving efficiency in the use of resources

The Danish DPA has optimised its efficiency, especially in the handling of complaints and general information queries, by introducing the Lean management practices on process effectiveness working method (the Lean principles). This involves mapping out internal working processes and identifying potential inefficiencies to create more effective work processes. As a result, case processing time decreased from 2–4 years in 2015 to less than 1 year in 2022. Increased efficiency in complaints- handling enabled the DPA to step up 'preventive' activities, such as advisory work and promoting public awareness of GDPR compliance.

Source: Denmark, Danish Data Protection Authority (Datatilsynet), 'Processing times' ('Sagsbehandlingstider').



Promising practice: exploring opportunities to secure additional funding

In some Member States, DPAs are able to secure additional funding through fees, donations or the recovery of financial penalties. In addition, DPAs might have the opportunity to secure additional funding through the EU or other external sources, subject to applicable national law.

Sources: Council of Europe, Report on the Funding of Data Protection Authorities,

Strasbourg, 2021. For more information, see 'EU funding supporting the implementation of the General Data Protection Regulation (GDPR)'.

Having well-resourced DPAs is essential for the enforcement of the fundamental right of data protection, as set out in the Charter of Fundamental Rights, EU law and CJEU jurisprudence, and acknowledged in FRA's previous reports on DPAs' role in the EU [51]. Adequate financial, human and technical resources are necessary to ensure that DPAs run efficiently and effectively as independent supervisory authorities [52]. FRA has also emphasised that adequate resources are a precondition for the ability of DPAs to perform their advisory, supervisory and awareness-raising tasks and exercise their powers fully independent of any external influence [53]. Sufficient resources are also key to ensuring the right to good administration and independence, which, as a general principle of EU law, binds all EU Member States. This statement applies equally to other human rights players, such as national human rights institutions and oversight bodies of intelligence services, as described in previous FRA reports [54].

DPAs have developed a set of practices to mitigate inadequate human and financial resources, using them in the most effective way despite constraints, as described in the boxes in this section.

Promising practice: automated procedures to support human resources

To expedite certain processes and reduce workloads, some DPAs have digitised specific procedures. For example, interviewees from Spain and Portugal reported that complaints can be submitted online only by filling in a compulsory form. The complainer must use a digital ID when submitting the form. These online forms were found to be useful in avoiding multiple, time-consuming communications with the data subject about the information and evidence necessary for their complaints to be further processed. In Spain, new automated procedures have been used to help DPAs differentiate between the different levels of severity of complaints received.

In addition, in cases of less serious allegations, the DPA might consider issuing a warning to the data controller concerned instead of initiating a sanctioning procedure. This practice has helped spare resources for more complex and time-sensitive complaints.

Sources: Interviews with the staff of Portuguese, Spanish and Romanian DPAs.

Promising practice: optimising human resources for enhanced efficiency

Many DPAs reorganised their available human resources following the entry into force of the GDPR. To increase efficiency, some DPAs have found it useful to periodically review how their human resources deliver on the tasks assigned to them by the GDPR. As a result, some DPAs have streamlined certain areas of expertise across their main activities. For example, in Finland, the DPA does not allocate staff to advisory and enforcement tasks. Instead, legal experts provide guidance and advice in their respective fields of specialisation.

Source: Interviews with staff of several EU DPAs.

Promising practice: efforts to motivate DPA staff when recruited through the public administration

In Lithuania, efforts have been made to motivate civil servants working for the DPA by providing them with good working conditions and matching their skills with the area of work that interests them the most. Specific measures include providing motivational bonuses, offering training and guidance for professional development and allowing staff to participate in EDPB working groups according to their interests. In addition, staff have been given the opportunity to gain more expertise through secondments to other EU or international organisations. This has helped improve motivation and excellence among DPA employees and promote participation in external cooperation activities.

Source: Interviews with staff of the Lithuanian DPA.

Promising practice: outsourcing to external contractors

Interviewees from seven DPAs found outsourcing certain tasks to external contractors a useful practice. For example, in France, the DPA is considering outsourcing the handling of certain complaints to a properly trained external service provider. This provider would process recurring and/or simple complaints, such as requests for access to personal data. While helping to handle complaints

more quickly, this practice would enable internal resources and expertise to be directed towards more complex cases. In Malta, the DPA uses outsourcing for cases requiring intense forensics analysis. In Ireland, a framework contract with an external company has helped to fill gaps in the ICT skillset of the DPA, while the support of legal firms is sought for certain tasks (not for investigation purposes). However, some interviewees indicated that this is only a temporary measure as it cannot be sustained without adequate funding.

Source: Interviews with staff of several EU DPAs.

Promising practice: boost the capacity of DPOs in public administration

The Italian DPA has promoted several initiatives to strengthen the role of data protection officers (DPOs) in public administration. The aim was to increase the data protection capabilities of competent ministries and reduce requests for advice submitted to the DPA by public authorities (*). For instance, the Italian DPA drafted specific documentation to support the designation of DPOs and improve understanding of their role and tasks in the public sector (**). The DPA organised specific events, workshops and meetings with DPOs.

The Italian DPA also participated, with four other DPAs, in the T4DATA ('Training For Data') project, which included a series of transnational training activities for trainers (carried out in 2018) and, at the national level, numerous free training initiatives dedicated to DPOs operating in public entities. These included a series of seminars in various cities in Italy, a handbook and a large number of webinars held by the DPA examining numerous topics related to the GDPR and the national legal framework on the protection of personal data (***).

The role of DPOs is analysed in Section 3.5. of this report.

Sources:

(*) Interviews with staff of several EU DPAs.

(**) Italy, National Data Protection Authority for Data Protection (Garante per la protezione dei dati personali), Guideline on DPOs' appointment, responsibility and tasks in the public administration [document 9589104], 2021.

(***) Italy, National Data Protection Authority for Data Protection (Garante per la protezione dei dati personali), Training For Data (T4DATA) project, 2018-2019.

1.2. Freedom from external influence

> **The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers […], remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.**
>
> *Article 52(2) of the GDPR*

> **Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.**
>
> *Article 52(6) of the GDPR*

Under Article 52 of the GDPR, DPAs must act **completely** independently, which involves performing tasks and exercising their powers free from any direct or indirect external influence [55]. DPAs should act objectively, impartially and free from any instructions relating to the performance of their duties from the state and private actors, as clarified by the CJEU [56]. Moreover, Member States should not exercise any form of control over DPAs through national budgetary procedures and should ensure their financial autonomy, according to the GDPR [57].

Interviewees were asked about their views on, and any experiences of, influence from governments and/or other public institutions when carrying out their tasks and exercising their powers. This also included their financial autonomy when establishing their budgetary needs. FRA also asked about staff appointment procedures and whether these ensure independence. The following sections summarise the main findings.

1.2.1. Financial control must not compromise independence

The financial control that each DPA is subject to under national law must not affect its independence, according to the GDPR [58]. National budgetary procedures can significantly affect DPAs' ability to work independently, as pointed out by FRA in previous reports [59].

In most Member States, DPAs must submit their budgetary requests to the Ministry of Justice or other ministries for approval. Although responsible ministries may not decide on the breakdown of expenditure, they might have the power to scale down the DPAs' overall budget size. A few interviewees reported an underlying risk of underfunding, preventing DPAs from carrying out their duties with full autonomy. This may be the case particularly when the DPA's budget is attached to a ministry that is also the data controller of large national databases, processing sensitive personal data, as was reported in one Member State. It could create an impression of conflict of interest, whether valid or not, in cases where DPAs are not undertaking investigations of their budgetary authorities on their own initiative, a few interviewees said.

In addition, government delays in delivering budgets may also adversely affect DPAs' ability to conduct planned activities. It took approximately 2 years for DPAs in two Member States to receive their annual budget allocations, according to respondents.

Insufficient political support for DPAs' role and functions generally, often resulting in lower budgetary allocations, was noted in certain Member States. This is due to the following.

- There are misconceptions about DPAs' independent supervision of data processing, mostly among ministries of finance. For example, the GDPR can be seen as a hindrance to innovation, and there is a misconception that data protection does not generate revenue for the state and/or is not a primary need of the general population.
- There is a lack of understanding of the role and responsibilities of DPAs. In four Member States, budgetary authorities declined to increase DPAs' budgetary resources on the basis that the DPAs' functions had remained unaltered over time, unlike those of other public agencies. In two Member States, DPAs received fewer resources than other national regulators and agencies with a narrower mandate (e.g. cybercrime, corruption).
- Public awareness of the GDPR remains low in certain Member States.

In certain Member States, intense advocacy efforts by the DPA, targeting the public and national and EU institutions, have resulted in budgetary increases.

> **Another cause of the lack of resources is the perception of privacy as a luxury and not as a primary need. Nonetheless, when reading the proposal for an AI regulation discussed at the EU level, one can identify a list of potential risks related to data protection, confirming the need to have strong – and properly staffed – oversight mechanisms, such as DPAs.**
>
> *An n EU DPA staff member*

Promising practice: autonomy of DPAs when drafting their budgetary needs

The Spanish DPA has a certain autonomy when drafting its annual budgetary proposal, which is negotiated with the competent public budgetary authority (the tax ministry). The proposal is sent to the government so that it can be integrated, independently, into the state budget.

Source: Interviews with staff of the Spanish DPA; Spanish Data Protection Agency (Agencia Española de Protección de Datos), 'Budget management' ('Gestión presupuestaria'), 2024.

1.2.2. Government, parliament and other public body control

Most respondents agreed that DPAs operate independently from their government, parliament and any other public bodies. A majority of respondents also agreed that national accountability procedures – such as annual reporting to parliament or the European Court of Auditors' audits and evaluations – do not challenge DPAs' independence. Rather, they are used to verify the sound spending of budgets and identify deficiencies in DPAs' administration.

A few DPAs were also subject to national ombudspersons' inquiries on the handling of cases. In one Member State, it was reported that, while the DPA at first found it difficult to accept the opinion of another independent authority, it took on board the authority's critical assessment of how the DPA handled complaints, and it valued the review by an independent authority to firmly ground their request for a budgetary increase.

In some Member States, FRA research revealed DPA difficulties in performing certain mandatory tasks, primarily due to forms of 'indirect' influence by either the executive or the legislative body. This was further exacerbated by inadequate human and financial resources. Issues reported to FRA included:

- legislators being resistant to taking advice on incorporating data protection safeguards into the development and use of technologies; this was raised when tracking technology was set up to fight the spread of COVID-19 (as FRA has previously reported [60] and with respect to the use of technological equipment for security purposes;
- the government refusing to implement some suggestions made by the DPA with respect to its reorganisation and the distribution of its competencies, which the DPA considered important for enabling it to fully exercise its powers;
- the head of the DPA not being entitled to publicly answer to matters related to the DPA's work in parliament, since this is the responsibility of the ministry the DPA is attached to.

Interviewees raised specific concerns about some governments' practices, saying that they adversely affected their DPA's advisory function (Chapter 3 of this report looks into DPAs' advisory role in more detail). Several interviewees observed that governments set tight deadlines when requesting legal opinions on proposed legislation and/or addressed multiple, simultaneous requests to DPAs, which hindered their ability to deliver legal advice of sufficient quality. For instance, in one Member State, the DPA had 1 or 2 days to provide an official reply to a governmental request. Understaffed DPAs found this particularly problematic, and occasionally it resulted in the refusal to comply with the request. Furthermore, around five DPAs reported situations where legislators did not consult them, or consulted them only at a very late stage, on key files. Examples reported to FRA are described below.

- Interviewees from two Member States highlighted that during the legislative process the responsible parliamentary commissions do not systematically consult the DPA on policy and legislative initiatives involving the processing of a large number of personal data. This was particularly the case during the COVID-19 pandemic. In the opinion of one respondent, in most cases the government endorses the DPA's suggestions only to prevent public outcry, as it is only when the media picks up the DPA's concerns that these are considered by the legislator. In one Member State, a respondent stressed that regular exchanges with a dedicated parliamentary commission for data protection issues have ceased to exist.
- One interviewee stated that on many occasions the DPA found out about draft legislation through the media, as it had not published on the official portal as required.
- Several employees from one DPA affirmed that the government is generally reluctant to consult the DPA and only does so when it is compulsory.
- One interviewee observed that very few public bodies seek the DPA's advice (no more than two to three consultations per year), as they fear the outcome of the DPA's assessment.

Promising practice: providing advice at an early stage of the legislative process

Some DPAs are actively involved as experts in law-making working groups of the government or parliament. To ensure that the DPAs' advisory role is not compromised, DPA representatives do not hold voting rights in some countries.

Furthermore, in some Member States DPAs make sure that their expert advice is properly noted in meeting records to avoid situations where the legislator claims to have consulted them when adopting provisions that might give rise to issues concerning the right of data protection.

Source: Interviews with staff of two EU DPAs.

> **We can determine the compliance of an action with data protection law only during an inspection. When we are asked for advice, we can only give basic instructions and guidelines – we point out some past cases, what was the solution, what they didn't pay attention to, etc. We cannot carry out a thorough assessment.**
>
> *An EU DPA staff member*

Promising practice: ensuring good administration within the DPA through a code of ethics

The Spanish DPA has adopted a social responsibility plan and a code of ethics that permits any person to submit claims related to the internal procedures followed by the DPA.

Source: Spain, Spanish Data Protection Agency (Agencia Española de Protección de Datos), 'Ethics and public integrity' ('Ética e integridad pública'), press release, 2022.

1.2.3. Appointment of data protection authorities' leadership: ensuring independence and transparency

> **Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by their parliament, their government, their head of State, or an independent body entrusted with the appointment under Member State law.**
>
> *Article 53 of the GDPR*

Ensuring that DPAs' leadership is free from any external influence or incompatible occupation is an essential guarantee of DPAs' independence, according to the GDPR [61]. In addition, DPA members should refrain from any action incompatible with their duties and perform their tasks free of any conflict of interest [62]. They should be selected through a 'transparent procedure' [63].

FRA has stressed the importance of DPAs' leadership being appointed in a transparent manner as an effective guarantee of independence from the political branches of government [64].

Interviewees did not report deficiencies in the transparency of DPA leadership nominations as a common problem across Member States. However, some interviewees highlighted ongoing challenges in ensuring the independence of DPAs' leadership. In one Member State in particular, interviewees stressed that the selection of the DPA's leadership is highly 'politicised'.

Some interviewees pointed out that conflicts of interest might occur when DPAs are institutionally attached to one ministry and are led by one director without a collegial body. In many EU Member States, the ministry of justice can potentially exercise some form of control over the DPA's activities by deciding on the overall size of its budget, as highlighted in Section 1.2.1. of this report. Interviewees from one DPA observed that this risk might be exacerbated when the ministry of justice has to approve the director's leave, promotions, business trips, etc. Theoretically, the ministry can always exercise some form of influence on the director's activities, putting DPAs' independence at risk. One interviewee suggested that the ministry could refuse a director's trip to the EDPB sessions because the DPA has issued a decision of data breach against the Ministry of Justice (imaginary example).

2. Data protection authorities as supervisory authorities

For some authorities, the GDPR did not bring major changes to their supervisory and investigatory powers. However, the sharp increase in administrative fines, coupled with sudden but extensive communication on data protection when the GDPR was adopted, multiplied the number of complaints and related inspections DPAs must conduct. This has created a number of issues, directly and indirectly, as highlighted in Chapters 1 and 3.

While difficulties have been identified in investigating cross-border cases in particular – an issue acknowledged quite early on by DPAs and discussed at several EDPB meetings [65] – FRA research identified a number of challenges that can considerably slow down or otherwise affect investigations conducted by DPAs when acting as a supervisory authority.

The EDPB met in Vienna in April 2022 to address issues related specifically to the investigation of cross-border cases. It recognised that DPAs will 'collectively identify cross-border cases of strategic importance in different Member States on a regular basis, for which cooperation will be prioritised and supported by EDPB' [66]. Several arrangements were made to improve and facilitate cross-border cooperation. As a result, a list of proposals was prepared by the EDPB and sent to the European Commission in October 2022 [67]. In July 2023, the European Commission issued a proposal for a regulation laying down additional procedural rules on the enforcement of GDPR in cross-border cases (hereafter the '2023 proposed regulation') [68].

The 2023 proposed regulation aims to address several procedural differences among Member States' national rules and practices that hinder the effective and quick handling of cross-border cases. These differences include:

- the criteria used to decide upon the admissibility of a complaint;
- the procedural rights of the parties under investigation;
- the process used to develop reasoned objections under the GDPR's dispute resolution procedure (Article 65);
- the absence of deadlines for the different stages of cooperation among DPAs and in the dispute resolution procedure.

To tackle these issues, the 2023 proposed regulation aims to:

- establish a standardised form specifying the information required for all complaints under Article 77 of the GDPR, and common rules for the rejection of complaints;
- provide parties under investigation with the right to be heard at key stages of the procedure, with clarification on the content of the administrative file and the parties' right of access to it;
- develop a framework of cooperation to ensure facilitated and early exchanges between DPAs during cross-border cases;

- set deadlines for the different stages of the dispute resolution procedure.

In September 2023, the EDPB and the European Data Protection Supervisor (EDPS) issued a Joint Opinion on the 2023 proposed regulation [69]. Both institutions welcomed the proposal, noting that while the proposal will indeed support DPAs in the effective handling of cross-border cases, it will have an impact on DPAs' resources, and, therefore, these should be adequately increased to appropriately deal with the proposal's requirements. At the time of drafting this report, the proposal is subject to the ordinary legislative procedure within the European Parliament and the Council of the EU is in the process of examining it in its first reading [70].

Most DPAs were interviewed by FRA before the publication of the 2023 proposed regulation. Several of them did highlight that procedural differences make DPA cooperation difficult to implement, for example when deciding to carry out joint operations. Nonetheless, most respondents decided not to refer in detail to these procedural differences, as these are already being addressed by the European Commission's proposed regulation. In several cases, DPAs emphasised the positive role of the EDPB in accelerating the process of addressing this important challenge.

However, FRA research identified several other challenges that prevent DPAs from conducting supervisory and investigatory tasks effectively, and this chapter deals with these challenges. Respondents highlighted that while investigatory measures listed in the GDPR appear to be adequate, there is still room for improvement (Section 2.1), and that most DPAs are still looking for an efficient way to deal with the high number of complaints (Section 2.2). Finally, they reported that *ex officio* investigations are not being launched, despite the willingness of DPAs, due to staff shortages (Section 2.3).

2.1. Investigatory techniques

> **Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: … handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.**
>
> *Article 57(1)(f) of the GDPR*

Supervision of data controllers and data processors is central to the GDPR architecture: DPAs are obliged to handle every complaint lodged with their authority. Some DPAs emphasised that they consider their role to be **primarily** a supervisory one, and that providing advice should come second – that is, depending on the human, financial and time resources remaining once supervisory duties have been performed. The ability to conduct thorough investigations is a practical precondition to ensure supervision is conducted exhaustively and rigorously. Investigations can be conducted on the DPA's own initiative (as per Article 57(1)(h) of the GDPR) or following a complaint (as per Article 57(1)(f) of the GDPR). In all cases, DPA experts must be provided with:

- full access to all necessary information (notably, as per Article 30(4) of the GDPR, data controllers and data processors must make records of processing activities available to DPAs upon request);
- the full cooperation of the investigated party in terms of all necessary explanation on the data processing under investigation – as per Article 31 of the GDPR.

More specifically, investigative powers listed in Article 58 of the GDPR include the power to:

- order the controller and the processor to provide any information the DPA requires;
- carry out investigations in the form of data protection audits;
- carry out a review of certifications issued pursuant to Article 42(7);
- notify the controller or the processor of an alleged infringement of the GDPR;
- obtain from the controller and the processor access to all personal data and all information necessary for the DPA to complete its tasks;
- obtain access to any premises of the controller and the processor, including access to any data processing equipment and means.

Given that supervision is a major part of the DPA mandate, several interviewees emphasised how most of their resources are used to handle complaints, to the detriment of other tasks, as discussed in Section 1.1 of this report. Here again, several respondents stressed that the lack of resources was having a negative impact not only on the overall work DPAs can perform, but also on the ultimate objective of ensuring safe processing for personal data upstream.

> **"It would be effective to deal with preventative work; in that way, awareness would be higher and then there should be fewer complaints coming in. We are dealing with trees, instead of the forest.**

An EU DPA staff member

Several interviewees highlighted the importance of sanctions in the new supervisory architecture implemented under the GDPR. They feel that the sharp increase in the number of sanctions has led private companies to 'take data protection seriously', despite some respondents stating that litigation should always be considered as a last resort, even in cases where a complaint was submitted to them.

> **The increased level of sanctions is a big change from the 1995 directive to the regulation. This has escalated to the degree to which data protection is taken seriously. Before, the DPA usually had conversations with lower ranking IT staff members, whereas now the DPA meets with the directors of the companies and lawyers.**
>
> *An EU DPA staff member*

When questioned on their experiences and challenges related to the supervisory aspect of their mandate, a large majority of interviewees agreed that the GDPR, on a general basis, provides adequate tools. However, several of them highlighted some critical issues that undermine their overall ability to exercise their investigative powers. Investigating potential data protection breaches remains a complex exercise, and some respondents highlighted that some powers that would help DPAs to conduct their investigations are still missing.

2.1.1. Lack of diversity of investigatory techniques

DPAs' investigative powers are described in Article 58 of the GDPR. When asked about their experiences of using these measures, most interviewees agreed that the compliance model and investigatory tools are adequate and sufficient. However, not all DPAs enjoy access to the techniques necessary for the practical implementation of these powers.

Conducting supervision is particularly challenging without adequate resources. This includes human resources (the capacity of DPAs to recruit IT experts, for example), financial resources (the capacity of DPAs to schedule more on-site investigations, for example) and technical resources (the capacity of DPAs to invest in specific software to support their investigations

involving hardware and electronic devices). Some interviewees emphasised that, with a reinforced team, their DPA would be able to diversify and, ultimately, strengthen their investigatory methods.

In addition, several interviewees pointed out that, based on their experience, Article 58 lacks **concrete** investigative techniques that would be useful in data protection-related contexts. For two interviewees, the main challenge lies at the very beginning of the investigation: the identification of the data controller, notably when it comes to online platforms, applications or social networks. In their view, there are no techniques that would support them in doing this in an effective and timely manner.

Some interviewees regretted that neither the GDPR nor the national legislator has provided their DPA with additional concrete investigatory tools, such as the ability to search under a false name, consult computer sites under a client's name, or make purchases under a concealed identity. In addition, several respondents flagged the question of the admissibility of evidence in the digital era as an issue where DPAs lack guidance. DPAs are left alone to 'decide how far they should go to prove a violation, how much information is enough to prove systematic problems'.

> **Actions and functions set by the GDPR are too general. Those are interpreted in the national regulation. And this is where problems start to arise. It is not about the GDPR competency or scope, but it is about the scope of the national regulation. Often problems are related to the fact that we (at the national level) do not have the right tools. It would be more beneficial if the GDPR would describe more concrete tools that could be used by the DPAs.**
>
> *An EU DPA staff member*

2.1.2. Extending the scope of investigations

Several interviewees highlighted that investigations – both national and cross-border – can be hindered by a too-narrow scope. One explained that their national law does not permit them to extend the scope of the procedure during the investigation.

This issue was raised in the context of handling cross-border cases in particular, with DPAs involved in cases having different rules on extending the scope of the investigation. Despite the mechanisms developed in the GDPR to simplify and harmonise the handling of cross-border cases, difficulties concerning the scope of investigations that have prevented several cases from

being resolved in a smooth and timely manner remain. This issue was acknowledged quite early on by DPAs and has been discussed in several EDPB meetings [71] . It is one of the key proposals of the European Commission's 2023 proposed regulation [72] .

2.1.3. Enhanced involvement of data controllers

Several interviewees consider it important to involve data controllers during investigations, including by developing informal contacts with data controllers. Conditions for collaborating with third parties are essential and, therefore, should be better addressed in the GDPR, according to some interviewees.

> **We are sometimes trying to ease some of these bureaucratic hurdles by having direct exchanges with the controller and with the individual. … There is a large number of cases where, with just one phone call from us, the matter is sorted out. It is not formalistic, but it is effective.**
>
> *An EU DPA staff member*

Most interviewees cited data controllers' lack of cooperation as their main challenge. For some interviewees, the fact that the DPA cannot perform checks without warning data controllers about its visit is counterproductive, as they may delete or hide relevant information.

> **What the GDPR says in Article 58 is good; the DPA's procedure is also good – the problem that the DPA is facing in the field is the lack of interest from the data controller.**
>
> *An EU DPA staff member*

Several interviewees highlighted that the GDPR does not provide any leverage in cases where data controllers refuse to cooperate with the DPA. DPAs are mostly affected by this when attempting

to access to relevant documents, but one interviewee said that they also encounter this difficulty when they are assessing a data controller's claim that data cannot be shared for reason of confidentiality. One expert clarified that this absence of leverage generally results in the initiation of additional proceedings for failure to cooperate with the DPA, which significantly extends the time of the proceedings that have been initiated.

> **This is probably the biggest problem that we face, namely the data controllers – either not providing that information or providing low-quality information. The long delays in the information that you get from the data controller. That is probably one of the main reasons why quality can sometimes be compromised and [why] certain investigations are very stretched out in time.**
>
> *An EU DPA staff member*

Some interviewees considered the inclusion of sanctions in national legislation as good practice when data controllers refuse to cooperate. However, one interviewee highlighted that, despite the sanctions included in their national legislation in cases of non-cooperation, some data controllers only allow access to their premises when DPA staff are accompanied by a police officer. Other interviewees underlined that it is good practice to establish a good relationship with the police for this purpose.

Promising practice: increased transparency and visibility for data controllers

In Denmark, at the beginning of each year, the DPA publishes a plan of its future supervisory work. The plan contains only information on the type of supervision, without identifying data controllers' names, organisations or authorities.

Source: Denmark, Danish Data Protection Agency (Datatilsynet), 'Special focus areas for the Danish Data Protection Agency's supervisory activities in 2023' ('Særlige fokusområder for Datatilsynets tilsynsaktiviteter i 2023'), 2023.

Promising practice: informing data controllers in advance of the subject of the inspection

In Portugal, before an inspection, preliminary work is conducted to make sure that the issues of concern are properly checked and evidence is collected (e.g. based on the matters raised in the complaint). The inspection team then develops a targeted checklist. The DPA may or may not communicate in advance to the organisation that it will carry out an inspection. This depends on the nature of and the reason for the inspection, in order not to prejudice the action. However, often the data controller or data processor is informed beforehand of the date and time of the inspection, and if specific staff or policies should be available during the inspection. This is to reinforce cooperation and speed up the process, since it is quite important to ensure that the relevant personnel is present and able to provide all the necessary information to the DPA.

Source: Portugal, Article 8 of Law 58/2019.

All in all, investigations are dependent on data controllers sharing relevant information with the DPAs, as emphasised by one interviewee. DPAs that do not have the technological and/or human resources to conduct further audits must rely on the information provided to them by data controllers.

> **Our biggest challenge lies in the technological retrieval of data – and the police have the know-how for this. This expertise is something we lack. If we were to carry out an unannounced inspection and copy the server to verify what data are stored there, it would require certain technical know-how to be able to crack it and get the necessary security credentials.**
>
> *An EU DPA staff member*

Promising practice: amicable settlements and mediation as a faster and more effective way to ensure effective data protection

Some interviewees recommended considering amicable settlements and

mediation sessions between parties. In its contribution, the EDPB reported a large disparity between Member States on this matter: half of them had never resolved complaints through amicable settlements. Of the Member States who have done so, half have used this option for fewer than 50 cases, and half (Ireland, Luxembourg, Hungary and Austria) for several hundred cases.

Belgian law establishes the option of reaching amicable agreements through the intervention of the DPA's front office, clarifying that this would not compromise the supervisory competency of the DPA. In 2022, the DPA received 177 requests for mediation and handled (and closed) 139 mediation cases. Mediation requests related mainly to data protection issues concerning commercial practices, such as direct marketing; image processing and cameras; and data protection in the professional sphere.

This has several benefits, as it shortens the time devoted to the investigation and provides a remedy in a shorter time frame. One interviewee noted that, as the objective of the DPA is to provide the complainant with a legal remedy safeguarding their personal data, facilitating a mediation session leading to a settlement expedites the investigation process and effectively corrects the data protection issue.

Article 5 of the 2023 proposed regulation introduces the option of resolving complaints through amicable settlements. The EDPB and EDPS highlighted in their Joint Opinion that, in its current version, the proposal is not sufficiently comprehensive and clear to effectively support DPAs that wish to settle cross-border cases amicably. This procedure involves a number of challenges, related to differences in national procedural laws, that the proposal does not address.

Sources: For further information, see EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97, 2023; and Belgium, Data Protection Authority (L'Autorité de protection des données), Service de Première Ligne, and Médiation et traitement des plaintes, from the 2022 annual report.

Promising practice: cooperation with the judiciary

One interviewee highlighted that establishing close cooperation with the judiciary has positive benefits for the conduct of investigations. Their DPA received guidance from the prosecution service when producing internal guidelines on how to obtain relevant information in accordance with the law.

Source: Interviews with staff of an EU DPA.

Another interviewee regretted that, in many Member States, obligation to cooperate in an investigation is limited to data controllers and data processors, when it could greatly benefit the investigation to extend the duty to collaborate to every person or institution of interest.

Finally, some interviewees pointed out the difficulty of dealing with data processing by individuals. Unlike legal entities, individuals generally process personal data at home rather than in a public office. In such cases, the power of the DPA to access premises can conflict with individuals' right to inviolability of the home. If the person does not grant access voluntarily, the only way for the DPA to exercise its powers is to obtain permission from the court, which is a lengthy process, and may give individuals time to destroy evidence. For one interviewee, such situations leave an impression of impunity, undermining the effectiveness of the sanctions, which are either delayed by more than a year or not imposed at all.

> **The GDPR is built as a legal act limiting big data controllers. But we need to apply it to trivial cases. The majority of cases are about settling disputes between two natural persons... Application of a legal act aimed at something big to small cases is complicated.**
>
> *An EU DPA staff member*

2.2. Handling complaints

2.2.1. Large number of complaints

Most interviewees highlighted how their capacity to supervise the enforcement of the GDPR was jeopardised by the large number of complaints they continue to receive on a regular basis. For several interviewees, lack of resources remains the main issue challenging their ability to comply fully with their supervisory obligations. In some cases, DPAs have to request the support of colleagues from other departments/specialities in supervision tasks related to the handling of complaints, to compensate for its lack of human and/or technical resources. Furthermore, some investigatory techniques that could help process complaints in a swifter manner are not being used due to the lack of appropriate experts in-house.

In two cases, interviewees stated that a lack of human and financial resources also prevents them

from conducting inspections across the whole country. To overcome this, one interviewee said that they ask notaries to conduct on-site investigations for them, but that they do not consider this good practice, as notaries and their colleagues may not have the expertise and technology that the DPA needs to efficiently conduct the inspection. The interviewee highlighted the fact that 'in many cases, the notary's on-site inspection is useless; therefore, we end up having to go there to conduct the investigation'.

Promising practice: lack of resources can be mitigated by grouping similar complaints

Several DPAs indicated grouping complaints on similar issues as good practice. When a DPA notices that a high number of complaints about a specific issue (e.g. data related to debts) are being lodged, it identifies these as a 'hot topic' or priority. Once grouped, the DPA first updates their materials and guidelines and then investigates the complaints together.

Source: Interviews with staff of several EU DPAs.

Several respondents stressed that, when it comes to the obligation of DPAs to respond to data subjects, a less stringent set of rules and more efficient criteria should be provided, as DPAs differ in size, level of resources and degree of governmental support.

> **In this regard, there is a notable tension between Article 77 of the GDPR, which states that all complaints must be processed, and Article 57(1)(f) of the GDPR, which indicates that complaints must be processed to the extent necessary. Does every individual complaint need to undergo the litigation process, or is there a prioritisation to be made? This type of discourse is touchy, but in any case, a structured approach to complaints must be organised in a reasonable and rational manner by each national legislator.**
>
> *An EU DPA staff member*

Promising practice: data-driven approach – mining data from previous complaints to respond more efficiently to future

complaints

One interviewee described how the DPA uses data generated from its supervisory activities to target its activities. To do this, the DPA registers all case-related information in a uniform way in its database. Reports on breaches of data security are equally useful to help decide where to conduct investigations. The interviewee said: 'One could get the idea that organisations where multiple data breaches have been reported constitute suitable targets for supervision, but it might reflect that the particular organisation knows when to report a breach and when to not report a breach. What might be more interesting would be to supervise those who we never hear from.' The DPA also uses these data to identify specific sectors that its supervisory activities could target.

Source: Denmark, Danish Data Protection Agency (Datatilsynet), Supervision with Effect – The Danish Data Protection Authority's strategy for a data- and risk-based effort, 2020–2023 (*Tilsyn med effekt Datatilsynets strategi for en data- og risikobaseret indsats, 2020-2023*), 2020.

2.2.2. Complaints against public administrations

A few interviewees mentioned that national legislation prevents them from using the full spectrum of levies in cases involving public administrations. In one case, the interviewee criticised the fact that their powers for supervising public bodies in charge of security or human rights-related matters, such as ombudspersons, have been greatly reduced. Similarly, two interviewees from the same Member State highlighted the opt-out of the public sphere from administrative punishment altogether as 'a major loophole' in the GDPR. Some interviewees regretted that public authorities cannot be fined.

> **"There are now certain limitations here that did not exist before. There has been a considerable reduction in the control of the DPA over (public bodies), which I do not think is appropriate. In general, it is not okay for anybody to be exempt from the DPA's oversight. What the GDPR has stipulated, that DPAs are not competent for the courts when they are adjudicating in court cases, is fine. However, it is not fine that a body remains outside the scope of the DPA.**
>
> *An EU DPA staff member*

In a recent judgment, the CJEU clarified that a parliamentary committee of inquiry set up to supervise the executive power must respect the GDPR – as long as the purpose of their inquiry is not to safeguard national security [73]. Public bodies that operate in fields related to national security are not de facto exempted from the GDPR. Each data processing activity must be assessed individually, and the public body is only exempt from GDPR provisions in cases where data processing activities are intended to safeguard national security.

2.2.3. Joint operations involving several data protection authorities

Article 62 of the GDPR allows DPAs to conduct joint operations involving two or more EU DPAs, either joint investigations or joint enforcement measures. For a joint operation to take place, certain conditions need to be fulfilled. Five joint operations were initiated between 2018 and 2023, according to the EDPB's annual reports [74] and its contribution to the report on the application of the GDPR under Article 97 [75].

Joint operations could be a useful tool for DPAs to strengthen mutual learning and understanding of the application of the GDPR, according to some interviewees. A couple of respondents argued that since joint operations are not an established practice, DPAs might not be inclined to resort to them.

Several respondents challenged the practical applicability of joint operations and pointed out five reasons why they are significantly underused.

1. A large majority of interviewees claimed that effective implementation of joint operations, including joint investigations, would require the EU to harmonise administrative rules and procedures. At present, DPAs must follow national procedures, which are Member State specific. Procedural challenges may arise concerning admissibility of complaints, which range from formal handwritten or electronically signed submissions in some Member States to less formal email submissions in others. Different administrative deadlines to comply with, and differences in the procedural rights of the complainant, might also hinder effective coordination among DPAs. Generally, national laws do not often permit public officers from other countries or other authorities to participate in on-site inspections, due to confidentiality clauses and non-disclosure obligations.

> **Even among comparably similar national legal systems, these [joint operations] can be problematic.**
>
> *An EU DPA staff member*

2. Multiple interviewees agreed that joint investigations are resource-intensive, in terms of both human and financial resources. They often concern complex cross-border cases, requiring specialist legal knowledge, or sometimes IT expertise. These resources are already under strain at most authorities, as Section 1.1 of this report highlights. Significant financial and staffing constraints do not allow for spare capacity for external endeavours, particularly if this involves redirecting legal or IT experts. One respondent reported an instance when a joint investigation was not initiated for these reasons, and added that there should be a special team of employees for joint investigations.

> **Speaking about joint investigations, the problem of lack of resources is relevant again. The DPA is a bit reluctant to initiate a joint investigation or participate therein, because such investigations will normally be needed for big cases, and they require a lot of resources. If the DPA joins one joint investigation, it might need to put on hold some national cases. This is something that can benefit more the large DPAs – with more resources.**
>
> *An EU DPA staff member*

> **If seven people work on investigations in the whole of the country and that is not enough to meet all [national] needs, then it is difficult or impossible to conduct joint investigations outside the country.**
>
> *An EU DPA staff member*

3. The employment relationship between the lead DPA and the experts deployed from other DPAs remains unclear, according to one interviewee. National rules and practices might regulate the remuneration of external public officers and their secondment differently, and in the absence of a common approach a memorandum of understanding or other

arrangements should be in place before undertaking joint operations.

4. Some interviewees mentioned that identifying and using a common work language in joint operations was challenging. Language skills and knowledge might vary among DPA officers, and official documents might be available only in the national language. Interpretation and translation should be provided, although the language of the data subject should be used when delivering decisions.

> **It is possible to prepare and coordinate a document in English, but then it has to be translated into a national language and presented as a decision from one Member State's authority. So something as simple as that can influence the decision to cooperate.**
>
> *An EU DPA staff member*

5. Some interviewees claimed that there is an imbalance between relatively well-funded DPAs (that have the necessary resources to respond to cross-border cases without seeking the support of other DPAs) and DPAs with fewer resources (that might need support but might find it difficult to get involved because of a lack of resources).

> **From the perspective of a smaller data protection supervisory authority and a smaller EU Member State, I understand that for the supervisory authorities of Member States that have a much larger role, are bigger, have 10 times as many employees – joint investigations are probably not their priority when they have their own investigations in which they issue fines of hundreds of millions of euros. To put it in simple terms, these (joint investigations) are not high on their priority list. Perhaps they could assign a few employees to handle such cases as part of their activities, in order to enable smaller supervisory bodies, in terms of population and number of employees, to participate more promptly and adequately.**
>
> *An EU DPA staff member*

In addition to these practical difficulties, several interviewees argued that formal ways of cooperating under the GDPR do not lead to swift cooperation schemes, particularly in the framework of joint operations. Formal requirements combined with different interpretations of the GDPR risk prolonging the decision-making process in cross-border cases requiring an urgent response. Some interviewees considered that informal ways of cooperating can deliver better and more timely results. A few cooperation models have been tested in practice, as described in the boxes below.

> **Joint investigations are difficult in any case as every country is different, it has different companies, etc., so these investigations would never end if DPAs would do it jointly. In small groups it is doable; for example, the Baltic countries have a more similar culture and procedural rules.**
>
> *An EU DPA staff member*

Promising practice: Baltic state DPAs – joint preventive supervision of specific sectors

In addition to joint investigations mentioned in the GDPR, some DPAs have resorted to informal ways of cooperating with other DPAs to lessen the administrative burden for each authority. The DPAs of the Baltic states (Estonia, Latvia and Lithuania) launched a preventive joint supervision on the compliance of personal data processing in the field of short-term vehicle rental (e.g. electric scooters). The joint supervision aims to issue recommendations to strengthen the protection of personal data in this specific sector and contribute to more consistent supervision across the Baltic states.

Source: Estonia, Data Protection Inspectorate, 'Supervisory authorities of the Baltic states launch of coordinated inspection of the compliance of personal data processing in the field of short-term vehicle rental', 2022.

Promising practice: a group of DPAs investigated Vinted UAB

for GDPR non-compliance

The Dutch, French, Lithuanian and Polish DPAs have joined forces to investigate the GDPR compliance of the online clothing sales website vinted.com, operated by the Lithuanian company Vinted UAB. After a significant number of complaints about the website were received in those countries, the DPAs set up a working group – facilitated by the EDPB secretariat – to coordinate action and support the lead authority, the Lithuanian DPA, in issuing an enforcement decision. The cooperation provided the Lithuanian DPA with considerable human resource support. The EDPB has agreed to use this form of cooperation in the future.

Source: EDPB, 'Vinted investigation signals closer and stronger cooperation between personal data protection supervisory authorities', 2022.

Several interviewees referred to the DPAs' commitment to fostering joint operations in cross-border cases, as expressed in the 'Statement on enforcement cooperation' in April 2022 [76]. Some suggested that the following could be further explored in the short term, with EDPB support:

- the identification of strategic priorities for cross-border cases when initiating joint operations;
- the collection of information on best practices from initiatives similar to joint operations;
- the development of an example of a joint investigation; the EDPB secretariat could take the initiative to conduct a joint investigation in a Member State to elaborate on the methodology for joint investigations and identify key procedural steps and resource needs;
- the development of training activities; the EDPB secretariat could facilitate training for all DPAs, to develop a common understanding and find a solution for practical issues in joint operations.

Most interviewees supported reform of the GDPR to set out a uniform procedure, binding at the EU level, that harmonises procedures and rules. A few interviewees underlined that 'binding' procedural mechanisms may be constitutionally challenging if, for instance, the supervisory authority from one Member State was able to conduct investigations in another Member State without the approval of its authorities.

Promising practice: informal collaboration between EU DPAs on specific topics

One interviewee mentioned that there are some examples of promising practices in terms of collaborations or conversations between national DPAs. These were described as very useful, even though they do not count as joint operations. The interviewee referred to actions developed when Italy made a decision to ban ChatGPT due to lack of compliance with the GDPR, and other DPAs considered

doing so. The interviewee's DPA established a European task force so that the different DPAs could follow a similar approach, and all of them initiated *ex officio* preliminary investigation actions against the US company OpenAI, owner of ChatGPT.

Source: Interview with staff of an EU DPA.

2.3. Ex officio investigations

An *ex officio* investigation takes place when a DPA initiates an investigation without prior notification of a data breach or a complaint filed by a data subject. While a significant number of own-initiative investigations have been launched [77], interviewees identified a number of limitations that DPAs face when conducting *ex officio* investigations, notably the large number of complaints (Section 2.2.1), and the lack of sufficient time and resources (Section 1.1).

There are three main obstacles preventing DPAs from launching more *ex officio* investigations:

- the large number of complaints,
- insufficient resources,
- time constraints.

Most interviewees raised concerns about resources being taken away from *ex officio* investigations because of the obligation to process every individual complaint received (in very large numbers, as highlighted in Section 2.2). This is quite problematic given that, as interviewees highlighted, *ex officio* investigations are arguably more important for the wider public than individual cases. They can include cases that the public may not be aware of, and therefore cannot make a complaint about.

> **"In the past, when there were not so many complaints, we could do more inspections, probe the ground ourselves and find out that there was a need for additional action in a certain area. The large number of complaints dictates the pace, and the ex officio inspections cannot be done as much. Our position is that these ex officio inspections help in advance to ensure that infringements do not occur in the most pressing areas. I would have liked to see more ex officio inspections in the health sector, in telecommunications; it seems to me that we could prevent a lot of infringements in this way.**

An EU DPA staff member

Given the time necessary to respond to each complaint within a certain deadline and the time-consuming nature of *ex officio* investigations, most interviewees raised lack of resources as an obstacle to carrying out *ex officio* investigations.

Nevertheless, individual complaints can help identify key areas and thus allow DPAs to prioritise self-initiated investigations in these areas, as highlighted by one interviewee.

> **We have no choice but to process each complaint. A large part of the effort is focused on processing complaints and notifications, leaving less room to use ex officio investigative powers. The resources are the decisive factor here, as the major part of them have been concentrated on processing complaints and notifications.**

An EU DPA staff member

The majority of interviewees emphasised that they would like to have more resources and time to conduct *ex officio* investigations. In fact, *ex officio* investigations can support the effective implementation of data protection, as they increase DPAs' ability to identify breaches that data subjects or data controllers are not aware of.

> **What we would also like to do more is ex officio investigations, because a lot of the digital world people don't see themselves. And we do see. People can't complain about that because they don't know at all.**

An EU DPA staff member

3. Data protection authorities as advisory authorities

> **We have invested in advisory work and guidance because we work preventively as well as reactively. Before, the Data Protection Authority would launch an investigation based on a complaint. Today, this has changed, and we now go into matters in which we have not received complaints. … We believe that by being proactive and working preventively, we can increase the level of data protection. If we only handle complaints, we neglect all those cases that have not been reported. If we don't work preventively, we only see the tip of the iceberg.**
>
> *An EU DPA staff member*

The GDPR has enhanced DPAs' advisory role, particularly its role in advising data subjects, data controllers and the public at large. Among the advisory tasks included in Article 57 of the GDPR is that DPAs should raise public awareness and understanding of data protection risks, rules, safeguards and rights associated with data processing [78]. They should advise national parliaments, governments and other public institutions on the potential implications of draft legislative and administrative measures on data protection [79]. They should also advise data controllers on high-risk data processing, following a data protection impact assessment [80].

The DPAs' advisory function is of utmost importance, according to a large majority of interviewees. The DPAs' advisory role is key to effectively enforcing data protection across the EU as, according to many interviewees, advising data subjects and data controllers prevents data protection breaches and complaints.

However, several interviewees mentioned that the DPAs' advisory function in fact conflicts with their supervisory tasks. Lack of resources (as emphasised in Chapter 1) prevents them from implementing the advisory tasks that the GDPR has entrusted to them. In most DPAs, oversight and supervision absorb most time and staff. Some respondents considered their authority to be **primarily** a supervision authority, and not a 'consultant'.

> **Whether we have sufficient resources is a relative question. We have the resources we have, and we have to make that work. If the ambition is that the DPA should increase its advisory activities, more resources should be allocated. It depends on the ambition.**
>
> *An EU DPA staff member*

One interviewee claimed that their DPA was able to exercise its advisory role only after receiving some additional budget to recruit and assign staff.

> **Earlier, when the DPA's resources were more limited, the DPA had to reduce its guidance function to be able to deal with the obligation to process complaints and do oversight. But now that the DPA has more resources, the DPA is allocating them towards guidance again as it is a useful preventative measure.**
>
> *An EU DPA staff member*

Interviewees mentioned two main ways of advising the general public on data protection issues: (1) by publishing guidance and (2) by organising workshops and/or public events with data controllers from the private and public sectors. Here, a difference can be observed between more and less experienced DPAs [81]. According to interviewees from more experienced DPAs, providing advice is a regular task of a DPA, whereas for more recently established DPAs, this is generally a secondary task. Less experiences DPAs struggle to find the time, human and financial resources, and technical knowledge to develop guidance and organise awareness-raising activities.

DPAs also deliver targeted advice, either in their responses to formal governmental or parliamentary queries on legislative proposals, or in their responses to data controller queries on future or ongoing data processing. Although time-consuming, several interviewees highlighted the added value of responding to these queries. It could help settle or prevent a misunderstanding in the application of the GDPR or help guide a controller to address data protection risks *ex ante*. It could also help foster a good relationship between the DPA and data controllers.

> **[The] personal contact approach is very useful. In writing, a lot gets lost (officials are not able to express themselves in an understandable way and people also interpret writings differently). Thus, it helps a lot when the DPA calls the person and explains the consequences of certain processing. Concerned entities are often not aware of data protection rules; hence, they are very grateful to the DPA when the DPA calls and explains to them and helps them to fix the non-compliance.**
>
> *An EU DPA staff member*

This chapter describes the challenges DPAs face when implementing the advisory tasks entrusted to them by the GDPR, as reported by interviewees. It examines difficulties in providing advice to data subjects and the general public (Section 3.1), to data controllers (Section 3.2), and to public bodies on legislative initiatives (Section 3.4), as the GDPR requires [82]. In addition, it reports on some interviewees' experiences of providing advice to researchers (Section 3.3) and highlights the importance of DPAs' partnership with data protection officers (DPOs) (Section 3.5). Finally, the last section of this chapter sheds light on the challenges that DPAs face when dealing with new technologies (Section 3.6).

3.1. Advising the general public

> **Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory … (b) promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing. Activities addressed specifically to children shall receive specific attention.**
>
> *Article 57(1)(b) of the GDPR*

FRA's findings identified similar trends in the public's understanding of data protection safeguards. On the one hand, DPAs noticed that awareness of data protection increased greatly following the adoption of the GDPR, which resulted in a rapid and substantial increase in complaints. On the other, DPAs found that a large majority of complaints are trivial or unfounded, and that very few complaints are lodged concerning sensitive data processing and misuse of personal data in the digital sphere.

In other words, while individuals' awareness of their rights has increased, an understanding of what the right to data protection entails is still lacking.

A majority of interviewees agreed that providing advice and reinforcing the public's understanding of what data protection means is an effective use of DPAs' resources and, ultimately, improves their ability to fulfil their mandate. Here again, lack of resources was said to have a negative impact on the ability of DPAs to provide direct and adequate advice in response to individual requests. For instance, some interviewees mentioned their incapacity to meet with individuals living outside the capital.

> **"The DPA lacks the financial means to organise events or to take part in other events – especially outside the capital. Because the authority doesn't have regional offices to decentralise the work, it needs to answer demands from opinions from all over the country via email – to mayors, to governmental county-level services (e.g. health insurance, pensions), to data controllers, etc.**
>
> *An EU DPA staff member*

In some Member States, DPAs have set up hotlines for individuals to enable the authority to assess the merits of their grievance before they file an official complaint. Most interviewees pointed out to FRA that a handful of staff must be dealing with high numbers of minor or petty complaints, often similar in content (e.g. related to neighbours installing a CCTV camera, a recurring complaint mentioned by most interviewees). Nonetheless, these hotlines require additional human and financial resources, which many DPAs are lacking.

Systematic complaints handling – as explained in the box Promising practice: a group of DPAs investigated Vinted UAB for GDPR non-compliance – also supports DPAs in finding the appropriate advice for the general public and data controllers in a swift and evidence-based manner.

> **The idea is that they (junior lawyers) are there to take legal questions, but, in practice, it is more than this, such as questions about the processing of current cases, and, when the public hears our name, many people think that our organisation handles much more than what is in our mandate, with individuals calling in to report how their integrity has been violated, putting our colleagues in a therapist-like role at times.**

An EU DPA staff member

Promising practice: providing advice in a regular, structured and systematic manner based on complaint assessments

Some interviewees pointed out that the regular and systematic logging of recurrent complaints received and advice provided on specific issues has helped avoid duplication of effort among DPA staff members. These repositories and databases include different tools, such as a list of standard responses, a catalogue of examples of good decisions, and a regular update of the questions and answers published on the DPA's website.

Source: Interviews with staff of several EU DPAs.

3.2. Advising data controllers

> **Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: … (d) promote the awareness of controllers and processors of their obligations under this Regulation.**

Article 57(1)(d) of the GDPR

> **The controller shall consult the supervisory authority before processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.**

Article 36(1) of the GDPR

A majority of respondents highlighted the importance of providing guidance to data controllers, both to ensure correct implementation of the GDPR and to reduce workload when investigating data processing. Interviewees from multiple DPAs said that such requests must be prioritised given the tight deadline to respond established in the GDPR [83] .

Several interviewees referred to the obligation, under Article 35 of the GDPR, to conduct a data protection impact assessment (DPIA) in cases where 'a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'. When the data processing would result in a high risk to individuals' right and freedoms, and in the absence of measures taken by the controller to mitigate the risk, Article 36 of the GPDR requires data controllers to consult with the DPA.

However, some respondents noted that, in practice, data controllers rarely seek the DPA's advice pursuant to Article 36 of the GDPR. The scarcity of requests and prior DPIAs is a direct consequence of many data controllers' lack of understanding of the potential risks of inadequate data processing. Interviewees agree that awareness-raising actions targeting specific fields of activities should be conducted to prevent inadequate data processing.

Several interviewees highlighted specific difficulties that further complicate DPAs' function of advising data controllers in both the public and private sectors. First, in some cases DPAs might not be able to assess the potential risks of a processing operation without carrying out an on-site visit; however, as reported by some interviewees, this can only happen during *ex post* inspection. Second, some interviewees found that the lines between their advisory and investigatory roles are sometimes blurred. While DPAs wish to provide data controllers with clear guidance on data protection safeguards in data processing, in practice they can give only general advice. Interviewees clarified that this was to avoid DPAs, in the case of investigations, having to supervise the implementation of their own guidance.

> **If someone wants very detailed advice on their own system, for example, it could easily create a situation where, if the data subject later complains to us, we would have to assess the actions of a controller that we have previously advised on. [Hence,] we can [only] provide general guidance.**
>
> *An EU DPA staff member*

Promising practice: develop targeted and sector-specific guidance

In Sweden, the DPA's information service can send information letters. These letters explain to parties involved in a complaint what legal obligations the GDPR demands of individuals or organisations with access to and responsibility for personal information. The objective of these letters is to get the responsible actors within different organisations to comply voluntarily with the GDPR.

Source: Interview with staff of the Swedish DPA.

Promising practice: development of sandboxes

Some interviewees underlined the importance of dedicating more time and resources to the development of sandboxes. While there is not a common definition of a sandbox, the European Commission's Better Regulation Toolbox describes regulatory sandboxes as schemes in which stakeholders can test innovations in a controlled environment, under the guidance and oversight of a competent authority.

An interviewee said:

… the sandbox method is a very successful way of working as it allows us to give better guidance on new technology while we learn an enormous amount about the technology itself. For example, we gained knowledge of AI technology federated

learning, discovering things we would never have known otherwise. We sat with data scientists involved in the project and looked in detail at how the algorithm was built, learning what it means and what consequences the technology has for data protection.

Source: European Commission, *Better Regulation Toolbox, 2023.*

Third, some respondents highlighted difficulties that apply specifically to advising public authorities and bodies when they are acting in their capacity as data controllers, that is, when the DPA provides advice to them on specific data processing, and not within the procedure of advising on draft laws or legal initiatives. In some Member States, DPAs are not allowed to issue fines to public entities, only recommendations. Hence, as one interviewee explained, DPAs' advisory role is not sufficiently acknowledged by public authorities, as recommendations are not enforceable. Some interviewees also claimed that public bodies distrust, and sometimes fear, DPAs when it comes to asking them for opinions on data processing, as highlighted in Section 2.2.2. For instance, one respondent witnessed a case where a public sector body developed a data processing operation without contacting the DPA in advance because of a fear of a 'no' from the DPA's side. Thus, 'public authorities rather develop and deal with consequences later … ', as one interviewee put it.

3.3. Focus – advising researchers is challenging

To support research and innovation, the GDPR includes a 'special regime for scientific research' in Article 89, as explained in the EDPS's preliminary opinion on data protection and scientific research [84], which applies to the processing of personal data for 'archiving in the public interest, scientific or historical or statistical research purposes' [85]. In this context, Article 89 of the GDPR allows for certain exceptions to the data protection guarantees under certain conditions (e.g. the existence of technical and organisational measures).

During the COVID-19 pandemic, several DPAs were confronted with increasing requests to provide advice on the use of sensitive medical data of COVID-19 patients for research purposes. The box Promising practice: develop targeted and sector-specific guidance describes an example.

Promising practice: DPA advice on scientific research during the COVID-19 pandemic

In the Netherlands, the House of Representatives asked the DPA for an opinion on the use of vaccination data for research on the high mortality rates during the COVID-19 pandemic. The DPA recommended that Statistics Netherlands could use

the data from the National Institute for Public Health and the Environment for the intended purposes. The DPA stated that this research was permitted under the GDPR, but called on the Ministry of Health, Welfare and Sport to consider legislation clarifying the use of health data for scientific research.

Source: The Netherlands, Dutch Data Protection Authority (Autoriteit Persoonsgegevens), Request for advice on research into excess mortality (Advise AP onderzoek oversterfte), 2023.

Most respondents, however, could not recall any practical experience of providing advice to researchers in the field of scientific research, apart from the advice delivered during the COVID-19 pandemic. Among those who could recall some examples, only a few stated that the GDPR has allowed for a certain consistency and awareness the of safeguards that should be put in place when processing personal data for research-related purposes.

> **There is an incentive among researchers to carry out a lot of anonymisation, pseudonymisation and encryption, decentralised data storage and early deletion, because this gives them the freedom to use data for their own purposes.**
>
> *An EU DPA staff member*

For several interviewees, however, the implementation of Article 89 of the GPDR has been challenging [86]. In 2019, national differences in the implementation of Article 89 were identified in a study commissioned by the EDPB [87]. In this report, FRA research identifies the following two challenges.

First, the complexity of the applicable legal framework and uncertainty about the legal basis of data processing were repeatedly mentioned as an issue of concern in this context. In addition to the GDPR, specific legislation may apply to the processing of personal data in a certain field; for example, sectorial laws regulating medical research [88], clinical drug trials [89] and statistics [90], at both the EU and national levels [91]. The plethora of applicable EU and national legislation has made it difficult for researchers – and data controllers – to identify a legal basis for a processing operation, according to many interviewees. Many interviewees mentioned that EDPB guidance in the area of clinical trials is useful in this respect [92]. The data subjects concerned may also be affected by the lack of legal clarity, ultimately discouraging them from

exercising their rights [93]. Both researchers and the general public would therefore benefit from further guidance on correctly applying the GDPR for the purpose of research, to avoid legal uncertainty hindering innovation. The importance of providing further guidance, especially on sharing sensitive data with researchers and monitoring discrimination caused by bias in algorithms, was underlined in FRA's previous work [94].

Second, respondents noted that in some Member States public authorities have been reluctant to grant access to personal data for research purposes and that, in a couple of Member States, the GDPR has often been used as justification for refusing such access. One respondent explained that the GDPR states only under what circumstances information **might be** provided, but does not address under which circumstances it **must be** provided, hence creating uncertainty. Therefore, granting access to data for research purposes by public authorities is another field that requires further clarification, potentially through the development of specific EDPB tools or guidance.

In addition, some interviewees mentioned that the GDPR should not be used to justify refusing access to data, but as a legal framework governing this access.

> **We have provided guidance to researchers in several cases, and we often had to open doors to researchers where the added value of the research warranted this, and the data controller was being extra, and unnecessarily, cautious. The role of the DPA is to open doors by suggesting anonymisation and proposing different methodologies, encouraging researchers to exercise proportionality, because often researchers ask for significantly more information than what is needed to extract their conclusions.**
>
> *An EU DPA staff member*

Against this background, interviewees from a few Member States questioned whether the GDPR provides sufficient legal clarity to enable them to consistently transpose the derogations and safeguards provided for in Article 89 across the EU. One respondent suggested that the provision should require Member States to adopt national legislation on the applicable derogations under the GDPR when data are processed for scientific research purposes. Such legislation is prescribed in Article 85 of the GDPR, which states that the applicable derogations for processing data for journalistic purposes should be prescribed in national law [95].

As a final point, some respondents brought to FRA's attention that in most EU Member States DPAs are no longer providing prior authorisation for the use of personal data for scientific research purposes. This was a requirement under Directive 95/46/EC [96], repealed by the GDPR.

In one Member State, the DPA still provides 'permission' for certain personal data processing for research purposes, but it does not authorise the processing of sensitive data, which falls under the competency of the national ethics committee. Some respondents found that the authorisation system was useful for keeping DPAs informed, updated and aware of potential data protection risks in data processing in the field of research.

DPAs have developed several practices and initiatives to address these concerns and raise awareness among researchers and data controllers of the applicable data protection safeguards when processing data for research purposes. Some of these practices are highlighted in the following boxes.



Promising practice: research plans that justify the need to obtain personal data

In Hungary, the DPA systematically requires researchers to provide a research plan justifying the need for obtaining personal data. This is submitted to the public institution along with the request for access to the data. This was confirmed in a DPA decision, which clarified that while archived material containing personal data should not be consulted by researchers, this prohibition may be lifted if the researcher complies with additional requirements, including providing a detailed research plan and attaching to his/her application a supporting statement from the public body conducting the research.

Sources: Interviews with staff of the Hungarian DPA; Hungary, National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság), Decision NAIH/2016/2504/27/H, 2017.



Promising practice: privacy research days

Since 2022, the French Data Protection Authority, the National Commission on Informatics and Liberty (CNIL), has organised a 'Privacy Research Day' to build bridges between researchers and data protection regulators. The event gathers legal experts, computer scientists, designers and researchers in social science.

Source: France, National Commission on Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés), 'Privacy research day: Discover the program of the first CNIL's international conference', 2022.

Promising practice: online guidance on scientific research and data protection

The Finnish DPA has published online a 'data protection roadmap for scientific research', which provides guidance to controllers when considering data protection in different phases of research and the lifespan of data. The roadmap consists of 10 steps that researchers should follow. They include defining the basis of the processing, ensuring data protection subjects' rights, and documenting the implementation of data protection principles and other procedures specified in the GDPR during the lifespan of the research project. The roadmap is also available in English.

Source: Finland, Data Protection Authority, 'Scientific research and data protection'.

Promising practice: developing dialogue and exchanges with research and statistics institutes

Several DPAs have developed channels for exchange with research and statistics institutes. For instance, the Italian DPA developed a regular exchange with a network of DPOs working with research-related bodies. In addition, it is cooperating closely with the Italian National Institute of Statistics (ISTAT). Following the advice of the authority, ISTAT succeeded in pseudonymising a large number of personal data.

Source: Interview with staff of the Italian DPA.

Promising practice: developing cooperation with ethics boards

In Lithuania, the DPA cooperates closely with the Academic Research Ethics Board. The two institutions have worked together to develop guidelines on how to conduct research and how to reconcile this with data protection. Similarly, they cooperated in drafting the Health Data Re-Use Act, which regulates the use of health data for research purposes. In Latvia, DPA representatives take part in the

Commission on Ethics in Research at the University of Latvia, where researchers present their plans and the DPA can provide its assessment on data protection, if necessary. In Malta, the Data Protection Act requires researchers to obtain prior authorisation from the DPA before processing genetic, biometric, health or social care data. To comply, the DPA collaborates with the University of Malta's Research Ethics Committee, which issues an initial assessment of each research proposal, including data protection compliance. The DPA then decides whether to authorise the research or not. This collaboration ensures compliance with the law.

Source: Interviews with staff of several EU DPAs.

3.4. Advising on legislative initiatives

> **Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: … (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing.**

Article 57(c) of the GDPR

> **Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.**

Article 36(4) of the GDPR

Providing advice and legal opinions to governmental or public bodies is not a new responsibility of DPAs. Some respondents highlighted that, prior to the GDPR, domestic legal frameworks entrusted DPAs with advisory responsibilities, that is, providing detailed opinions on legislative draft proposals or other administrative measures affecting the individual rights to data protection. In some cases, however, respondents emphasised that the GDPR did make clear the obligation of state authorities to consult the DPA. Some interviewees did acknowledge increased interest from the government in the DPA's opinions.

Several interviewees indicated that providing advice on draft laws is a crucial task, if not a priority, as it may prevent future complaints and data protection risks by ensuring the inclusion early on of data protection safeguards in the law. The sense of making it a priority is strongly reinforced when they see the direct impact of their recommendations in the amendments, or even sometimes in the withdrawal, of draft legislative texts, according to some interviewees.

> **The DPA is a kind of preventive supervisor of legislation. It is actually quite nice that the DPA has this function of advisory body. The DPA recently issued its opinion on a new bill … In this opinion the legislator was told that this bill cannot become law because it is in violation of the EU Charter. … Because the DPA is a supervisory body with investigatory and sanctioning powers, its opinions and recommendations carry more weight. These are not really opinions but legality assessments.**
>
> *An EU DPA staff member*

DPAs should be able to provide advice on their own initiative, by commenting on any legislative initiative, as long as there are data protection implications, according to some interviewees. They should not only respond to official requests prior to the enactment of legislation. In practice, however, lack of resources prevents DPAs from providing unsolicited recommendations, despite their will to do so.

> **What the DPA would really like to do is provide unsolicited advice, but, due to capacity problems, we don't get around to doing that.**
>
> *An EU DPA staff member*

Only a few respondents acknowledged increased interest from the government in their opinions following the entry into force of the GDPR. Most respondents pointed out some deficiencies undermining the delivery of independent advice, as Section 1.2.1of this report outlines.

- Several respondents underlined that DPA recommendations, being non-binding, are not always considered by the legislator. The same goes for policymakers, who are not obliged to incorporate DPAs' advice into negotiated legislation. However, interviewees insisted on the importance of acting proactively during legislative processes.
- Some respondents noticed differences between DPAs and other comparable public bodies (e.g. ombudspersons) in the provision of legal advice and recommendations on draft laws. In one case, an interviewee expressed concern over the fact that a recent amendment now prohibits the DPA from providing fundamental comments, that is, comments that should be considered by the authority in charge of the legal proposal. In another Member State, the DPA is not allowed to request a constitutional review unless an inspection procedure is launched – while other public bodies may do so.
- Several interviewees lamented the fact that their government does not always consult the DPA prior to the enactment of legislation that affects the protection of personal data. Several reasons were indicated. In some cases, the failure to request the DPA's opinion was attributed to a lack of understanding of the potential data protection implications of a draft law. In one case, the interviewee mentioned some hostility from the government, which perceives the DPA as a barrier to innovation – but clarified that such hostility ceases after the DPA provided clarification.

> **"And then there are still issues that the government and parliament still forget on matters of data protection. For example, when changes to the … Law were under discussion, the DPA was not heard.**
>
> *An EU DPA staff member*

> **We are not seen in a good light by certain quarters because, for them, data protection is there to stop innovation, to stop processes, to pose restrictions, to put safeguards which might stifle innovation. So, this is a general perception.**
>
> *An EU DPA staff member*

- Fourth, the absence of government consultation, or the very short deadline provided to the DPA to respond to a request for legal opinion – as described in Section 1.2.1 – were noted to not only hinder DPAs' capacity to provide advice during legislative processes, but also contribute to the large volume of complaints received by DPAs, as the quotes below describe.

> **The COVID-19 pandemic was a difficult experience for the DPA, which would have preferred that the government contacted the DPA when drafting the measures, but did not – there would have been much less anger among the people and the DPA would have received far fewer complaints.**
>
> *An EU DPA staff member*

> **For example, the DPA received a hundred complaints, virtually identical, as a result of one processing of personal data, until the DPA announced, through the media, that it was already dealing with the matter and that no further reports were necessary. The DPA would have had far fewer problems if the government had consulted the DPA. On many occasions, the DPA learned of the content of a draft law through journalists.**

An EU DPA staff member

Promising practice: regularly exchanging with authorities and acting proactively

Some interviewees highlighted the importance of acting proactively to reinforce DPAs' advisory role during the legislative process, both by contacting ministries and requesting to be kept up to date on potential future legislative initiatives, and by providing unrequested recommendations on draft laws. In general, respondents who mentioned acting proactively also told FRA that processes and exchanges are generally going smoothly with governmental bodies.

One interviewee also mentioned that a collaboration with the ministry of justice proved to be very successful: 'When the project finally reaches the Ministry of Justice, it either introduces the DPA as an advisor or asks for the authority's opinion if the initiator has omitted this aspect'.

Source: Interviews with staff of several EU DPAs.

- Fifth, interviewees insisted that neutrality and prudence are key when approached by ministries with questions related to future draft laws. DPAs may give advice during the drafting of a text but they must clarify that this is not a formal assessment on their part and it is not a guarantee that the draft proposal is data protection compliant.

> **We are expected to say in such a case that one solution is legal and another is not. We cannot say that. We can only do that when there is an inspection, when some personal data processing is actually under way, and only then can we make an assessment … We give basic instructions, we point out some past cases, what was the solution, what they didn't pay attention to, etc. We certainly give some guidelines. The problem with this is that you don't get all the relevant information. It is human nature to give information that leads to the conclusion that a certain solution is appropriate. They don't tell you the downside, either deliberately or not, because they are not aware of (the downsides), because that's why they come to us for our opinion.**

An EU DPA staff member

Promising practice: create guidelines specifically tailored to ministries developing legal initiatives

In some Member States, DPAs have developed guidelines specifically aimed at ministries in the process of developing new laws, to guide them and ensure that data protection is taken into account. Another interviewee mentioned that training is being organised for lawyers working in ministries. However, for now, it remains difficult to assess the real impact of these measures.

Source: Interviews with staff of several EU DPAs.

- Sixth, and contrary to the trend identified by some DPAs, several interviewees highlighted that they receive a high number of official requests to comment on draft laws, even when these have no data protection implications. Interviewees expressed different views on this. It was perceived by some as a positive trend where the legislator is taking the protection of personal data seriously. However, some respondents were concerned that such a large number of requests from governmental bodies is hampering DPAs' activities and may ultimately prevent them from developing in-depth analyses. Two interviewees said they believe this to be intentional.

- Seventh, in some Member States, DPAs have noted that their government still lacks an understanding of the potential risks to data protection. This is particularly the case in the area of legislation on the digitalisation of public processes.

This lack of understanding translates into concrete challenges, delaying the provision of legal opinions, according to some interviewees. On the one hand, it has resulted in a lack of clarity about certain data processing operations. On the other hand, DPIAs are rarely conducted before consulting the DPA.

Promising practice: enhanced cooperation with DPOs in ministries

In one Member State, the DPA reported good cooperation with the DPO's office within one of the ministries. After the office was established, the DPA noticed a real improvement in the understanding of data protection implications of draft laws.

Source: Interviews with staff of an EU DPA.

3.5. Data protection officers: privileged partners for data protection authorities

The requirement included in Article 37 of the GPDR to establish a DPO was not a new requirement of the GPDR. However, the regulation did broaden the obligation to data controllers and data processors that might not have been required to contract a DPO under the 1995 directive. The task of the DPO is to inform, advise, and act as a contact person between the controller/processor and the DPA.

A large number of DPOs were recruited in a short period of time following the entry into force of the GDPR. In 2019, a study by the International Association of Privacy Professionals [97] (IAPP) estimated that 500 000 organisations had registered a DPO across Europe [98].

Several interviewees discussed the impact of this on DPAs. Some respondents connected it with their recruitment difficulties, associating the large-scale DPO recruitment by private and public entities with a data protection experts' 'brain drain'. Interviewees also flagged the salary imbalance that can exist between private and public sector employment as an additional difficulty for DPAs when competing with the private sector to recruit high-level experts in such a niche field, as Section 1.1.2 discussed in more detail. This difficulty is shared by public authorities in general. In three Member States, the DPA evidenced the absence of a DPO either in public bodies or in both

private and public bodies and requested these bodies to hire a DPO, it was reported to FRA.

> **The majority of municipalities either no longer have the data protection officers (they are required to have one, but as they are exempted from fines, they usually opt for saving the money and are no longer paying for DPOs), or outsource the issue to someone who does not function properly.**
>
> *An EU DPA staff member*

Some interviewees highlighted how DPOs have been playing a crucial role in their work, by preventing potential violations of the GPDR, thanks to their understanding of the legal frameworks, and by developing a meaningful and useful communication channel between the DPA and data controllers.

Promising practice: communication and training material tailored to DPOs

Several interviewees mentioned the development of information materials specifically targeted to DPOs as a good practice to reinforce their knowledge. These tools take different forms, such as the organisation of workshops, training or conferences, the publication of guidance, the setting up of a DPOs' network, the regular sending of information bulletins, etc.

Source: Interviews with staff of several EU DPAs.

The role of the DPO is regarded as an essential preventive measure for effective enforcement of the GDPR, and, for several interviewees, DPOs are considered to be partners.

3.6. Lack of expertise to for responding to challenges related to new technologies

> **Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. … Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.**
>
> *Recitals 6 and 7 of the GDPR*

> **Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: … monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular, the development of information and communication technologies and commercial practices.**
>
> *Article 57(1)(i) of the GDPR*

Respondents were asked about the capacity of their authority to respond to challenges stemming from new technologies, such as AI and machine learning, and encompassing blockchain and crypto assets, the internet of things, facial recognition and connected vehicles, for example.

A majority of respondents believe that the tools provided in the GDPR are, in theory, sufficient. However, most of them also mentioned several issues that can have an impact on their effectiveness in addressing issues stemming from the use of new technologies.

- First, several respondents indicated they are mostly unprepared when it comes to understanding and assessing new technologies.
- Second, a number of interviews were ambivalent about the adequacy of the GDPR, believing that it is adequate but insufficient. Most interviewees referred to the generic and

technological neutrality of the GDPR as both a positive and negative. With regard to AI, it leaves too much room for interpretation, and DPAs believe that guidance is greatly needed. For instance, one interviewee explained that when it comes to AI the GDPR is reaching its limits, as AI is creating a conflict with the data minimisation principle.

- Third, several interviewees expressed concerns about the clarity of their role in the constellation of multiple data-related acts. Because other EU laws on new technologies (such as the Digital Services Act and the proposed Artificial Intelligence Act) also directly touch upon data protection issues that are covered in the GPDR, how to coordinate and deal with potential overlaps of mandates of supervisory authorities remains unclear [99] .

> **The GDPR is technology neutral. But it is difficult to pigeonhole some new technologies. An example concerns blockchain: who is the controller and who is the processor?**
>
> *An EU DPA staff member*

> **The technological neutrality of the legislation in this matter leaves the task of constructing an understanding of new technologies, and their relation to the GDPR and other regulatory instruments, on the shoulders of the judicial system. Often these interpretative matters are not limited only to constructing what is personal data, but more broadly what is technology.**
>
> *An EU DPA staff member*

Most respondents indicated that their authority has had almost no practical experience or concrete cases involving new technologies. For those who have had some experience, the cases related mainly to video surveillance, the use of biometrics, the use of AI and machine learning, and large-scale leaks of personal data. According to these respondents, the main challenges when dealing with AI and new technologies lie in:

- the access given by the data controller to the DPA inspector, which depends on the level of

trust the data controller has in the inspector, given the related trade secrets and sensitivity attached to such technologies;

- the access to information/premises by non-EU data controllers, and, notably, these being based in non-EU countries (e.g. the United States or China);
- the feasibility of assessing the proportionality of the use of personal data;
- the feasibility of assessing the explainability and transparency of the use of such technologies.

Despite the relative absence of concrete cases, the majority of respondents underlined that they mostly feel unprepared when it comes to new technologies. Interviewees identified (1) the lack of time to conduct research, test cases, etc. on specific technologies and (2) a shortage of IT experts among DPA staff with knowledge and experience of new technologies.

Respondents highlighted this as an issue that is preventing them from (1) conducting appropriate research on the tensions between new technologies and data protection, and (2) providing data controllers with appropriate guidance. For instance, two respondents referred to blockchain as an example of a technology that may not be compliant with some provisions of the GDPR. Given that blockchain works with an unchangeable chain of blocks it may not be compliant with the principle of accuracy [100] or the right to rectification [101] or erasure [102]. Another respondent emphasised that anonymity is a real issue when dealing with cases involving new technology, as more advanced technologies cannot rely on fully anonymised data. In addition, anonymisation becomes more difficult, as modern techniques allow for tracking anonymised data back to data subjects. At the same time, the GDPR requires data used for the development of these technologies to be anonymous.

A few respondents also noticed unpreparedness on the side of the data controllers regarding new technology, further reinforced by the fact that data controllers do not use tools such as prior consultations and DPAIs.

Several respondents once again made a link to human resource shortages, notably IT specialists, as indicated in Section 1.1.2. Several interviewees believe that the only way to overcome these difficulties is to increase cooperation with the EDPB and with other DPAs from EU Member States and European Economic Area countries. Some respondents highlighted the potential for the EDPB pool of experts to provide DPAs with technological expert knowledge they may lack.

> **We as an institution would like to deal with new technologies and their impact. Because, in my opinion, it is the aim of the GDPR – to follow the new technologies and to ensure that those do not violate human rights and that we maintain the balance ... However, unfortunately, due to minor disputes between private persons (that represent a large part of complaints received), we are unable as a supervisory authority to examine those cases which really impact the aim of the GDPR.**
>
> *An EU DPA staff member*

Promising practice: Establish a research team dedicated to new technologies within the DPA

The Polish DPA has established a new department – the Department of New Technologies – which is among other things responsible for:

- preparing opinions on new technological solutions in terms of their impact on the security of personal data processing;
- analysing and participating in the drafting of opinions and documents on technological developments and their impact on personal data protection within international working groups;
- drawing up opinions and providing consultations to other DPA departments, within the framework of the matters they deal with, on the processing of personal data in IT systems;
- drawing up opinions on issues relating to the processing of personal data in IT systems;
- monitoring new technological developments with regard to data processing and providing information about them to the other departments of the DPA.

The Department of New Technologies has its own staff but regularly coordinates with employees from other departments, such as the IT department, which supports the new department with its expert knowledge.

Sources: Poland, Statutes of the Personal Data Protection Office; Poland, Polish DPA Annual Report 2021 *(Sprawozdanie z działalności prezesa urzędu ochrony danych osobowych w roku 2021),* 2021, pp. 17 and 24.

Interviewees were ambivalent about the adequacy of the GDPR to answer such challenges. For most of them, the technological neutrality of the EU data protection legislation is a positive thing. However, a majority of respondents indicated that the GDPR is not sufficient for addressing data protection concerns related to the use of new technologies. One respondent observed, for example, that 'what is complicated is how to judge whether a new technology fits within the GDPR'. Giving the example of AI, the respondent said that it is difficult to assess whether algorithms that have used personal data for training purposes but do not process personal data once launched would be covered by the scope of the GDPR.

The challenge of applying data protection law to new technologies, such as AI and algorithms, was also highlighted in FRA's 2020 report on AI and fundamental rights [103].

> **So, there is always a rather large gap between the important questions that come up in the context of new technological development and the guidance EDPB can give; I think this gap will always be a large one.**
>
> *An EU DPA staff member*

Several DPAs expressed some uncertainty about what to expect regarding their role in the European Commission's numerous recently adopted and proposed acts related to data, including the Artificial Intelligence Act [104], the Digital Services Act [105], the Digital Markets Act [106], the Data Act [107], the Data Governance Act [108], the interoperability acts [109] and the Single Digital Gateway Act [110]. Several interviewees also expressed concern that the relevant legal frameworks may be fragmented, potentially resulting in contradictory legal requirements and conflicts with other national regulatory authorities.

In July 2022, the EDPB and EDPS expressed similar concerns about the Commission's proposal for a regulation on the European Health Data Space: 'Regarding the governance model created by the proposal, the tasks and competencies of the new public bodies need to be carefully tailored, particularly taking into account the tasks and competencies of national supervision authorities, the EDPB and the EDPS in the field of processing personal (health) data. Overlap of competencies

should be avoided and fields of and requirements for cooperation should be specified' [111] .

> **It also becomes more and more complex with the upcoming new legal instruments, for example with the new legal acts (the Artificial Intelligence Act, the Data Governance Act, the Data Act, etc.) for which the DPA will certainly play a role even though such role is not yet exactly clear yet. Our challenge is: how can the DPA give proper supervision on this?**
>
> *An EU DPA staff member*

Promising practice: DPAs coordinating the supervision of AI with other national regulators

The Dutch DPA has had a coordinating role in the supervision of algorithms since 2023. This role involves coordinating the work of various agencies with competencies in supervising algorithms and AI. Coordinating duties include identifying and analysing cross-sector risks, promoting a joint interpretation of standards in supervisory practice and establishing a public register for AI algorithms in the Netherlands. It will also foster a better understanding of data protection legislation and may prevent misinterpretations of new developments, such as algorithms, by other regulators.

Source: The Netherlands, Dutch Data Protection Authority (Autoriteit Persoonsgegevens), '*Algorithm Supervisor Establishment Note' ('Inrichtingsnota algoritmetoezichthouder')*, 2022.

4. Data protection authorities as cooperating authorities

> **The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: … draw up guidelines for supervisory authorities …; issue opinions on draft decisions of supervisory authorities …; promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities; promote common training programmes and facilitate personnel exchanges between the supervisory authorities …; promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide …; maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.**
>
> *Article 70(1)(k), (t), (u), (v), (w) and (y) of the GDPR*

The creation of the EDPB as an exchange platform for DPAs to develop guidance and to cooperate is not an innovation of the GPDR: national DPAs have been meeting since the 1995 directive entered into force through the so-called Article 29 Working Party. However, the GDPR gave the EDPB a separate legal personality, as it now operates as an independent body of the EU, and it broadened the tasks and powers allocated to the board and its secretariat.

In its first evaluation of the GDPR, the European Commission emphasised the key role that the EDPB must play in the new EU data protection accountability framework, which has the notions of harmonisation and cooperation at its core [112]. These notions are central to the feedback FRA received when discussing with DPA staff members how they assessed their collaboration and the role of the EDPB. In the 'Statement on enforcement cooperation' [113] adopted in April 2022, the EDPB demonstrated its commitment to promoting harmonisation to enhance cooperation in the GDPR enforcement framework.

Interviewees agreed that strong cooperation between DPAs ensures swift enforcement and interpretation of the GDPR. Some respondents identified a need for a common methodology to

help overcome practical issues related to the procedures to follow when engaging in cooperation with other DPAs. In particular, there is a need for information on best practices and guidance that would help to ensure smooth cooperation between authorities.

4.1. The European Data Protection Board's added value

The responses received by FRA concerning the EDPB were mostly positive. Several interviewees – notably from smaller Member States – said that the EDPB is playing a positive role in reinforcing the cooperation, exchanges and discussions between them. Specifically, they said that the pilot exchange programme [114] is a good source of expertise from more experienced DPAs. The EDPB's secondment programme was established in 2019. Paused during the COVID-19 pandemic, it started again in a pilot phase in 2022 and will be deployed throughout 2023 and 2024. The programme aims to facilitate the exchange of staff members, for a short period of time, between authorities.

> **The EDPB works as a discussion forum, where the national supervisory authorities can share information and discuss topics of interest such as national practices, differences in the national procedural rules, and protocols.**
>
> *An EU DPA staff member*

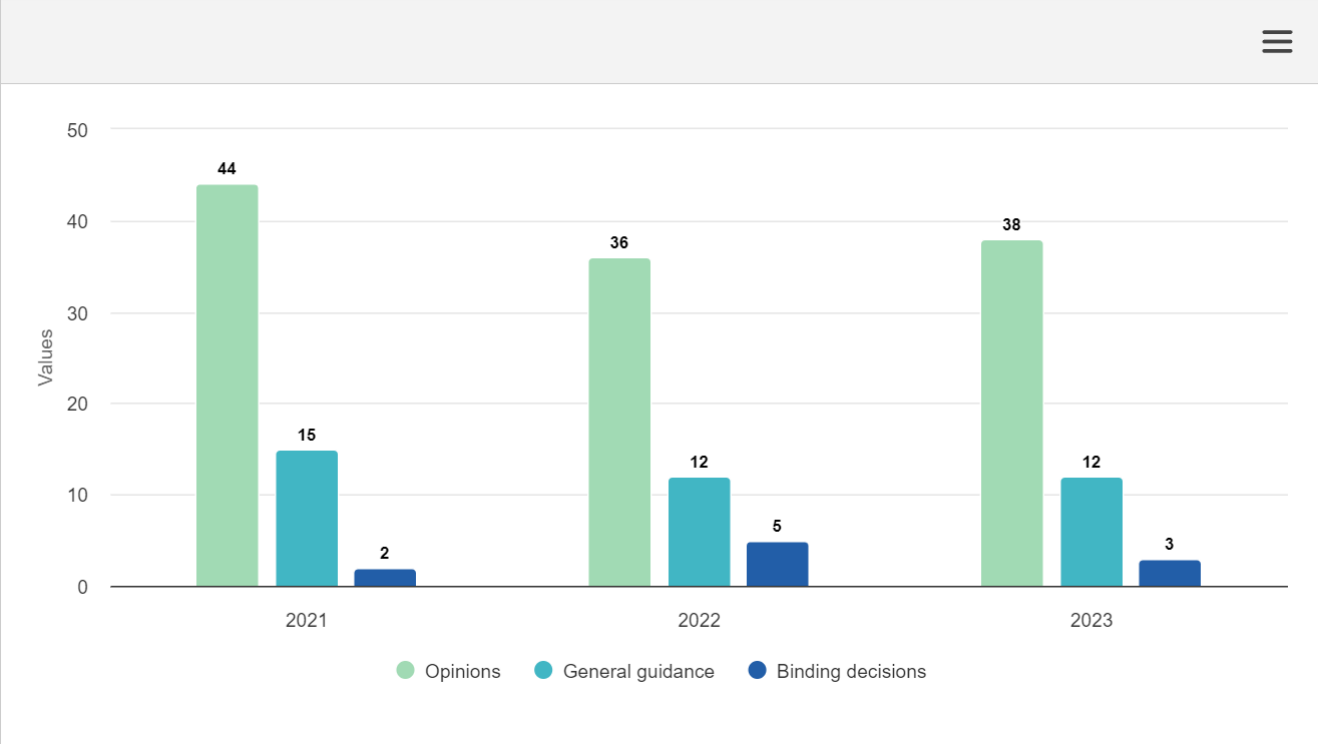
The second aspect of the EDPB that was praised by interviewees is the number of opinions, guidelines and guidance documents it produces (see Figure 1). Several interviewees underlined how useful the guidance is in supporting their work, highlighting some of them in particular. The usefulness of the EDPB's guidelines on the enforcement of sanctions and fines was often mentioned, but also its guidelines on the transfer of data to non-EU countries and those on measures to supplement transfer tools to ensure compliance with the EU's level of protection of personal data. One interviewee also mentioned an example of positive collaboration with the EDPB in a case where they asked for further information on a procedure that lacks detail in the GDPR. Another interviewee highlighted the work conducted within the EDPB subgroup as 'becoming more and more important for day-to-day enforcement issues'. Some interviewees mentioned that they often use, or refer to, EDPB guidelines to inform data controllers. Finally, some interviewees also highlighted the EDPB initiative to create a pool of experts, allowing DPAs to call on experts with specific professional backgrounds to complement their work.

For some interviewees, the EDPB's work in this regard is particularly important, as it supports,

from a more global perspective, the aim of the GDPR to effectively harmonise data protection across the EU, despite Member States' procedural differences. One interviewee said that 'the EDPB guidelines allow [us] to find a common starting point'.

Figure 1 – EDPB documentation published, 2021 to 2023

Number of opinions, general guidance (including guidelines) and binding decisions published by the EDPB, per year.



Sources: EDPB, 'Guidelines, recommendations, best practices', 2024; EDPB, 'Binding decisions', 2024; EDPB, 'Opinions', 2024.

> **The EDPB does a great job of establishing a uniform approach; however, the lack of an EU-level uniform procedural code is still an obstacle that even the EDPB cannot overcome.**
>
> *An EU DPA staff member*

Several interviewees praised the work of the EDPB while noting that the secretariat is

understaffed. One said: ‘The secretariat is generally found to be reliable, neutral and unbiased’. Interviewees said that the secretariat provides DPAs with ‘a very high level of expertise’, and, in short, that ‘the role of the EDPB secretariat is the very heart of the EDPB’.

> **The EDPB secretariat does a great job. It facilitates national data protection authorities in cooperation with tools. It is understaffed, but the people working there are very competent and dedicated.**
>
> *An EU DPA staff member*

> **The EDPB secretariat is key and has so far duly responded to its mission despite its own understaffing problems.**
>
> *An EU DPA staff member*

One interviewee also said that, while ‘the system is not perfect and needs some fine-tuning, the EDPB is proactive in seeking feedback, comments and proposals for improvements’.

However, despite interviewees’ generally positive views on the EDPB, several of them also highlighted that they expect the EDPB to reinforce its role in several aspects. The next section outlines recommendations proposed by some of the interviewees.

4.2. Concerns about the European Data Protection Board

While the majority of respondents generally praised the numerous guidelines produced by the EDPB as a useful tool to support both their work and their awareness-raising activities, some interviewees suggested that these could be improved by enhancing their quality and developing more practical (less theoretical/broad) guidance. One interviewee mentioned that, in their experience, the guidelines are ‘massive’ and ‘unapproachable for audiences without legal training’.

> **Practically, the data controller does not know how to implement what the EDPB recommends.**

An EU DPA staff member

> **The guidelines of the EDPB are there, but there might be small details in cases examined at the national level that differentiate a case from the other and can change the entire picture.**

An EU DPA staff member

> **The EDPB has issued opinions that are interesting and useful to some extent, but, when you see their examples, they are rather easy cases and do not reflect what usually happens in practice.**

An EU DPA staff member

The issue of resources was also raised by several DPA staff members when discussing the EDPB. While the board is praised for the amount of work it produces, several interviewees voiced concerns about the considerable amount of additional work for DPAs that the EDPB's related tasks represent, stating that they invest 'heavily' in the EDPB's work. This was raised not only by interviewees from smaller EU Member States; however, interviewees from smaller Member States expressed regret that their current size is preventing them from participating in all EDPB activities as they are expected to.

> **Due to the lack of resources, the DPA does not get as involved in the cross-border cases and into EDPB work as it could.**
>
> *An EU DPA staff member*

4.3. Looking ahead: the European Data Protection Board's development

Some interviewees highlighted the inner bureaucracy of the board, which affects the speed of its processes, with one mentioning up to '400 meetings' to discuss similar topics. One interviewee believes that 'during the elaboration of the EDPB documents too much attention is paid to some petty issues'.

> **The EDPB could work more to make the processes more effective in their entirety, everything from plenary meetings to more strategic discussions of the large problems facing the EU.**
>
> *An EU DPA staff member*

Some interviewees were more pessimistic about the ability of the EDPB to overcome the inherent complexities of its tasks. One interviewee insisted that the significant differences between DPAs, notably in terms of human resources, cannot be overcome through cooperation within the board.

Some interviewees suggested ways of furthering the positive impact of the board. For several of them, the Internal Market Information System (i.e. the IT platform helping national authorities across the EU to cooperate and exchange information) is not user-friendly enough and should be revised. Some interviewees also emphasised that the case database should be more consistent and could also include statistics/metrics on the DPAs' work. Finally, one interviewee believed that exchanges within the EDPB could be more transparent.

> **The current case database available on the EDPB's website is sporadic and does not necessarily contain all decisions a national DPA may find relevant and important.**

An EU DPA staff member

Annex: Methodology

Article 97 of the general data protection regulation (GDPR) provides that 'by 25 May 2020 and every 4 years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council'. In May 2020, the European Commission published its first review [115] (the 2020 report). For the second evaluation of the GDPR, due to be published in 2024, the European Commission invited FRA to conduct qualitative research, collecting the experiences, challenges and best practices identified by data protection authorities (DPAs) in implementing the GDPR.

Data were collected through interviews with DPA representatives and analysed to complement the data collection performed by the European Commission, and the reports prepared by the European Data Protection Board, the European Parliament and the Council of the European Union.

In cooperation with the European Commission, FRA developed a questionnaire building on the tasks of the DPAs as listed in Article 57 of the GDPR.

The questionnaire covered nine areas:

1. the institutional capacity of DPAs;
2. modern technological challenges;
3. the independence of DPAs;
4. raising public awareness;
5. the investigatory powers of DPAs;
6. sanctioning GDPR violations;
7. cooperation between EU DPAs and the GDPR consistency mechanism;
8. cooperation with other national regulators;
9. the protection of personal data and competing fundamental rights.

The questionnaire allowed for semi-structured interviews. It included 16 open questions, where interviewees were invited to describe any challenges they were confronted with directly in their work or have been informed about. Interviewees were also invited to reflect upon the possible causes of these challenges, the potential consequences for data protection and potential mitigation measures. Mitigation measures included both existing practices (referenced through the report) and measures DPA staff believed could be beneficial, but that were not tested yet.

In 2022, the questionnaire was tested by FRA through interviews in four Member States, with the objective of ensuring its relevance and identifying potential shortcomings. The questionnaire was welcomed by DPAs where it was tested, and, on this basis, FRA contracted Franet [116], its network of experts in the Member States, to conduct interviews in 21 Member States. All Franet interviewers received 1 day's training in December 2022 to harmonise the approach and ensure

the highest quality of interview methodology.

By mid-2023, interviews were conducted with DPAs in all 27 Member States. To gather adequate material covering all nine topics, and for FRA to collect sufficient data, three interviews were conducted per Member State. In two Member States only two interviews were conducted, and in three Member States only one interview was conducted, due to workload or availability of staff. Overall, 70 interviews were conducted.

The aim was to interview staff in different positions to ensure a variety of views and experiences and obtain a comprehensive overview. The aim was to conduct interviews with:

- the head of the DPA (e.g. president, chair);
- the official in charge of national and/or international cooperation work at the DPA;
- the official in charge of processing complaints, investigations, and/or sanctions at the DPA.

Given the differences in the organisational structure and in the experts' profiles among the DPAs, a certain margin of flexibility was granted to the DPAs and to Franet in the selection of the interviewees for profiles 1 and 2.

In addition, it was not possible to interview these exact profiles at all DPAs. In five Member States, the DPAs could participate in only one or two interviews (out of the three interviews mentioned above). The main reason for this was their workload, which prevented staff members from dedicating more time and resources to this research.

In two Member States, one interview was conducted with all three staff members at the same time. In one Member State, interviews were conducted only with staff members and not the head of the DPA, while in another only the head of the DPA participated in the interview. Given that this affected only a small number of Member States, and that at least one or two interviews could be conducted in all Member States, this did not affect the whole data collection and data analysis conducted by FRA.

All interviews were conducted face to face, either by FRA or by Franet, in the language of the Member State. With the consent of the interviewees, interviews were audio-registered, for the purpose of checking the transcript of the interviews. The audio transcripts were deleted at the end of the research. For further information on the data protection principles applied to this research, you may refer to the data protection notice published on FRA's website [117] .

The objective of the interviews was to collect DPAs' experiences, focusing on the challenges they face in implementing the GDPR and on the promising practices they have identified to respond to these challenges.

Due to overlaps in the responses and in the trends identified by FRA, the report does not follow the structure of the questionnaire. The challenges identified by the respondents are presented based on their relevance to DPAs' independence, their supervisory powers, their advisory tasks and their cooperation at the national and EU levels. Furthermore, interviewees did not identify any relevant challenges under the ninth area related to the protection of personal data and competing

fundamental rights.

FRA analysed the fieldwork data, using Maxqda software to support the identification of trends and common challenges. It also compared the data with previous evidence that FRA has collected on the role, effectiveness and independence of DPAs, described in Box B 1, to identify recurrent issues over the years.

In this report, given that up to three interviews were conducted within each Member State, trends were identified based on the number of Member States mentioning a challenge:

- when a challenge was mentioned by only one interviewee in less than three Member States, the report refers to ‘a few respondents’;
- when a challenge was mentioned by several interviewees in less than three Member States, the report refers to ‘some respondents’;
- when a challenge was mentioned by several interviewees in four to seven Member States, the report refers to ‘several respondents’;
- when a challenge was mentioned by several interviewees in 7 to 13 Member States, the report refers to ‘many respondents’;
- when a challenge was mentioned by several interviewees in more than 14 Member States, the report refers to ‘most respondents’ or ‘a majority of respondents’;
- when a challenge was mentioned by several interviewees in 26 or 27 Member States, the report refers to ‘a very large majority of respondents’.

Interviews were conducted anonymously to obtain the most trustworthy insights into experiences, as this allowed interviewees to speak more freely. Quotes and promising practices were sent out to each interviewee to ensure the anonymity of the former and the accuracy of the latter. Where available and useful, interviewees provided FRA with public sources of information, which were integrated in the report as official references. On a few occasions, the DPA did not, and could not, provide FRA with further references, and the source of the practice was identified as stemming from the interviews FRA conducted with one or several DPAs.

Abbreviations

- **AI** – artificial intelligence
- **CJEU** – Court of Justice of the European Union
- **DPA** – data protection authority
- **DPIA** – data protection impact assessment
- **DPO** – data protection officer
- **EDPB** – European Data Protection Board
- **EDPS** – European Data Protection Supervisor
- **FRA** – European Union Agency for Fundamental Rights
- **GDPR** – general data protection regulation
- **IAPP** – International Association of Privacy Professionals
- **ICT** – information and communications technology
- **IT** – information technology

Endnotes

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general data protection regulation) (OJ L 119, 4.5.2016, p. 1).

[2] See FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010.

[3] FRA, Access to data protection remedies in EU Member States,Publications Office of the European Union, Luxembourg, 2014.

[4] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final).

[5] The legal standards are described in detail inFRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018, Chapter 5.

[6] An overview of the national fines can be found using the GDPR Enforcement Tracker. In addition, the GDPR hub of the civil society organisation 'NOYB' regularly publishes a summary of the most relevant DPA decisions: see GDPRtoday.

[7] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final).
() The legal standards are described in detail in FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018, Chapter 5. See also FRA, Fundamental Rights Report –2021, Publications Office of the European Union, Luxembourg, 2021, Chapter 7.

[8] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final), p. 5.

[9] See FRA, The General Data Protection Regulation – One year on – Civil society: Awareness, opportunities and challenges, Publications Office of the European Union, Luxembourg, 2020.

[10] EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97 , Brussels, 2023, pp. 15 and 31; EDPB, Overview on resources made available by Member States to the data protection supervisory authorities,2022, p. 5; EDPB, Overview on resources made available by Member States to the data protection authorities and on enforcement actions by the data protection authorities, 2021. See also Commission staff working document accompanying Commission communication – Data protection rules as a pillar of citizens empowerment and the EU's approach to digital transition – Two years of application of the General data protection regulation (SWD(2020) 115 final), Chapter 2.4; Council of Europe, Report on the Funding of Data Protection Authorities, Strasbourg, 2021.

[11] EU, Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, p. 391), Art. 8(3).

[12] EU, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ C 326, 26.12.2012, p. 1), Art. 16(2).

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31), Art. 28(1).

[14] GDPR, Art. 52.

[15] See CJEU, C-210/16, Wirtschaftsakademie, 5 June 2018; CJEU, C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015; CJEU, C-288/12, European Commission v Hungary, 8 April 2014; CJEU, C-614/10, European Commission v Republic of Austria, 16 October 2012; CJEU, C-518/07, European Commission v Germany, 9 March 2010. For more information, see FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018.

[16] Art. 52(2), (3), (4), (5) and (6) of the GDPR provide for conditions that are necessary for DPAs' independence. Art. 53 governs the appointment of DPA members.

[17] For an analysis of Art. 52 of the GDPR, see FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018, Chapter 5.1.

[18] FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010; FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018, Chapter 5; FRA, Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, Vienna, 2012, Section 4.2.1.

[19] FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010; FRA, Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, Vienna, 2012, Chapter 4.1.1.

[20] FRA,Access to data protection remedies in EU Member States, 2014, Chapter 4.2.

[21] FRA, Access to data protection remedies in EU Member States, 2014, p. 46.

[22] FRA, Access to data protection remedies in EU Member States, 2014, pp. 47–49.

[23] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final), p. 6.

[24] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final), p. 6.

[25] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final)

[26] EDPB, Overview on resources made available by Member States to the data protection supervisory authorities,2022, p. 5; EDPB, Overview on resources made available by Member States to the data protection authorities and on enforcement actions by the data protection authorities, 2021. See also Commission staff working document accompanying Commission communication – Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – Two years of application of the general data protection regulation

(SWD(2020) 115 final), Chapter 2.4; Council of Europe, Report on the Funding of Data Protection Authorities, Strasbourg, 2021.

[27] According to EDPB data and analysis from 2023 included in the EDPB's contribution to the European Commission's report on the application of the GDPR, three DPAs considered that their human, financial and technical resources were sufficient, four DPAs stated that they had sufficient financial and technical resources but insufficient human resources; two DPAs reported that their human and financial resources were adequate; and three DPAs indicated sufficient technical resources. In one Member State, the budget was reduced. See EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97,2023, p. 33.

[28] EDPB (2023), Contribution of the EDPB to the report on the application of the GDPR under Article 97, 2023, p. 33.

[29] EDPB (2023), Contribution of the EDPB to the report on the application of the GDPR under Article 97,2023, Section 4.4.

[30] FRA, Fundamental Rights Report – 2020,Publications Office of the European Union, Luxembourg, 2020, Chapter 6.3.2; FRA, Fundamental Rights Report – 2021, Publications Office of the European Union, Luxembourg, 2021, Chapter 7.1.

[31] GDPR, Art. 57(f) tasks DPAs to handle complaints within a reasonable time; Art. 77 guarantees the data subject's right to lodge a complaint with a DPA and to receive information on the progress and outcome of the claim from the DPA.

[32] GDPR, Art. 57(1)(f), establishes that DPAs should handle complaints within a reasonable time; Art. 77 guarantees the data subject's right to lodge a complaint a DPA and to receive information on the progress and outcome of the claim from the DPA; Art. 78(2) prescribes the right to an effective remedy when a DPA does not handle a complaint or does not inform a data subject within 3 months.

[33] For an overview of the IT systems, see FRA, Handbook on European law relating to asylum, borders and immigration, Publications Office of the European Union, Luxembourg, 2020, Chapter 2.

[34] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

[35] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, Article 1).

[36] According to Article 49(2) of the Digital Services Act, Member States may assign specific tasks to other competent authorities, in addition to the appointed Digital Service Coordinator, who remains responsible for ensuring the supervision of providers of intermediary services. See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1). For example, in Italy the national law explicitly envisages a cooperation between the Digital Service Coordinator (the Authority for Communications) and the DPA; See Article 15 of Law-Decree No. 123/2023 of 16 September 2023 on digital security of children. In the Netherlands and in France, it is proposed that the DPA, together with other authorities, will be the competent authority responsible for the supervision of providers of intermediary services and the enforcement of the DSA. For the Netherlands, see Article

3.1. of Proposal of Law 36531-2, proposed on 2 April 2024. For France, see Article 25 of the project of law number 175 of 17 October 2023.

[37] Commission proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final).

[38] Artificial Intelligence Act, Article 5(5).

[39] Artificial Intelligence Act, Article 53(2).

[40] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council, (OJ L, 2024/1358, 22.5.2024).

[41] Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817, (OJ L, 2024/1356, 22.5.2024).

[42] EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97, 2023, p. 33.

[43] EDPB,Contribution of the EDPB to the report on the application of the GDPR under Article 97, 2023, pp. 15 and 31; EDPB, Overview on resources made available by Member States to the data protection authorities and on enforcement actions by the data protection authorities,2022, p. 5; EDPB, Overview on resources made available by Member States to the data protection supervisory authorities, 2021. See also Commission staff working document accompanying Commission communication – Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – Two years of application of the general data protection regulation (SWD(2020) 115 final), Chapter 2.4; Council of Europe, Report on the Funding of Data Protection Authorities, Strasbourg, 2021.

[44] Art. 57 of the GDPR outlines DPAs' tasks, such as monitoring and enforcing the application of the GDPR, promoting public awareness, providing advice to the national parliament and the government, and dealing with complaints lodged by data subjects. Art. 58 lays down the investigative, supervisory, authorisation and advisory powers of DPAs.

[45] GDPR, Art. 52(4).

[46] GDPR, Art. 52(5).

[47] CJEU, C-614/10, European Commission v Republic of Austria, 16 October 2012, paragraph 41.

[48] FRA, Access to data protection remedies in EU Member States, Publications Office of the European Union, Luxembourg, 2014, p. 9; FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II,Publications Office of the European Union, Luxembourg, 2010, Chapter 4.1.1.

[49] See EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97 , 2023, p. 33;EDPB, Overview on resources made available by Member States to the data protection supervisory authorities ,

2022, p. 5; EDPB, Overview on resources made available by Member States to the data protection authorities and on enforcement actions by the data protection authorities, 2021.

[50] For further details on complaints handling under the GDPR, see Art. 57(1)(f), Art. 77 and Art. 78(2).

[51] FRA,Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010;FRA, Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package, 2012.

[52] FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II, Publications Office of the European Union, Luxembourg, 2010, p. 42.

[53] FRA, Data Protection in the European Union: The role of national data protection authorities, FRA opinion on GDPR, Vienna, 2010, p. 42.

[54] FRA, Strong and Effective National Human Rights Institutions – Challenges, promising practices and opportunities, Publications Office of the European Union, Luxembourg, 2020; FRA, National human rights institutions in the EU Member States – Strengthening the fundamental rights architecture in the EU I, Publications Office of the European Union, Luxembourg, 2010; FRA, Surveillance by Intelligence Services – Volume I: Member States' legal frameworks, Publications Office of the European Union, Luxembourg, 2015; FRA, Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update, Publications Office of the European Union, Luxembourg, 2017; FRA, Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – 2023 update, Publications Office of the European Union, Luxembourg, 2023.

[55] GDPR, Art. 52; GDPR, recitals 117, 118 and 121.

[56] FRA, Council of Europe and EDPS, Handbook on European Data Protection Law – 2018 edition, Publications Office of the European Union, Luxembourg, 2018, Chapter 5.1; CJEU, C-518/07, European Commission v Federal Republic of Germany (Grand Chamber), 9 March 2010, para. 27; CJEU, C-614/10, European Commission v Republic of Austria (Grand Chamber), 16 October 2012, paras 59 and 63.

[57] GDPR, Art. 52(6).

[58] GDPR, Art. 69.

[59] FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the fundamental rights architecture in the EU II,Publications Office of the European Union, Luxembourg, 2010.

[60] FRA, Coronavirus Pandemic in the EU – Fundamental rights implications: With a focus on contact-tracing apps, Bulletin 2, Publications Office of the European Union, Luxembourg, 2020.

[61] GDPR, Art. 52(2).

[62] GDPR, Art. 52(3).

[63] GDPR, Art. 53(1).

[64] FRA, Data Protection in the European Union: The role of national data protection authorities – Strengthening the

fundamental rights architecture in the EU II,Publications Office of the European Union, Luxembourg, 2010, Chapter 4.1.1.

[65] EDPB, Minutes of the 43rd plenary meeting, 15 December 2020, Section 4.1.3. See also EDPB, 'EDPB moves ahead with closer cooperation on strategic cases', press release, 2022; and EDPB, 'Swift adoption of regulation to streamline cross-border enforcement needed', press release, 2023.

[66] EDPB, Statement on enforcement cooperation, 28 April 2022.

[67] EDPB,Letter to Commissioner Reynders, 10 October 2022.

[68] Commission proposal for a regulation laying down additional procedural rules relating to the enforcement of GDPR (COM(2023) 348 final).

[69] EDPB and EDPS, Joint Opinion 01/2023 on the proposal for a regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, 2023.

[70] For more information, see the steps of the ordinary legislative procedure for Procedure 2023/0202/COD on EUR-Lex.

[71] EDPB, Minutes of the 43rd plenary meeting, Section 4.1.3, 15 December 2020. See also EDPB, 'EDPB moves ahead with closer cooperation on strategic cases', press release, 2022; and EDPB, 'Swift adoption of regulation to streamline cross-border enforcement needed', press release, 2023.

[72] Commission proposal for a regulation laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 (COM(2023) 348 final).

[73] CJEU, 'A parliamentary committee of inquiry must in principle comply with the general data protection regulation', press release, Luxembourg, 2024.

[74] EDPB, Annual Report 2021, 2022, p. 66; EDPB, Annual Report 2020, 2021, pp. 55 and 68; and EPDB, Annual Report 2019, 2020, pp. 29 and 31.

[75] EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97 , 2023.

[76] EDPB, Statement on enforcement cooperation, 28 April 2022.

[77] EDPB, Contribution of the EDPB to the report on the application of the GDPR under Article 97 , 2023, p. 47.

[78] GDPR, Art. 57(1)(b).

[79] GDPR, Art. 57(1)(c).

[80] GDPR, Art. 36(2) and Art. 57(1)(l).

[81] While some Member States established a DPA in the 1970s, others did so only after the adoption of Directive 95/46/EC.

[82] GDPR, Art. 57.

[83] GDPR, Art. 36, provides that 'Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller'.

[84] EDPS, A preliminary opinion on data protection and scientific research, 2020, p. 16. See also European Parliamentary Research Service,How the general data protection regulation changes the rules for scientific research, PE 634.447, 2019.

[85] GDPR, Art. 89 and Art. 5(1)(b).

[86] GDPR, Article 89, provides for safeguards and derogations in relation to processing data for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.

[87] EDBP, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, 2019.

[88] Directive 2004/23/ECof the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells (OJ L 102, 7.4.2004, p. 48).

[89] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use (OJ L 158, 27.5.2014, p. 1); European Commission, 'Question and answers on the interplay between the clinical trials regulation and the general data protection regulation', 2014; EDPB, Opinion 3/2019 concerning the questions and answers on the interplay between the clinical trials regulation (CTR) and the general data protection regulation (GDPR), 2019.

[90] Several pieces of EU legislation govern statistics depending on the subject area. See 'EU legislation on statistics'.

[91] For an overview of sectorial legislation adopted at the national level to regulate the use and collection of personal data for research purposes and its interplay with the GDPR, see Milieu, Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research, 2021. The study was commissioned by the EDPB.

[92] EDPB, Opinion 3/2019 concerning the questions and answers on the interplay between the clinical trials regulation (CTR) and the general data protection regulation (GDPR), 2019.

[93] See also European Commission, Directorate-General for Health and Food Safety, Assessment of the EU Member States' rules on health data in the light of GDPR, Publications Office of the European Union, Luxembourg, 2021.

[94] FRA, Bias in Algorithms – Artificial intelligence and discrimination, Publications Office of the European Union, Luxembourg, 2020, p. 15.

[95] GDPR, Article 85(2), provides for exemptions and derogations from some GDPR chapters, when processing of personal data is conducted for journalistic purposes or the purpose of academic artistic or literary expression. Article 85(3) obliges Member States to adopt laws based on Article 85(2).

[96] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281,

23.11.1995, p. 31).

[97] IAPP is a large association that brings together professionals and experts on privacy and data protection. It is a non-profit organisation working to develop and foster understanding related to privacy and data protection.

[98] IAPP, 'Study: An estimated 500K organizations have registered DPOs across Europe',16 May 2019.

[99] Council of the European Union, Council position and findings on the application of the GDPR – Consultation of Member States, Brussels, 8 November 2023, para. 18.

[100] GDPR, Art. 5(1)(d).

[101] GDPR, Art. 16.

[102] GDPR, Art. 17.

[103] FRA, Getting the Future Right – Artificial intelligence and fundamental rights, Publications Office of the European Union, Luxembourg, 2020.

[104] Commission proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final).

[105] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

[106] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 14.9.2022, p. 1).

[107] Commission proposal for a regulation on harmonised rules on fair access to and use of data (Data Act) (COM(2022) 68 final). See also European Parliament, 'Parliament backs plans for better access to, and use of, data', press release, 2023; European Council, 'Data Act: Council adopts new law on fair access to and use of data', press release, 2023.

[108] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

[109] See European Commission, 'Interoperability', for a list of acts related to interoperability, namely Regulation (EU) 2019/818, Regulation (EU) 2019/817, Delegated Regulation (EU) 2021/2103, Implementing Regulation (EU) 2021/2224 and Delegated Regulation (EU) 2021/2222.

[110] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1), as amended on 24 September 2023.

[111] EDPB and EDPS, Joint Opinion 03/2022 on the proposal for a regulation on the European Health Data Space, 2022, p. 4.

[112] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to

the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final).

[113] EDPB, Statement on enforcement cooperation, 28 April 2022.

[114] EDPB, Annual Report 2019, 2020, which includes details of the 2023-2024 work programme; and EDPB plenary minutes.

[115] Commission communication – Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the general data protection regulation (COM(2020) 264 final).

[116] For more information, see the Franet website.

[117] FRA, 'Research project on "GDPR – The experience of data protection authorities"', data protection notice, 2022.