FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

THE LAW ENFORCEMENT DIRECTIVE

DATA PROTECTION CHALLENGES IN PRACTICE

REPORT



Contents

Key findings and opinions 4

Ensuring a better understanding of, and compliance with, the Law Enforcement Directive within competent authorities 4

FRA opinion 1 6

FRA opinion 2 6

FRA opinion 3 6

FRA opinion 4 7

Reinforcing the role of data protection officers under the Law Enforcement Directive 7

FRA opinion 5 8

FRA opinion 6 9

FRA opinion 7 9

Reinforcing national data protection authorities' resources and means to fulfil their mandate regarding the Law Enforcement Directive 9

FRA opinion 8 10

FRA opinion 9 11

FRA opinion 10 11

Introduction 12

1. Applying data protection principles: insights from police and judicial authorities 17

1.1. Competent authorities' understanding of the core principles of the Law Enforcement Directive 18

1.1.1. Lawfulness of processing of personal data for law enforcement purposes 19

Distinction between the General Data Protection Regulation and the Law Enforcement Directive 20

Conditions applying to international transfers of personal data 21

1.1.2. Operational data protection requirements: purpose limitation and data minimisation 23

Purpose limitation 25

Data minimisation 25

Issues raised in relation to both principles 27

Guidance and data protection officers' role in supporting the implementation of both principles 28

1.1.3. Data security and technical safeguards 29

1.1.4. Data accuracy and data protection in general as safeguards of investigations' effectiveness 32

Accuracy of personal data 32

Personal data based on facts versus personal assessments 33

1.2. Ensuring data security and providing accountability 35

1.2.1. Protecting data security and handling data breaches 36

1.2.2. Handling data subjects' requests 39

1.2.3. Competent authorities investigated by the data protection authority 44

1.3. Seeking advice and cooperation 48

1.3.1. Seeking and receiving advice 49

1.3.2. Cooperation among competent authorities 52

2. Providing expertise: the key role of data protection officers 54

2.1. Resources 56

2.2. Training and expertise 61

2.3. Data protection officers' relationships and recognition within the organisation 64

3. Supervising the Law Enforcement Directive: the views and experiences of data protection authorities 68

3.1. Enforcing the Law Enforcement Directive: data protection authorities' dedicated resources and expertise 69

3.2. Investigating competent authorities 72

3.2.1. Resources and investigatory powers 72

Challenges related to the use of artificial intelligence and modern technologies 72

Challenges related to accessing data during investigations 73

Challenges related to data protection authorities' expertise in cases related to the Law Enforcement Directive 74

3.2.2. Data protection authorities' cooperation with competent authorities and data protection officers 74

3.2.3. Enforcement and corrective powers 76

Conclusion 79

Annex 1: Methodology 81

Endnotes 85

About this publication 88

Key findings and opinions

Criminal investigations involve the large-scale processing of highly sensitive personal data, such as witness statements, biometric information and digital evidence. Effectively using such data for law enforcement purposes without violating the rights of people is notably regulated through EU data protection law. While the need for establishing a comprehensive evidence base for law enforcement is clear, any processing of personal data of natural persons in this context has to comply with the right to the protection of personal data.

The Law Enforcement Directive (LED) [1] establishes rules for processing personal data by competent authorities in order to protect fundamental rights and freedoms, in particular the protection of personal data. Competent authorities include any public body that is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including in relation to threats to public security. Competent authorities include, in particular, law enforcement authorities, prosecutor's offices and judicial authorities (e.g. courts).

This report examines how competent authorities apply data protection in practice, focusing on the implementation of the LED.

Although closely related to the General Data Protection Regulation (GDPR) [2], the LED is less well known. As a directive, the LED sets minimum standards but allows EU Member States to have flexibility in terms of its implementation, leading to differences across national systems.

Drawing on 132 interviews across all Member States, this report provides practical insights into how law enforcement and judicial authorities apply the LED. The interviews cover both operational officers and data protection officers (DPOs) working in law enforcement, as well as judicial authorities (i.e. prosecutors and investigating judges). Interviews were also conducted with national supervisory authorities (i.e. the national data protection authorities (DPAs) that are in charge of monitoring the application of the LED). The results contribute to an EU-level assessment of how the LED is applied and to providing suggestions for future improvements for the practical implementation of the LED.

Ensuring a better understanding of, and compliance with, the Law Enforcement Directive within competent authorities

Article 4 of the LED establishes the principles for the legal framework applicable to competent authorities when processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences. These include the principles of data minimisation, purpose limitation and data security. The first two, although closely linked, relate to different concepts and have different objectives: purpose limitation means that personal data must be

collected for specified, explicit and legitimate purposes and that its processing must remain tied to those specified purposes, while data minimisation signifies that, for a given purpose, only data that are adequate, relevant and not excessive should be collected and used. Data security involves the implementation of technical and organisational measures to ensure the confidentiality and integrity of personal data. In addition, the LED requires that Member States verify the appropriateness of data storage, either by specifying time limits in their national legislation or by conducting regular inspections.

Most interviewees working in competent authorities, including police and judicial authorities, are aware of these concepts and, from the perspective of the DPOs interviewed by the European Union Agency for Fundamental Rights (FRA), these concepts represent a positive evolution towards data protection within these authorities. However, the interviews also show that the data protection principles set out in the LED are not always fully understood by staff working within competent authorities. Data minimisation and purpose limitation are often confused and are not seen as separate principles. Data security measures are seen as a means to ensure both data minimisation and purpose limitation. While data security measures may indeed support the authorities' obligations to collect (and store) the necessary data for a specified purpose, the practical means of implementing data security measures need to be clarified.

In addition, some shortcomings were identified when it comes to knowledge of the applicable legal framework regulating data storage. Several interviewees among operational staff in competent authorities were unaware of the applicable rules concerning time limits and regular inspections.

Interviews with staff working in competent authorities show, in some cases, an over-reliance on data management information technology (IT) systems used by competent authorities to ensure data protection requirements (including features such as the automatic deletion of data, obligated motivation fields or loggings). However, very few DPOs working at competent authorities referred to regular inspections or audits of the data management system to ensure that data protection principles were appropriately secured in practice.

The interviews with staff working in competent authorities also point to structural challenges regarding the accuracy of personal data (Article 4(1)(d) of the LED). When asked about measures to ensure the accuracy of data, several of these interviewees were unable to describe specific safeguards, and some explicitly stated that there was no continuous or proactive monitoring in place to ensure data quality. While data may be updated in the course of day-to-day operational work, regular checks were described as not feasible. In some cases, the same data are stored separately in different databases, meaning that updates made in one system do not automatically apply to others, potentially resulting in outdated or duplicate records. A few of these interviewees noted that police and judicial authorities use separate, non-interoperable systems. In addition, some representatives from the judiciary indicated that their role in ensuring data accuracy is limited, as they rely on information collected during pretrial investigations by other actors, notably the police.

Finally, in relation to international data transfers, interviewees pointed out that some uncertainties

remain. Specifically, the lack of adequacy decisions adopted with non-EU countries creates both legal and technical difficulties for competent authorities transferring data to non-EU countries, as the assessment of what would constitute 'appropriate safeguards with regard to the protection of personal data' is difficult and requires competent authorities to invest time and human resources. From a practical perspective, some interviewees also mentioned a lack of legal clarity when it comes to accessing specific foreign-based data, either because of these data being saved in clouds or because the types of data (e.g. genetic data) are regulated differently across the EU.

As demonstrated by a few promising practices identified in this report, any concrete measures aimed at reinforcing the implementation of data protection principles largely depend on evidence-based analysis of the situation within each Member State. National evaluations of data protection awareness within law enforcement and judicial authorities allow evidence-based initiatives to be undertaken to reinforce the application of the LED in practice.

FRA opinion 1

Member States should consider undertaking a systematic assessment of the level of awareness and understanding of the applicable national data protection framework for law enforcement purposes among those responsible for applying it. The objective of such an assessment would be to propose evidence-based measures for tackling a lack of awareness or understanding of the legal requirements stemming from this legal framework. Such an assessment should describe how competent authorities handle personal data, in particular sensitive categories, and whether they respect core principles of data protection law.

FRA opinion 2

Member States and relevant EU agencies (e.g. the European Union Agency for Law Enforcement Training (CEPOL), the European Union Agency for Criminal Justice Cooperation (Eurojust) or the European Union Agency for Law Enforcement Cooperation (Europol)) should develop further guidance and training that clearly explains the objectives of each data protection principle in the context of law enforcement work and the measures that should be consistently implemented to ensure the practical implementation of these principles. Such guidance and training should be specific to the LED, adapted to the work of the competent authority and tailored to each professional group (criminal investigators, cybercrime experts, IT professionals, etc.) that, within the authority, may process personal data.

FRA opinion 3

Member States should regularly evaluate whether their technical and organisational measures

(e.g. the automatic deletion of data, obligated motivation fields and loggings **to handle data subjects**) that have been put in place to comply with some of the LED requirements (notably data minimisation, purpose limitation, data accuracy, data erasure and data storage) are sufficient and effective.

FRA opinion 4

The European Commission and the European Data Protection Board (EDPB) should provide further guidance on the rules applicable to international data transfers to non-EU countries when no adequacy decisions have been adopted. The guidance should explain the criteria based on which competent authorities should evaluate appropriate safeguards. In addition, EU institutions and Member States should take measures to identify specific challenges faced by competent authorities when it comes to cross-border access to personal data (e.g. evidence stored in clouds based in non-EU countries or access to DNA databases), to develop targeted, clear and practical guidelines for competent authorities.

Reinforcing the role of data protection officers under the Law Enforcement Directive

Article 32 of the LED requires controllers to designate a DPO, although Member States may exempt courts and other independent judicial authorities from this obligation when acting in their judicial capacity. Article 33 introduces a broad mandate for the DPO, requiring their involvement 'in all issues which relate to the protection of personal data'.

Despite the gaps in knowledge reported earlier, most of the DPOs interviewed have observed improvements in staff awareness of data protection requirements. At the same time, many DPOs stated that fulfilling their role remains challenging for several reasons.

First, a lack of resources is a recurring concern. Most of the interviewees among the DPOs reported facing a heavy workload, and many indicated that they have no or only very small teams and support. More than half of the DPOs interviewed reported that they cannot focus exclusively on tasks related to data protection and are required to perform additional duties, such as tasks that they used to perform in their previous law enforcement position before being appointed as a DPO. In addition, the large volume of requests related to the Schengen information system was mentioned during several interviews. Several interviewees indicated that both their teams and other staff within their organisations lack sufficient technical expertise. This includes expertise on the way data are processed and the use of AI systems. The absence of dedicated IT specialists constrains DPOs' ability to engage meaningfully with technologically complex processing operations. Overall, many DPOs described being largely dissatisfied or only moderately satisfied with their working conditions, noting that resource constraints confine their role to day-to-day operational tasks rather than enabling proactive or in-depth work.

Second, interviewees from competent authorities pointed to gaps in training and guidance, despite the clear requirement in Article 33 of the LED that controllers should support the DPO by maintaining their expert knowledge. Most DPOs indicated that they were already employed within the authority before being appointed to the DPO function, and many of them had not received specific training on the LED. Available training opportunities, including external training courses and conferences, were described as predominantly focused on the GDPR and insufficiently tailored to the specificities of data processing by law enforcement or judicial authorities.

While data protection impact assessments (DPIAs) were generally considered useful, for instance for early risk detection, DPOs reported experiencing a lack of concrete guidance in conducting them. Several interviewees explained that they largely develop DPIA templates on their own and would welcome more detailed and case-specific guidance at the EU or national level.In this area, the lack of IT expertise was again highlighted as a compounding factor that can sometimes prevent DPOs from developing exhaustive, detailed DPIAs.

Finally, the DPOs interviewed described challenges related to the organisational positioning of DPOs, despite Article 33 of the LED, which requires Member States to support controllers in ensuring that 'the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. DPOs who are not positioned at the managerial level reported experiencing resistance from colleagues when recalling applicable data protection procedures. Some of the DPOs interviewed indicated that they do not always receive the information necessary to adequately review and assess impact assessments. Several DPOs reported being asked to perform tasks that fell outside their mandate, such as providing general legal advice (beyond Article 34 of the LED, which requires DPOs to advise controllers on the correct implementation of the LED's requirements). Others explained that, in order to foster goodwill and cooperation, they often adopt a service-oriented approach, accompanying operational staff rather than exercising a control function. Several DPOs reported that operational staff sometimes expect them to carry out assessments or take decisions on their behalf. The DPOs interviewed by FRA highlighted instances of role confusion, in which advisory input is perceived as instruction and operational responsibilities are informally shifted to the DPO.

Experts working in DPAs emphasised the importance of DPOs' independence. In this regard, several DPOs working in competent authorities highlighted that both their independence and the recognition and effectiveness of their mandate are strongly related to their position in the organigram of the authority and are reinforced when they are not in a subordinate position.

FRA opinion 5

Member States should make sure that each competent authority has a data protection office with sufficient staff and expertise to enable them to carry out their tasks effectively, as required by Articles 32 and 33 of the LED. To give practical effect to this obligation, Member States should ensure that each competent authority has access to an adequately staffed data protection function covering both technological and legal expertise. This includes allocating adequate time

for in-depth and proactive assessments and for providing targeted guidance to operational staff.

FRA opinion 6

The European Commission, in cooperation with Member States and the EDPB, should support the development of further guidance aimed at DPOs working within the scope of the LED to ensure the consistent application of the directive. This could include a train-the-trainer approach to strengthen DPO expertise, clearer guidance on when a DPIA is required and consideration of a DPIA template tailored to law enforcement processing, taking into account the specific features of the LED framework and common high-risk processing activities, with a view to enhancing efficiency and reducing fragmentation.

FRA opinion 7

Member States should ensure that the organisational positioning of DPOs safeguards their independence and provides access to the necessary expertise within the authority. As required in Articles 32 to 34 of the LED, the scope of the DPO's role should be clearly defined in order to enhance the awareness about their exact tasks and responsibilities among the authority's staff, ensuring that advisory functions are not conflated with operational decision-making or general legal, IT or cybersecurity tasks beyond the DPO's mandate.

Reinforcing national data protection authorities' resources and means to fulfil their mandate regarding the Law Enforcement Directive

Under the LED, DPAs are tasked with investigating compliance, handling and making decisions on complaints from individuals and promoting public awareness of data protection rights. They have the power to access premises, systems and information to conduct their inspections and investigations effectively. DPAs also have corrective powers: they can issue warnings, reprimands and binding orders to bring processing operations into compliance, including ordering the rectification, erasure or restriction of unlawful data processing. They also advise national institutions on legislative and administrative measures, cooperate with other EU supervisory authorities and the EDPB, where relevant, and have the authority to engage in legal proceedings to ensure the effective enforcement of the national provisions transposing the LED.

In practice, as the findings confirm, most DPAs suffer from a shortage of staff, time and expertise when it comes to overseeing the application of national provisions transposing the LED. The lack of resources affecting DPAs with respect to GDPR-related tasks was highlighted by FRA as a recurring problem in previous reports in 2014, 2019 and 2024. Several interviewees working in DPAs highlighted that, as a result of this resource shortage, their DPA prioritises the GDPR over

the LED and concentrates resources on the most pressing (and mandatory) part of their work: addressing complaints. Although the volume of LED-related complaints to the supervisory authorities may not be high, the range of tasks described earlier is broad. The interviews with DPAs also show that the lack of resources has direct and concrete implications for a number of tasks that are not, or not often enough, conducted by DPAs. The main impact lies in the inability of some DPAs to conduct more regular audits and monitoring on their own initiatives. Several DPAs also struggle to develop expertise on technologies that may be used by competent authorities and expertise on preparing for new regulations that intersect with the scope the LED, such as the AI Act [3].

The interviews with DPAs show that the overall scope of and importance given to tasks performed by competent authorities that may have LED-related implications clearly indicate a need for increased (and specialised) human resources in DPAs across Member States, to support them in supervising these authorities more frequently and more effectively. In addition, DPAs in which a sector or unit was created to deal exclusively with LED-related cases have declared that they are under less resource pressure than other DPAs.

Finally, while some respondents from DPAs emphasised that the investigations benefited from good cooperation with competent authorities, several of them identified what they considered to be a serious lack of expertise and understanding of LED requirements within law enforcement and judicial authorities. When it comes to cooperation during investigations or inspections, while most interviewees indicated that they did not face any issue in accessing documents, even when these were classified, some interviewees reported that, in some cases, police authorities have been reluctant to hand over documents. Interviewees working in DPAs with no or limited access to classified information indicated that this does prevent them from effectively investigating competent authorities. In addition, some interviewees working in law enforcement authorities indicated that they believe that the DPA has no authority to investigate them. Finally, a challenging point raised by some interviewees concerns the fact that supervisory and competent authorities do not always agree on what constitutes 'necessary information' for the purpose of an investigation, in the sense of Article 47(1) of the LED, which requires that DPAs should have the power to 'obtain from the controller … all information necessary for the performance of its tasks'.

FRA opinion 8

Member States should provide national DPAs with sufficient resources to ensure that DPAs have sufficient human, financial and technical resources to fulfil each of their tasks as provided by the LED. This includes conducting ad hoc inspections, providing advice and ensuring in-house expert knowledge and understanding. The European Commission should ensure that its periodical report on the implementation of the LED covers the appropriateness of resources allocated to DPAs. Expert knowledge of DPAs should cover potential data protection interferences stemming from the use of AI systems or other advanced technologies, as well as the intersection between data protection legislation and other legislation, such as the AI Act. Where it is not the case, national

DPAs should consider creating separate, dedicated units for dealing exclusively with matters of data protection falling under the scope of the LED.

FRA opinion 9

Member States and EU institutions should develop specific guidelines clarifying the processes under which DPAs' inspections and investigations should be conducted under the LED, to ensure access to effective remedies. Guidance should, in particular, clarify what 'necessary information' means and should provide practical explanations of cases in which the exemptions to data subjects' rights may be applied. Guidelines should provide DPAs with clear and practical examples that support them in their assessment.

FRA opinion 10

Member States should consider implementing rules and safeguards to ensure the mandatory and efficient cooperation of competent authorities during DPAs' inspections and investigations, while safeguarding the effectiveness of criminal investigations. In Member States where DPAs do not have access to classified information, Member States should consider providing DPAs with such investigatory power.

Introduction

Crime prevention and criminal investigations generate vast amounts of personal data, from victims' statements and witness information to biometric identifiers and digital traces. These can include some of the most sensitive personal data and are routinely processed by law enforcement and judicial authorities. According to the European Commission, 85 % of criminal investigations rely on electronic evidence, coupled with a significant increase of requests for data from service providers (covering both internet and over-the-top service providers) in the past years [4]. Ensuring that such data are used effectively to combat crime while safeguarding fundamental rights is a central, yet challenging, concern of EU data protection law.

This report provides insights into the experiences, practices and challenges of law enforcement and supervisory authorities when implementing data protection law, based on the EU Law Enforcement Directive (LED) [5].

The LED governs the processing of personal data for law enforcement purposes. More precisely, Article 1 of the LED imposes rules and principles to ensure 'the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. Competent authorities include both law enforcement and judicial authorities and are defined in Article 3 of the LED as 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. Supervisory authorities refer to the national data protection authorities (DPAs) in charge of monitoring the application of the LED at the national level.

The LED is considered a *lex specialis* of the General Data Protection Regulation (GDPR) [6]. It is less well known than the GDPR and has been under-researched since its entry into force in May 2016 and has not benefited from much guidance [7]. Although deemed to be as complex as the GDPR, DPAs and, at the EU level, the European Data Protection Board (EDPB) have developed very few guidelines to support data controllers in correctly applying its principles,as interviews highlighted. The findings of the European Union Agency for Fundamental Rights (FRA) provide unique insights into the practices and challenges of both competent authorities and supervisory authorities, supporting informed decision-making for EU and national institutions.

Several significant judgments of the Court of Justice of the European Union (CJEU), however, were delivered during and after FRA's fieldwork. While their implications are not yet be fully reflected in the practices documented in this report, this corpus of judgments provides practitioners with guidance on issues that the interviewees raised during fieldwork. Legal clarifications developed by the CJEU notably include the delineation between the LED and the GDPR [8], the fact that the processing of special categories of personal data should be strictly necessary [9] and the

application of core LED principles such as data minimisation and storage limitation [10]. This developing case-law provides a firmer basis for the consistent application of the directive across the EU.

The LED was adopted to address the specific needs of competent authorities in the field of criminal law. Its scope covers the processing of personal data by police, prosecutors, courts and other competent bodies for the purposes of prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties. While the LED shares core principles with the GDPR (e.g. lawfulness, fairness, purpose limitation, accuracy and data security), it differs in key areas, notably in the broader exemptions and restrictions it permits to protect investigations and public security, as well as its tailored rules on data subjects' rights, oversight and international cooperation. More specifically, whereas Article 6 of the GDPR sets out a list of the different cases under which processing of personal data is lawful, Article 8 of the LED requires processing to be necessary and provided for by law. Data subjects' rights are also more restricted to safeguard law enforcement objectives. In addition, the LED contains more explicit operational requirements around law enforcement processing, including safeguards on data quality/accuracy and security, alongside data storage and logging.

While the GDPR directly applies in the EU Member States, the LED requires Member States to transpose its provisions into national law. The LED sets minimum standards for the processing of personal data by law enforcement and judicial authorities, while allowing Member States some discretion regarding implementation. As a result, while the LED's objectives and principles are reflected across national legislation, differences in legal definitions, supervisory frameworks (including investigatory powers or remedial avenues) or optional clauses (e.g. the rules on data transfers to non-EU countries) exist across Member States [11]. Member States had until May 2018 to finalise their transposition into national law of the LED. In July 2022, the European Commission published its first report on the application and functioning of the LED [12]. The report concluded that the LED has generally been transposed satisfactorily across Member States and represents a key pillar in the EU's data protection framework for criminal law enforcement. The report also flags a number of unresolved issues, particularly in relation to inconsistent national transpositions, limited statistical monitoring, varying data breach procedures and complaint notification practices and continuing legal uncertainty due to ongoing case-law. While most infringement procedures were closed by the end of 2025, in June and July 2026, the European Commission opened infringement procedures by sending letters of formal notice to Belgium, Bulgaria, Czechia, the Netherlands, Poland, Slovenia and Spain, as well as a reasoned opinion to Germany, for failing to comply with the LED [13]. The second report of the Commission on the application and functioning of the LED is expected to be published in the second half of 2026.

To ensure an accurate, detailed and comprehensive analysis of the LED's application in practice, FRA collected experiences from professionals working in, or with, competent authorities under the LED. These research findings can inform and feed into the European Commission's forthcoming evaluation of the LED (similarly to the FRA report published in June 2024 on the GDPR in practice, which focused on the experiences of DPAs; see box '2024 FRA report: GDPR in Practice –

Experiences of data protection authorities*'). To learn about experiences in practice, FRA conducted interviews with relevant actors involved in implementing and supervising the implementation of data protection law under the LED, including:

1. operational staff working in law enforcement and judicial authorities (61 interviews);
2. data protection officers (DPOs) working in law enforcement and judicial authorities (prosecutors and investigating judges) (42 interviews);
3. staff working on questions related to the supervision of the LED in national DPAs (29 interviews).

FRA conducted between three and six interviews in each of the 27 Member States, conducting a total of 132 interviews. Fieldwork was carried out in the first half of 2025. More details on the methodology can be found in Annex 1.

2024 FRA report: *GDPR in Practice – Experiences of data protection authorities*

In June 2024, FRA published a report on the experiences of DPAs from the 27 Member States when implementing the GDPR. The report highlights key issues, showcases best practices and suggests solutions.

- Lack of resources. Underfunding and a lack of staff hamper the authorities from fully carrying out their mandates. New EU laws, such as the AI Act (*), and EU border management systems will create additional tasks for them. These will be difficult to implement without appropriate resources. Member States should secure the necessary financial, human and technical resources to allow DPAs to fulfil their role.
- Supervisory powers. DPAs already have investigative powers, but they need more tools to reinforce their supervisory capacity, such as the ability to conduct undercover investigations or the possibility to fine organisations that refuse to cooperate. The European Commission and the EDPB should assess which tools are needed and reinforce the legal framework if necessary.
- Exchange of best practices. Lacking resources, DPAs often need to prioritise complaint handling over other tasks. To better support authorities in the processing of large numbers of complaints, the EDPB should provide more guidance and facilitate the exchange of best practices. This may also require the EDPB being granted more resources.
- Consultation and providing advice. DPAs are often not consulted on new legislation or are given tight deadlines. Some public authorities also do not consult with DPAs before launching a data processing operation. To ensure

that data protection principles are considered in legislative proposals, Member States should consult with DPAs and seek their advice in advance. They should also encourage public institutions to more systematically consult with DPAs.

- New technologies. The GDPR provides useful tools for dealing with new technological challenges, but many DPAs struggle to properly regulate them. Together with DPAs, the EDPB should identify specific technology-related areas where more clarity is needed. DPAs should work more closely together when advising on new technologies.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Source: FRA, GDPR in Practice – Experiences of data protection authorities, Publications Office of the European Union, Luxembourg, 2024.

This report aims to support the evaluation of the LED with respect to fundamental rights protection based on the experiences of practitioners and experts. It provides unique insights into the practices and challenges of those processing personal data in a law enforcement context, as well as of those supervising such practices. The results provide findings from a variety of practitioners in the field without claiming to be representative of all relevant stakeholders, given that the findings are based on in-depth qualitative interviews, which are – by their very nature – limited in number.

The interviews covered questions about:

- the practical implementation of the LED, looking into requirements related to the core data protection principles of the LED;
- experiences and challenges related to inspections and investigations of potential interferences with the LED;
- experiences and practices of seeking or providing advice;
- existing cooperation networks or cooperation systems supporting the enforcement of data protection, namely between DPOs, between competent authorities or between competent authorities and DPAs.

During the interviews, some interviewees (from all groups interviewed during this research, that is, DPAs, law enforcement authorities and judicial authorities) raised what they perceived to be incorrect transpositions of some of the LED requirements into their national legislation. These concerns of potential incorrect transpositions linked to specific LED provisions related to, notably,

data subjects' rights and criminal/judicial proceedings exemptions. While these concerns may give indications of a need to review some of the national acts transposing the LED, these were not further analysed by FRA, given its mandate, and therefore are not reported in detail in this report.

The report starts with an analysis of the experiences of officers from law enforcement and judicial authorities when handling personal data under national data protection laws transposing the LED. It highlights issues linked to the awareness and knowledge of data protection law, as well as operational practices for implementing data protection requirements. While Chapter 1 focuses on the experiences of operational staff processing personal data, it incorporates the views of DPOs in relation to the understanding and awareness of the LED principles within their organisation.

The second chapter focuses on experiences and views of DPOs within competent authorities (from both law enforcement and judicial authorities), focusing on their roles, experiences and relationships within their authority. Chapter 2 includes the perceptions of DPOs' role within the organisation (both by them and by their colleagues), the evolution they witnessed since the entry into force of the LED and the limitations or challenges they have identified in their day-to-day work.

Chapter 3 reports on the experiences of DPAs in overseeing data protection law with respect to personal data processing in the law enforcement context. It looks at their available resources and the specific challenges related to the enforcement of the LED by these supervisory authorities.

1. Applying data protection principles: insights from police and judicial authorities

To collect first-hand experiences of the understanding of, and potential challenges related to, the application of data protection principles, FRA interviewed three staff members of competent authorities (as per the LED, see box 'Competent authorities within the scope of the LED (Article 3(7))') per Member State: two in law enforcement authorities and one in a public prosecutor's office.

Competent authorities within the scope of the LED (Article 3(7))

The LED defines competent authorities as:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

For the police, interviews were conducted with 16 officers working as criminal investigators, 15 cybercrime investigation specialists, four officers working in border criminal investigations, three officers with legal or data protection specialisations (other than DPOs), two data analysts, two officers in charge of international cooperation and one officer in charge of staff management. For judicial authorities, interviews included 12 prosecutors, three judges, two state attorneys and one investigator, with specialisations including cybercrime, digital investigations, international cooperation and data protection (see Annex 1).

Overall, the analysis shows that, within competent authorities, the staff interviewed were aware of the requirements stemming from data protection legislation, but often lacked a clear understanding of the exact meaning and purpose of these requirements. A few interviewees also questioned the extent of their responsibility towards data protection requirements.

This chapter looks in detail at the main patterns identified of how competent authorities understand and implement legal requirements stemming from data protection legislation.

The first section reports on the awareness, and on the understanding of the meaning, of the LED's

core requirements as listed in Article 4 of the LED. It looks in particular at interviewees' awareness of the legal basis allowing them to collect and process personal data, at the challenges of correctly understanding the notions of 'data minimisation' and 'purpose limitation' and at how these requirements can be confused with data security and police effectiveness.

The second section describes some of the obligations of competent authorities and the challenges that operational staff may face when implementing those obligations. This section focuses on questions related to ensuring the security of personal data, addressing data breaches, handling data subjects' requests and cooperating with DPAs when the competent authority is being inspected or investigated.

Finally, the third section details how interviewees from competent authorities seek and receive advice.

1.1. Competent authorities' understanding of the core principles of the Law Enforcement Directive

Article 4 of the LED clarifies the meaning and objective of the six core principles enabling the effective protection of individuals when their personal data are processed by law enforcement and judicial authorities (see box 'LED core principles (Article 4 of the LED)').

LED core principles (Article 4 of the LED)

1. Lawfulness and fairness: personal data must be processed lawfully and fairly, ensuring respect for individuals' rights and freedoms.

2. Purpose limitation: data must be collected for specified, explicit and legitimate law enforcement purposes and not further processed in a way that is incompatible with those purposes.

3. Data minimisation: the personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy: personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to correct or erase inaccurate information.

5. Storage limitation: data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes of processing.

6. Integrity and confidentiality: appropriate technical and organisational measures must be in place to ensure data security, protecting against unauthorised or

unlawful processing and accidental loss, destruction or damage.

FRA asked interviewees about their awareness of, understanding of and – where relevant – difficulties in relation to the practical implementation of these principles.

1.1.1. Lawfulness of processing of personal data for law enforcement purposes

Under the LED, the principle of lawfulness set out in Article 4(1)(a) is given concrete expression in Article 8. Pursuant to that provision, the processing of personal data by competent authorities is lawful only when it is necessary for the performance of a task carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security, and when it is based on EU or Member State law. Such law must, at a minimum, specify the objectives of the processing, the categories of personal data to be processed and the purposes of the processing.

In relation to this principle, FRA asked interviewees whether they were aware of the legal basis allowing them to collect and process personal data. In a large majority of interviews, operational staff from law enforcement competent authorities were well aware of the legal basis, referring to the national criminal proceedings code, to the national law transposing the LED and/or to the national act establishing law enforcement powers. This also extends to interviewees from judicial authorities, who mostly referred to national criminal procedural laws as the basis for data processing, with some of them also referring to the national legislation transposing the LED.

In parallel, some interviewees working as operational staff within law enforcement authorities said that assessing the lawfulness of data processing and compliance with related legal requirements was not their responsibility. They considered these issues to have already been addressed by other actors, particularly prosecutors, who authorise data collection and processing, and information technology (IT) experts, who provide systems designed to incorporate data protection requirements.

> **In my view, [ensuring the protection of personal data] is not our responsibility to guarantee that. We have rights and obligations defined by the Criminal Procedure Code.**
>
> *An officer at a law enforcement authority*

> **The databases are fully compliant with the law when we receive them. We do not need to contact the DPO because everything has already been taken care of by the time the databases reach us as the end users.**
>
> *An officer at a law enforcement authority*

Some interviewees working as operational staff in law enforcement mentioned that they were aware of several laws applying to them and that this multiplication of legal requirements makes the understanding of the legal basis and related requirements that apply to their data processing more difficult. Some interviewees also emphasised that, in their view, the current legal framework is not adapted to the reality of criminal investigations, notably when it comes to new technologies or when conducting cross-border investigations.

> **In my view, it has been a mistake to design the regulation so that the laws continuously refer to each other with expressions such as 'to the extent that' and 'where applicable'. It would be clearer if all the necessary provisions were written directly into a single law, so that they could be read consistently in one place without constant searching and interpretation. The current structure of cross-references creates many practical problems.**
>
> *An officer at a law enforcement authority*

Distinction between the General Data Protection Regulation and the Law Enforcement Directive

Potential difficulties related to the lawfulness of data processing were also discussed with DPOs working in competent authorities. They were asked whether they found it difficult to distinguish between the GDPR and the LED. Some of the respondents acting as DPOs indicated that, while this might have created some confusion at the beginning (notably in relation to traffic policing,

administrative sanctions or border controls, in relation to which Member States have adopted different approaches), it is not the case any more. Several of the DPOs interviewed stated that these were not, in fact, real difficulties, but only 'residual' difficulties. As mentioned by a few of them, uncertainties on the approach to follow remain for data processing that involves a 'combination of principles from both the LED and the GDPR'. Some of the examples given referred to digital file management systems for collecting personal data that may be related to both criminal and non-criminal investigations. However, among judicial authorities, some interviewees called for more guidance and clarification on the interpretation of the LED in relation to the GDPR, also noting that the LED is not well known enough among professionals.

Conditions applying to international transfers of personal data

When it comes to international transfers of personal data processed for law enforcement purposes, the LED sets out in Articles 35–40 specific requirements to ensure that such transfers occur only when there are adequate safeguards to protect individuals' rights and freedoms, including limits on onward transfers, purpose limitation and proportionality. Such transfers will be lawful only if one of the following legal bases is in place: an adequacy decision adopted by the European Commission; in the absence of an adequacy decision, appropriate safeguards; or, in the absence of both an adequacy decision and appropriate safeguards, derogations for specific, exceptional, situations (e.g. to protect the vital or legitimate interests of the data subject or to prevent an immediate and serious threat to public security). An adequacy decision under Article 36 of the LED is a formal determination by the European Commission that a non-EU country ensures a level of personal data protection that is essentially equivalent to that guaranteed within the EU for law enforcement purposes. At the time of writing, the European Commission has adopted one adequacy decision under the LED, namely with the United Kingdom. The limited availability of adequacy decisions places greater weight on appropriate safeguards under Article 37 and, in their absence, derogations for specific situations under Article 38. Reliance on these more decentralised mechanisms may lead to differing approaches across Member States.

> **"The requirements set out, among others, in Article 35 of the Law Enforcement Directive (LED) and the guidelines of the European Data Protection Board (EDPB) place a heavy burden on data controllers. Specifically, data controllers are expected to conduct an in-depth analysis of the relevant legislation for each country they cooperate with – a task that proves unfeasible in practice due to language barriers and limited capacity.**
>
> *An officer at a law enforcement authority*

DPOs working in competent authorities were asked to describe the processes followed by their authority to ensure the protection of personal data when these data are transferred to competent authorities in non-EU countries and international organisations. Almost all of them demonstrated being well aware of the legal framework (and notably the necessity to have an adequacy decision in place). A few DPOs interviewed by FRA stated that they, as DPOs, do not deal with such transfers, as these are exclusively under the responsibility of their international cooperation unit. None of them reported having consulted their DPA for further guidance on this. Some of them referred to the International Criminal Police Organization (Interpol) legal framework, with one interviewee mentioning that this framework is 'easier' and another one clarifying that this is a 'strategic choice', as 'Interpol provides a framework that offers certain safeguards and … a lot of guidance'.

> **Our primary approach is to first explore whether the data transfer can be addressed through existing channels like Interpol, rather than immediately engaging with the complex hierarchy of third-country transfer conditions. The adequacy decision has been particularly beneficial in simplifying our data transfer processes. We prioritise using established international frameworks and maintain a cautious approach to transfers that fall outside these standard mechanisms.**
>
> *A DPO at a law enforcement authority*

Several DPOs also mentioned that they do not have many cases involving international data transfer. However, some DPOs did mention challenges, referring notably to transfer to non-EU countries with no adequacy decisions and the difficulty of precisely defining what appropriate safeguards consist of. As one interviewee puts it: 'consequently, there is a tendency to rely on the exceptions instead in individual cases. But exceptions are not intended to be used repeatedly and systematically.'

> **So, practically, now, there are no data protection agreements on law enforcement with data protection with Asian countries. But we have the old ones, that we use. The directive says that old agreements remain in force until they are amended. If you ask me, this is a loophole in the directive.**
>
> *A DPO at an interior ministry*

In addition, specific cases were mentioned as more challenging, such as the use of software or databases (including cloud storage) in which companies are based outside the EU, specifically in the United States. One DPO working in a law enforcement authority referred to the wish expressed by operational staff to access and use data collected by companies offering genetic services based on the collection of DNA information. Finally, one DPO working in a prosecutor's office identified as a recurring issue the lack of a definition of what 'structural transfers' consist of (as opposed to 'incidental transfers'), since, in their view, 'a request for legal assistance is by definition incidental, as it relates to a specific criminal case'. These concerns from DPOs echo concerns raised by operational staff working in law enforcement, as discussed earlier. Interviewees from competent authorities (DPOs and operational staff alike) who raised these concerns agreed that these issues stem from a lack of legal clarity and that further guidance at the EU level would be beneficial.

> **If you do not have the skills [to work in a technical area, such as genetic genealogy] in [Member State] or Europe, and they do in third countries, then these rules become a problem.**
>
> *A DPO at a law enforcement authority*

1.1.2. Operational data protection requirements: purpose limitation and data minimisation

Article 4(1)(b) and (c) of the LED establish, respectively, the principles of purpose limitation and

data minimisation. Purpose limitation requires personal data to be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. Data minimisation requires the data processed for a given purpose to be adequate, relevant and not excessive. Recital 26 further clarifies that the purposes should be determined at the time of collection and that personal data should be processed only when the purpose cannot reasonably be achieved by other means.

The two principles are closely connected, but perform distinct functions. Purpose limitation determines what personal data may be used for, whereas data minimisation constrains the number and type of data processed for that purpose [14] . Data minimisation may in this sense be understood as an operational consequence of purpose limitation: whether data are adequate, relevant and not excessive can be assessed only in relation to a sufficiently specified purpose [15] .

Purpose limitation under the LED does not impose an absolute prohibition on subsequent processing for another law enforcement purpose. Under Article 4(2), processing by the same or another controller for a purpose set out in Article 1(1), other than that for which the data were collected, is permitted only when the controller is authorised to process the data for that purpose under EU or Member State law and the processing is necessary and proportionate to that other purpose. In the case of *Inspektor* v *Inspektorata kam Visshia sadeben savet*, the CJEU confirmed that these conditions apply even when both the original and the subsequent purposes fall within the scope of the LED. The CJEU held, in particular, that data collected for the detection and investigation of a criminal offence and subsequently processed to prosecute a person following the conclusion of that investigation are processed for another purpose within the meaning of Article 4(2). [16]

Operational staff described a range of ways in which purpose limitation and data minimisation are applied in practice. Only a few interviewees explicitly highlighted the data protection impact assessment (DPIA) as a key moment when these principles are examined, namely when launching or changing processing activities. At the same time, several operational staff in law enforcement described applying these principles as part of everyday casework: lead investigators determine what information is necessary for the case, decide what should be retained or deleted and make case-by-case judgements on what is relevant and proportionate to the investigative purpose. Several interviewees working as operational staff in law enforcement also referred to the existence of internal guidance supporting this work, including policies, system-specific internal directives or practical tools and support measures such as checklists, training or DPO-led guidance.

Similarly to what was mentioned in relation to the lawfulness of processing (see Section 1.1.1), some interviewees pointed to prosecutors' and judges' decisive roles in constraining what data may be collected or used in a given case, while others referred to IT-system configurations (e.g. logging and access restrictions) as practical safeguards.

Purpose limitation

When discussing purpose limitation, some interviewees working as operational agents in law enforcement authorities stated that reusing data for other purposes was not possible. They referred to the facts that (1) data that are directly linked to a case are not useful for other cases and (2) once the data are transferred to the prosecutor and/or the investigation is closed, the data are deleted, anonymised or encrypted. Nevertheless, several interviewees stated that the reuse of data is possible when:

- the grounds for the reuse of data are established in law;
- the prosecutor authorised the reuse;
- the investigator in charge of the original investigation for which data were collected agreed to the reuse.

Some interviewees also stated that, in their views, the reuse of data for other criminal investigations is generally permissible, given that the purpose would 'stay the same'. Two interviewees mentioned that the purpose is covered by the necessity to reuse data for crime prevention purposes, with one interviewee referring to their 'duty to act'.

> **"And there is naturally the question 'What is actually the purpose now?' … I'll just give an example: the police has a stated task for which I collect personal data. So quite classically 'XY is suspected of bodily harm'. Then I have the dataset available. And this dataset, I can now use it for all possible police purposes … The narrower the purpose is, the more complex the construct becomes and nobody can handle that any more.**
>
> *A DPO at a law enforcement authority*

Data minimisation

When it comes to data minimisation, most interviewees working as operational staff in law enforcement authorities linked this principle to police effectiveness (see Section 1.1.4): collecting irrelevant or unnecessary data was seen as hindering, rather than helping, an investigation. Some interviewees also said that 'bulk collection' was unrealistic because processing large volumes of

data requires significant technical and human resources.

The principle of data minimisation was often seen as problematic, as it can conflict with the obligation to preserve the integrity of evidence, on one hand, and with the essence of conducting investigations, on the other hand – by both judicial and law enforcement authorities. Deleting data only because their relevance cannot be asserted at the beginning of the investigation would, for example, hamper the investigation itself; some interviewees referred to this as the principle of 'better to have than to need', clarifying that this principle does not apply for data falling under the scope of Article 9 of the GDPR (special categories of personal data). Special categories of personal data include data that reveal information such as racial or ethnic origin or political opinions, genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health and data concerning a natural person's sex life or sexual orientation. The processing of these data categories warrants special protection, is authorised only when strictly necessary and is subject to safeguards as set out in Article 10 of the LED (see box ' Fundamental rights implications of the use of remote biometric identification in the context of law enforcement').

> **It is difficult to assess what information is unnecessary. If it is clearly unnecessary – for example if it is discovered that coercive measures have yielded information about some third party that is in no way related to the matter – then that is easy. But if the information might possibly relate to the specific subject of the investigation or the matter under investigation, then it is hard to draw a clear-cut line and say that this can simply be deleted, because it may indeed contain relevant evidence. And even if it does not, it leaves open the possibility that the suspect can later claim in court that it contained exculpatory evidence supporting their innocence.**
>
> *An officer at a law enforcement authority*

Fundamental rights implications of the use of remote biometric identification in the context of law enforcement

In October 2026, FRA published a report on the fundamental rights implications of the use of remote biometric identification (RBI) for law enforcement purposes. RBI

is a technology that allows the identification of people at a distance without their active involvement or participation. While such systems provide opportunities to enhance public security, protect people from crime and find victims of crime or missing people, their development and use also raise serious fundamental rights concerns.

The FRA report outlines the legal framework governing RBI use in the EU, notably the AI Act, EU fundamental rights law and the EU data protection *acquis*. These laws set stringent requirements for RBI use, restricting or prohibiting its use by law enforcement, but also by other public and private actors outside law enforcement.

The report examines – based on legal analysis, interviews with law enforcement practitioners and other experts and a quantitative survey with members of the public – key fundamental rights challenges that can arise with RBI use for law enforcement purposes. It provides insights into how to enhance the protection of fundamental rights when considering the use of such powerful systems.

The findings of the report aim to inform the implementation of the AI Act and, more broadly, the fundamental-rights-compliant use of RBI for law enforcement purposes across the EU.

Source: FRA, Remote Biometric Identification for Law Enforcement Purposes – Fundamental rights implications, 2026.

Issues raised in relation to both principles

FRA findings show that, in several cases, operational staff working in law enforcement authorities (and, to a lesser extent, from judicial authorities), were not well aware of the exact meaning of the principles of data minimisation and purpose limitation; these staff referred mainly to data security measures – which can also support these principles in practice – as safeguards for both (see Section 1.1.3). Two types of measures, notably, were described as a way to ensure either purpose limitation or data minimisation: first, several interviewees referred to features of their electronic devices (e.g. logging access, limited entry data or automatic deletion) and, second, several interviewees referred to the protocols requiring specific authorisation for staff to access the data. In addition, some interviewees confused the two: when asked about purpose limitation, they referred to the fact that they collect only necessary data (i.e. referring to measures linked to data minimisation rather than purpose limitation).

> **The law stipulates 18 types or categories of data we can collect from an air carrier. If within the data (received from the air carriers) appears the data that we are not authorised to collect … automated procedures within the system automatically ignore such data in a way that such data is no longer visible to us at all.**
>
> *An officer at a law enforcement authority*

Among judicial authorities, two interviewees challenged requirements linked to purpose limitation, arguing that if data relevant to one criminal investigation are obtained during another investigation for a different purpose, the use of these data in newly initiated or ongoing criminal proceedings should be permitted. Similarly, some interviewees (from both law enforcement and judicial authorities) expressed irritations towards what is perceived as rigid and/or time-consuming requirements, arguing that these requirements are taking away the possibility to focus on material agendas for the sake of administrative tasks of limited added value.

> **If I am to be honest, from my point of view, instead of dealing with the actual protection or effective handling of personal data, we are dealing with an incredibly bloated amount of administration that uses amazing formulations (like 'purpose limitation' or 'data minimisation'). Even though I am a lawyer, I do not understand these.**
>
> *An officer at a law enforcement authority*

Guidance and data protection officers' role in supporting the implementation of both principles

Several of the DPOs interviewed by FRA stated that the question of purpose limitation is one of the core issues on which they are consulted upon. They indicated that the guidance provided by them is case specific and, generally, the main issue is to define whether the purpose should be

understood broadly or narrowly. Indeed, while several agents working in law enforcement could not refer to the existence of written guidelines on either the purpose limitation principle or the data minimisation principle, a few interviewees in law enforcement did refer to their DPO as a source for further guidance, as a mandatory validation step or in relation to general guidelines developed by their DPO. As an exception to the general absence of written guidance reported to FRA, one interviewee working with a database stated that their department has established an 'internal methodological instruction that contains specific rules and protocols for responding to requests'.

> **Do any rules or guidelines on how to collect as little data as possible exist? That's not something I have seen. From our perspective, it is a matter of collecting the data that is necessary after our assessment to solve the task. I am sure, if you go through the preparatory works pertaining to the [country] Police Act you will see different considerations to be taken into account, but this is not put in a frame and hung up on the wall.**
>
> *An officer at a law enforcement authority*

To summarise, FRA interviews reveal significant challenges in applying the LED's purpose limitation and data minimisation principles in practice. While it is clear that the LED core principles are not unknown by operational staff working in law enforcement and judicial authorities, staff could benefit from guidance and clarification on their exact purpose and meaning, as well as on the technical and organisational measures attached to them. Purpose limitation appears to be frequently stretched, with the reuse of data justified by broad interpretations of 'crime prevention' or investigative duties, despite recital 26's emphasis on explicit, narrow purposes. Meanwhile, data minimisation is perceived to clash with evidentiary needs, as indicated some practitioners, who state that they fear that deletion could compromise investigations or future proceedings. While technical safeguards (e.g. automated deletion and access logs) help, they do not replace substantive necessity and proportionality assessments. To align practice with the LED, stronger DPA oversight, targeted training and harmonised interpretations of 'necessity' and 'proportionality' are essential, ensuring that law enforcement's legitimate needs are aligned with fundamental rights protections.

1.1.3. Data security and technical safeguards

As detailed in the previous subsection, a majority of interviewees stated that the strict protocols (data storage, access limitation, logging, etc.) implemented by law enforcement authorities to ensure that only certain individuals are allowed to access specific files or databases were the main measures used to ensure that each of the data protection principles discussed are respected. From the perspective of several of the interviewees in law enforcement authorities, once the data are collected, they belong to the investigators. Consequently, access to data is restricted not based on purpose, but based on staff access rights.

When asked about data security, several operational staff did not identify significant challenges and stated that this is 'generally not an issue' and that most security breaches result from human errors. By contrast, one interviewee noted that, in their organisation, everything was legally in order, but personal data were not sufficiently protected from a technical perspective, leading to data breaches.

On data storage, most interviewees in law enforcement and judicial authorities were aware that the law sets time limits for deleting personal data or for periodically reviewing whether continued storage is necessary. Some noted that these limits vary depending on the type of data, the purpose of processing or the seriousness of the offence. A few interviewees also stressed that retention rules are complex and fragmented, with different legal provisions sometimes overlapping or conflicting. A couple of interviewees complained about these rules, namely a DPO working in law enforcement, who explained that they need to regularly negotiate deletion periods with DPAs, and an officer working in a judicial authority, who disagreed with data storage time limits because they limit the possibility to further analyse the data in the future, for example with the help of AI (see the following quote).

> **What I don't like about this is a practical reason. By destroying such files, we lose the ability to further analyse that data in the future, for example with the help of artificial intelligence. Because what does it mean to destroy data? Yes, I may not use it … But I can use it to establish patterns of criminal activity, behaviour … I must try to review the reasons for the crime, and so on. Moreover, I can use old, closed files to determine that there are, for example, connections with my current case.**
>
> *An officer at a judicial authority*

Most operational staff rely on automatic features of their file management systems (e.g. automatic deletion, blocking or flags of the data). When asked whether they were aware of regular

revision of the need to keep the data, most interviewees in judicial and law enforcement authorities stated that they did not know of any case in which internal controls of the data storage time limits were conducted. Only two interviewees referred to periodic reviews of the need to store data.

Promising practice: conducting cross-cutting inspections to identify a lack of awareness and develop targeted guidance (Finland)

In 2021, the Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto) in Finland carried out auditing and inspection activities of authorities involved in criminal justice and internal security. The competent authorities audited included the National Police Board, the Finnish Defence Forces, police departments, the immigration administration and the National Prosecution Authority.

These audits focused on how these bodies handle personal data, particularly sensitive categories such as criminal-justice data, and whether they respect core principles of data protection law (lawfulness, purpose limitation, data minimisation, security, documentation, etc.).

The DPA notably highlighted, in relation to data security, that:

- authorities handling sensitive and criminal-justice data are expected to maintain robust documentation and internal controls demonstrating lawful processing and accountability under GDPR principles;
- given the strong connection between data protection and information security, authorities are urged to implement appropriate technical and organisational measures and to clearly document these safeguards.

In December 2023, the Finnish Parliament adopted amendments to the national Data Protection Act (Tietosuojalaki, 1050/2018) and the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä, 1054/2018) to align Finnish law more closely with EU data protection requirements and to strengthen supervisory practices and individual rights enforcement.

Source: Office of the Data Protection Ombudsman, Annual Report of the Office of the Data Protection Ombudsman 2021, Helsinki, 2021; and Office of the Data Protection Ombudsman, Annual Report of the Office of the Data Protection Ombudsman 2023, Helsinki, 2023.

When it comes to data security and technical safeguards, interviewees highlighted a strong trust in and reliance on their technical and procedural safeguards (e.g. access controls, logging and automated deletion) to enforce not only data security requirements, but also data protection principles as a whole. While such measures are an important part of LED compliance and can help operationalise data protection principles in practice, they cannot by themselves ensure compliance with the LED's core requirements. They need to be accompanied by substantive assessments of legality, necessity, proportionality, purpose limitation, data minimisation and storage limitation. The lack of proactive, human and/or external (by DPAs) reviews (beyond automated systems) could further weaken accountability. In addition, indeterminate storage justified by future investigative potential could conflict with the storage limitation principle set out in Article 4(1)(e) and recital 26's emphasis on necessity.

1.1.4. Data accuracy and data protection in general as safeguards of investigations' effectiveness

Several DPOs stated that the LED was 'not as revolutionary as announced': in their views, most of the concepts and requirements set out in the LED already existed. Interestingly, several operational staff explained that, for them, data protection principles such as data minimisation were already being applied to guarantee **effective** investigations. Similarly, the findings suggest that considerations of investigative effectiveness also shape approaches to data quality and to personal data based on facts or assessments.

Accuracy of personal data

Almost all interviewees stated that it is 'in the interest of the investigator' to work with accurate data. However, when questioned on how they ensure the accuracy of personal data, some of them could not describe specific measures and others noted explicitly that continuous or proactive monitoring to ensure data quality was not in place. As one interviewee put it, data are updated through day-to-day work, but regular check-ups are simply not feasible.

Respondents who did indicate ways to ensure the accuracy of data referred to the cross-checking of data with other national databases 'when time allows'. In one Member State, a control mechanism exists whereby, before information is added to the central law enforcement database (covering people, vehicles, places and facts), designated staff review the content and key terms for data quality and check whether retention remains necessary.

In a few cases, interviewees explicitly mentioned that police databases are linked to authoritative governmental sources (e.g. municipal registers) to support data quality. However, a few interviewees referred to the fact that, sometimes, the same data are stored separately and in different databases, meaning that updates made in one system do not automatically apply to others, which can result in duplicate records that become outdated and/or differ from each other.

A few interviewees noted, for example, that the police and the courts use separate information systems that are not interoperable.

At the same time, several interviewees from the judiciary claimed that their responsibility for ensuring data quality was limited, as the data are collected by other actors in pretrial investigations, notably the police. Thus, they do not engage in extensive control of accuracy of the data collected by the police, possibly only checking when certain data are questioned. Nevertheless, a few interviewees shared that, in their institutions, there are several mechanisms ensuring the quality and adequacy of personal data, such as:

- the existence of data repository systems that allow corrections to be made to input data, which are then automatically updated across all existing records;
- existing safeguards that prevent the entry of inconsistent data;
- automatic updates;
- formal procedures when handling corrections of data;
- the inclusion of records of incorrect data for traceability.

> **The workload for police officers is currently so high that the incentive to enter and manage superfluous data is low.**
>
> *A DPO at a law enforcement authority*

Personal data based on facts versus personal assessments

The question of effectiveness and professionalism was also raised by several interviewees in law enforcement and judicial authorities when discussing how they approach the obligation of the LED to distinguish between personal data based on facts and data based on personal assessments, to ensure data quality in line with Article 7 of the LED. While respondents had contradicting replies, interestingly, both approaches were justified by the effectiveness of the investigations.

- Several respondents stated that the police or the prosecutor could simply never work with data based on personal assessment, as this would endanger the investigation itself. Investigators analysing forensic evidence clearly stated that they would never come across data based on anything but facts.

> **[P]ersonally, I have always found it difficult to know … what is meant by data based on personal assessments because in police work, everything is always factual. Everything they record … must be facts, and it is on the basis of these facts that the judicial authorities must judge whether or not the person is guilty. So, I find it difficult to see what, in the context of police work, [could be] based on … personal assessments.**

A DPO at a law enforcement authority

- For other respondents, by contrast, integrating data based on personal assessment is an inherent part of the work of operational staff, building on experiences, hearsay or extracts from communication during surveillance operations.
- Some interviewees indicated that such data should be flagged in the system, labelling them as, for example, 'soft data' (as opposed to 'factual data') or flagging their reliability and importance. However, another interviewee from a judicial authority, by contrast, claimed that differentiating between factual data and personal assessments would conflict with the national procedural norms of criminal law and the fundamental principles of evidentiary evaluations. A few operational staff also noted that, in the absence of guidelines, it is difficult to distinguish between data based on facts and data based on personal assessments.

> **[Our work] does not focus on citizens' rights but is concerned with ensuring that data quality is high so that the data can be used as evidence in court.**

A DPO at a law enforcement authority

- While several interviewees from judicial authorities explicitly noted that they do not work with personal data based on personal assessments, some of them observed that it may be difficult or even impossible to make this distinction and implement the requirement formally, justifying this as the approach required to achieve effective criminal investigations.

Promising practice: scoring the reliability of the data (Belgium)

In Belgium, the police must score the 'trustworthiness' (both the content and the source) of the information that is inherently considered to be less certain in the database. There is a specific field for the police to fill out, usually in the form of metadata in relation to a document in a database. The source is assessed as one of the following: always trustworthy (code A), usually trustworthy (code B), not trustworthy (code C) or cannot be assessed (X). The certainty of the information is assessed as one of the following: certain (code 1), observed by the source (code 2), heard and confirmed (code 3) or heard and not confirmed (code 4). It is the responsibility of the investigator to estimate the scores.

Source: FRA interview in Belgium.

FRA interviews revealed a pragmatic, but sometimes inconsistent, approach to data accuracy and quality under the LED, driven primarily by investigative effectiveness rather than strict compliance. While practitioners recognise that accurate data are critical for investigations, proactive measures (e.g. regular reviews or cross-system updates) are rarely implemented. Interviewees highlighted specific issues, such as interoperability gaps between police and judicial systems and dependency on external actors (e.g. prosecutors for deletion triggers), as potential areas for further inaccuracies, which may in turn create accountability blind spots.

FRA interviews also showed that there is an uneven understanding among operational staff working in law enforcement authorities of the requirement to distinguish between factual data and personal assessments in line with Article 7 of the LED. While some practitioners reject the notion of 'assessment-based' data entirely, insisting that all information must be factual to ensure evidentiary validity, others acknowledge that operational work inherently relies on subjective inputs (e.g. intelligence and hearsay). The interviews revealed the need to tie data accuracy not only to police effectiveness, but also to data protection compliance. Effectiveness-driven approaches can undermine accuracy and therefore can compromise both investigations and fundamental rights.

1.2. Ensuring data security and providing accountability

The LED framework provides competent authorities with targeted instructions and processes to address requests from data subjects and handle potential breaches. Data subjects' rights are described in Chapter III of the LED and include the right to request that competent authorities provide them with specific information related to the processing of data pertaining to them, the right to access these data and the right to rectify or erase data held by competent authorities

about them. Limitations to these rights are permitted, in cases that are clearly defined in Article 15 of the LED. That is, these rights can be restricted for the following purposes: to avoid obstructing official or legal inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; to protect public security; to protect national security; or to protect the rights and freedoms of others.

Obligations of competent authorities are described in Chapter IV of the LED. These include specific data security requirements, for instance the obligation to implement data protection measures 'by design and by default' in line with Article 20 of the LED. Further obligations include keeping records and logs of specific processing activities and implementing appropriate technical and organisational measures to ensure the security of the data in accordance with Articles 20, 24, 25 and 29 of the LED. The LED also includes targeted measures to prevent or mitigate interference with the protection of personal data, including cases in which a DPIA should be conducted as mandated by Article 27 of the LED, and processes to be followed to ensure appropriate notification and communication of data breaches as set out in Articles 30 and 31 of the LED.

1.2.1. Protecting data security and handling data breaches

The LED defines in detail the cases in which 'technical and organisational measures' should be taken to ensure the security of data. Interviewees working as operational staff in both law enforcement and judicial authorities were asked whether there were any challenges that they had experienced in their work with respect to the security of personal data.

Overall, interviewees had not witnessed and did not identify major challenges, and several expressed trust in their IT department and the technical safeguards they implemented. Among those who did identify challenges (several interviewees working in judicial authorities and several interviewees working in law enforcement), they referred almost exclusively to human errors, such as the loss of a universal serial bus (USB) key or a handwritten note with passwords on it. Some interviewees did identify IT-related challenges, including a lack of cybersecurity training, specific risks that modern technologies could potentially introduce (without clarifying what risks/technologies they were referring to) and unauthorised access. Within judicial authorities, interviewees identified the following issues as challenging for data security: the inability to anonymise sensitive information, the need to protect personal data when the identity of injured parties must remain confidential and managing the growing volume of data.

Interviewees working in law enforcement authorities also described examples of measures that they take to ensure data security. When it comes to preventing human mistakes from happening, some interviewees referred to cybersecurity training, to working 'in isolation' (i.e. alone) and to avoiding using a USB stick or similar devices. Interviewees also emphasised the clear and strict protocols and procedures that they have in place to ensure data security. As an example, in one case, a law enforcement authority decided to remove all shared accounts, allowing users to log into the information systems only through their individual credentials. A few interviewees also

observed that the topic is always a challenge, noting that security is costly and requires the allocation of certain resources. A lack of resources was indeed highlighted by a few interviewees as a challenge to ensuring data security. One interviewee, for instance, lamented that their authority focuses its attention on human resources, at the expense of technical infrastructure.

As described earlier, most operational staff working in law enforcement perceived risks related to cybersecurity as secondary (i.e. to risks posed by human mistakes). In general, digital data are believed to be sufficiently protected within the organisation. In one case, however, the interviewee insisted that data security was of the utmost importance, following leakages of police information to the press. However, this interviewee believed that the main challenge in ensuring data security in that case lay in their difficulty to identify 'the source of the leak'. Several respondents insisted that a 'zero-risk' policy was not realistic when it comes to cybersecurity, exactly because, in their views, the 'real risks' lie in mismanagement of data by staff.

> **There's no doubt about it, there's going to be challenges going forward. Technology changes. So, what's a challenge today? There could be a new challenge again tomorrow.**
>
> *An officer at a law enforcement authority*

Promising practices: regular assessment of access rights of law enforcement officers (Cyprus)

In Cyprus, to reduce human errors, a system of regular supervisory checks was put in place, whereby each police director regularly reviews the roles designated to their staff members to evaluate whether their right to access personal data is necessary and pertinent to their duties. A dedicated template was developed, and this form must be completed by every police member who wants to search the police IT system, explaining clearly why access is needed.

Source: FRA interview in Cyprus.

Promising practices: reinforcement of the cooperation

between the DPO and the cybersecurity department (France)

In France, to reinforce the security of data, the law enforcement authority's DPO contacted and reinforced their relationship with the cybersecurity unit. The DPO has regular bilateral meetings with their digital security colleague and is a statutory member of all security accreditation committees. The DPO believes that, by bringing the two organisations closer together, it enables a swifter response to the vulnerabilities they identify.

Source: FRA interview in France.

Finally, when asked whether they have specific software to identify data breaches, some interviewees in law enforcement and judicial authorities explicitly indicated that they were aware of dedicated solutions or software that existed in their competent authorities. Others stated that there are procedures in place, but they could not elaborate further, as this specific topic falls under the responsibility of other actors in their institutions (e.g. higher management or IT departments). One interviewee noted that the reason why their authority does not have dedicated software is because limited resources in IT do not allow new systems to be developed, with resources only being available for existing systems to be updated.

Some interviewees mentioned that, while they do not have automated warning systems, they apply other measures to identify personal data breaches or detect abnormal incidents. For instance, one interviewee said that they check log data when there is a suspicion of a personal data breach, while another interviewee noted that investigative actions are taken when they receive a complaint. Another interviewee said that issues are identified through targeted inspections conducted by designated personnel whose responsibilities include checking how data are processed and whether the particular database is accessed or used on a lawful basis.

DPOs were also asked whether they had developed a procedure for identifying personal data breaches, and several of them confirmed that they did. They were further asked if they were aware of guidelines that had been developed by their national DPA or the EDPB to guide the assessment of what is considered a breach and when it needs to be reported to the DPA. Some of them explicitly noted that they were aware of such guidelines and confirmed that these are very valuable in their work on the matter, with one of them indicating that EDPB opinions were the basis of that work to develop the procedure to identify breaches.

> **In our country, the [national DPA] serves as the supervisory authority, and the primary guidelines are set forth in the law. The EDPB provides excellent guidelines and produces invaluable materials. The EDPB has also reviewed and adopted many of the opinions issued by the Article 29 data protection working party, which have proven to be extremely valuable.**
>
> *A DPO at an interior ministry*

The interviews reveal some tendency to over-rely on technical safeguards and human vigilance to uphold data security under the LED. Most operational staff working in law enforcement and judicial authorities express confidence in their IT systems, highlighting that actual challenges stem primarily from human error (e.g. lost devices or poor password practices) rather than systemic vulnerabilities. Although procedural safeguards (e.g. individual logins and access reviews) exist, their effectiveness can be undermined by resource constraints and a lack of cybersecurity training. Some authorities indicated that they struggle with outdated systems or unauthorised access risks, particularly when new technologies introduce unexpected threats (without elaborating on what these technologies/threats are). In addition, breach detection and response seem to remain reactive rather than proactive. A strong security environment (including IT measures and staff awareness) is key both for the protection of data subjects under the LED and for the effectiveness of law enforcement, given that it supports the confidentiality, integrity and availability of law enforcement data, reduces operational risks and supports public trust in police authorities. As such, the security environment would benefit from reinforced cybersecurity measures and training, strengthened IT resources and infrastructures and clear accountability rules.

1.2.2. Handling data subjects' requests

The LED has established several rights for data subjects: the right to be informed (Article 13), the right to access their personal data (Article 14), the right to rectification, erasure or restriction of processing (Article 16), the right to lodge a complaint with a supervisory authority (Article 52), the right to an effective judicial remedy (Article 54) and the right to receive compensation for unlawful processing (Article 56). FRA asked both the DPOs and the operational staff of competent authorities whether they were entitled to handle data subjects' requests. Interviewees had varying responses, showing that the understanding of who is in charge of processing these requests differs across Member States.

Among the DPOs interviewed by FRA, several of them indicated that they are in charge of handling such requests, with some of them clarifying that they are the central contact point when it comes to data subjects' requests (meaning that other departments would forward them the requests that they receive). As highlighted by one interviewee, the centralisation of requests allows there to be consistency in the replies.

However, many DPOs stated that they do not handle these requests, with several of them stating that they do not believe this to be part of their mandate. When they do receive requests, they do not process them and instead transfer them to operational agents. One DPO clarified, however, that they would intervene in cases presenting problems or ambiguities. Finally, in one case, the DPO indicated that requests can be handled by either the DPO or the operational agent and that they had developed guidance and a template on this, which are available on their website.

FRA asked operational staff whether they were consulted on data subjects' requests. A majority of them indicated that they have not been involved in any such processes, with some also clarifying that they believed their authority had not encountered such requests. Other interviewees working as operational staff in law enforcement and judicial authorities indicated that they are consulted on such requests but that the requests are primarily handled by their DPO. All of them were aware of the existence of these subjects' rights.

Several of the interviewees (operational staff in law enforcement and judicial authorities and DPOs alike) who indicated that they handled and/or processed data subjects' requests did not report any significant issues. In a few cases, they indicated that they do not receive many requests, stating that the public is not well aware of the national legislation transposing the LED.

Among DPOs, a few interviewees mentioned that it could be difficult for them to confirm the identity of the individual asking to have access to their data. In their view, 'a signature alone cannot be considered a reliable means of identification' and, therefore, 'it is essential to update the [legal] provision regarding the data subject's right to access personal data to align with current authentication standards'. Another challenge identified by one DPO is the repetition of identical requests by non-EU nationals, which their office still needs to assess and respond to individually. One interviewee described a proposal for overcoming this challenge, namely limiting those who are authorised to represent data subjects to only lawyers who are authorised to work in the territory of the EU or the European Economic Area (the DPO of another Member State clarified that, in their case, all requests related to the Schengen information system (SIS) are dealt with by another department). Finally, a few DPOs mentioned that some requests are either 'unarticulated' or too generic (i.e. requesting to have access to 'all data') and that this creates time-pressure challenges in clarifying with the data subjects the exact content of their request within the period set out in the national legislation. Several DPOs indicated that, in the case of doubts, they would ask the operational unit for further information on the case and/or on whether the data subject's request could be answered positively.

When operational agents are directly involved in assessing data subjects' requests, a recurrent complaint is that dealing with such requests is time consuming and therefore takes up the time that could otherwise be spent on other 'valuable' investigating tasks. Some interviewees working

as operational staff, prosecutors or DPOs did complain about the number of requests that they receive or about requests being burdensome. Some of them pointed out that the biggest share of requests are related to SIS and/or concern non-EU nationals. In one Member State, the DPO indicated that they receive around 900 requests annually, of which approximately 10–15 % are appealed. This work was described by the DPO as being very time consuming; however, the DPO insisted that all requests are treated individually, on a case-by-case basis, and that each individual is informed of the decision and of the possibility to appeal. While some DPO interviewees indeed confirmed that each request is assessed individually, the DPO of one Member State indicated that 'some restrictions are built into specific systems. For example, no citizens are given access to data of the [specific system name] because the specific purpose of the database is to collect confidential information about potential suspects.'

> **"This employs a huge number of people within the police force, and it produces a huge amount of administration. [When] the subject asks what information the police have on them, the DPO sends out that request to all the regional headquarters where the local records are kept … This involves [the work of] dozens of people across the entire police structure to that one specific request … And very often [the response] is just simply stating 'Thank you for the inquiry. We've got nothing for you.' … Underneath the surface of that ordinary request and response, there is a huge agenda involving the whole structure of the force.**
>
> *An officer at a law enforcement authority*

Should the request endanger the pursuit of criminal investigations, competent authorities may deny the request. Restrictions to data subjects' rights can only be permitted on the basis of specific grounds in order to avoid obstructing inquiries, investigations or procedures; to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences; and to protect public security, national security or the rights and freedoms of others as set out in Article 15(1) of the LED.

Most of the interviewees working within law enforcement and judicial authorities did not report any complications with regard to potential restrictions to data subjects' rights. The few challenges identified during the interviews related to cases when the data subject was under surveillance measures or when information needed to be exchanged with other Member States that impose restrictions on the use of shared information, potentially resulting in conflicts between national legislations. One interviewee highlighted that this may create tension between national law and

international obligations and would require policy-level coordination.

One interviewee clarified that, in the case of doubt, they would first consult with colleagues internally and, if the doubt persisted, they would consult with the public prosecutor. In one Member State, the DPO indicated that they are obliged to first consult with the national DPA before restricting any of the rights of the data subjects. In another case, a prosecutor explained that their DPA requested that any restriction of these rights needed to be considered a postponement, not a denial. This means that, in this case, requests need to be re-examined at a later stage, when the grounds for refusal no longer apply.

Promising practice: centralisation of all requests within one DPO's office and regular exchanges of views with the DPA (Ireland)

In Ireland, the DPO office of the police, the Garda National Data Protection Office (An Garda Síochána), indicated that all data subjects' requests are centralised in their office. Requests received by other police divisions or business areas are forwarded to the DPO office. In its view, this has had a positive effect on the effectiveness and consistency of dealing with such requests. The DPO office has set out procedures for assessing each request against the available restrictions as stated in the law.

"This is a great benefit of having it centralised in that we train our team on the restrictions that can be applied and the reasons why they can be applied."

In addition, the DPO office holds quarterly meetings with the data protection supervisory authority in Ireland, the Data Protection Commission (DPC) (An Coimisiún um Chosaint Sonraí), to discuss cases and the rationale followed by them to apply restrictions.

"These conversations are typically constructive. The DPC's annual reports, and their compendium of case studies for the first five years of the operation of the GDPR and LED, often show complaints where they've found in our favour because our rationale was sound. Out of an annual average of 6 000 requests, our live complaint caseload with the DPC is normally around 30, which suggests most recipients are satisfied with our responses. Our approach focuses on transparency and providing clear explanations for any restrictions applied to data subject rights."

Source: An Garda Síochána (Irish Police), Garda National Data Protection Office (GNDPO), Ireland

A further procedural safeguard was reported in Austria. When the police restrict the information

provided in response to the exercise of data subjects' rights on grounds recognised by the LED, such as the protection of an ongoing investigation or national security, the DPA can conduct a confidential assessment. The DPA receives all of the relevant information from the police and assesses the lawfulness of the processing, the necessity of using the procedure in the specific case and whether the storage and other processing of the data comply with the law. Restricted information is not disclosed during the proceedings, but the data subject receives a reasoned decision indicating whether the complaint has been upheld or rejected [17]. This reflects Article 17 of the LED, under which data subjects' rights may also be exercised through the supervisory authority in the cases referred to in Articles 13(3), 15(3) and 16(4) of the LED. As clarified by the CJEU in case C-333/22, when the direct exercise of data subjects' rights has been restricted, Article 17 constitutesan additional guarantee for the data subject to verify that their data have been processed lawfully, rather than a general substitute for the direct exercise of their rights. Any restriction must apply only to the extent that, and for as long as, it is necessary and proportionate, and the DPA's decision must be subject to an effective judicial remedy. In Austria, the entire file, including the restricted information, is transmitted on appeal to the Federal Administrative Court, which may amend or overturn the DPA's decision [18].

Finally, some interviewees in both judicial and law enforcement authorities expressed concerns over the mere possibility of requests for the erasure of personal data, as this could tamper with the evidence of the file and the conduct of the investigation. In two Member States, interviewees declared that any requests to erase data were automatically denied.

> **From the moment an investigation is running, given that it's confidential, there is no reason to disclose information about the investigation, including personal data. So during the investigation, there is no reason to give access to personal data. We systematically refuse. This can be more easily accepted once the case is closed. Then we give access.**
>
> *A DPO at a judicial authority*

FRA interviews outlined some inconsistencies in how law enforcement and judicial authorities manage data subjects' rights. While awareness of these rights is high, their practical enforcement varies, with different roles attributed to DPOs and operational staff across Member States. Some DPOs centralise requests to ensure consistency, yet others defer entirely to operational teams or limit their role to advisory support. Operational staff, meanwhile, often lack direct involvement, with many reporting few or no requests, suggesting low public awareness of LED rights.

FRA interviews highlighted significant practical challenges. The identification hurdles mentioned by some interviewees (whereby verifying requesters' identities delays their responses) can put them at risk of non-compliance with LED timelines. In addition, the lack of clarity on the rules regulating restrictions can lead to ad hoc refusals. While some promising practices demonstrate how structured processes can improve transparency and legality, some interviews seemed to highlight more systemic issues (e.g. authorities automatically denying erasure requests).

1.2.3. Competent authorities investigated by the data protection authority

The LED mandates DPAs with supervisory and investigatory powers to verify the correct implementation of the directive by competent authorities (see box ' DPAs' investigation competence and investigatory powers'), with a notable exemption for judicial authorities, as stated in Article 45(2).

DPAs' investigation competence and investigatory powers

Article 45: Competence

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on it, in accordance with this directive on the territory of its own Member State.

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

Article 46: Tasks

1. Each Member State shall provide, on its territory, for each supervisory authority to:

(a) monitor and enforce the application of the provisions adopted pursuant to this directive and its implementing measures;

[…]

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, 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;

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

[…]

(i) conduct investigations on the application of this directive, including on the basis of information received from another supervisory authority or other public authority;

Article 47: Powers

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

All interviewees working in law enforcement and the judicial authorities (operational staff and DPOs alike) were asked whether they were aware of any investigation conducted by the DPA in their authority. Among the DPOs working in law enforcement authorities, some stated that they were investigated once, and one DPO stated that they were investigated several times. Two reported that they had only experienced GDPR-related investigations, and three stated that they had never been investigated. Among the 14 DPOs working in prosecutors' offices, most reported that their office underwent one or several investigations, three did not recall any investigation (although one insisted that they were not exempt from any supervision by the national DPA) and one recalled that the prosecutor's office was exempt from DPA supervision.

Most DPOs working in law enforcement indicated that their authority was regularly inspected (or audited) by the DPA. Some interviewees working in law enforcement authorities indicated that they believe that the DPA has no authority to investigate them. One interviewee from a law enforcement authority, for example, stated that 'the national DPA is not responsible for them, since police matters are state affairs'.

Among the 43 operational agents interviewed who were working in law enforcement, one third of them (from 10 Member States) were generally aware of their authority being investigated or audited. Two of these (from the same Member State but from two different entities) indicated that they actively participated in the inspections. Finally, among the interviewees working as prosecutors or judges, one prosecutor indicated that they believed that the prosecutor's office had undergone an investigation by the DPA, but they were unsure. Of the remaining interviewees, several were not aware of any investigation, a few stated that they had never been investigated, some were aware of complaints by data subjects to the DPA (without clarifying whether these led to investigations) and some of them stated that judicial authorities are exempt from the DPA's

supervision.

Most DPOs (in both law enforcement and judicial authorities) insisted that they had a very good relationship with the DPA, with some of them indicating that they actively participated in the inspections or investigations (e.g. accompanying the DPA agents). The good cooperation with, and crucial role of, DPOs was also highlighted by several respondents from DPAs (see Section 3.2.2).

However, among DPOs, a few of them (working in law enforcement) who were involved in inspections conducted by the DPA did report some communication challenges. These were related to what they considered to be a theoretical perspective of data processing from the DPA or to a time-consuming necessity 'to prepare the DPA's employees for the task, especially if the DPA sends young and inexperienced employees who do not know or understand the specific systems the police use'.

In judicial authorities, one public prosecutor and a few DPOs raised concerns regarding the supervision powers given to the DPA (especially when it comes to providing access to the files). In their view, a conflict between data protection and criminal procedural legislation may emerge when faced with investigations by the DPA.

> **It's simply difficult for us to always explain to the data protection authority how we work and why this is necessary and to recognise the differences, that we have to work differently and that the data protection regime, the LED regime, doesn't really suit us in this form, that's difficult.**
>
> *A public prosecutor at a judicial authority*

> **The main law regulating criminal proceedings is the procedural criminal code, which governs all actions and appears to preclude the need for involvement of any other regulation. The secrecy of pretrial information must be protected, and the requirement to disclose pretrial investigation information to the DPA conflicts with the provisions of the procedural criminal code.**

A DPO at a judicial authority

Two operational staff from one Member State working in law enforcement who actively participated in an inspection by a DPA indicated that the inspection proved to be demanding in terms of workload. One of these interviewees stated that requests from the DPA included statistics and data that 'they would not collect' and the second interviewee stated that the requests included 'written information, technical information, a presentation on procedures and processes, as well as demonstrations and logs'. The first interviewee clarified that all of the shortcomings were addressed; however, the second interviewee stated that this inspection proved to be particularly stressful, notably because of the difficulty to 'understand each other'; in the view of the interviewee, the DPA agents' understanding of their work was too 'theoretical' and 'disconnected from day-to-day law enforcement'.

> **The national DPAs … continue to enforce rules whose meaning has since shifted through interpretation.**
>
> *An officer at a law enforcement authority*

Some DPOs and one operational staff member working in law enforcement clarified that they consider these inspections and investigations to be very constructive. They have added value beyond the objective of the inspection, as DPAs use this time to provide them with advice. The corrective measures mentioned by interviewees include changing internal practices, issuing new guidelines, conducting targeted training sessions and communicating directly with the individual office, their entire unit or similar units. Several DPOs and a few operational agents clarified that specific procedures govern these inspections, including follow-up steps to be implemented by the DPO office to correct any misprocessing detected and implementing measures to identify and prevent the reoccurrence of such mismanagement. Interestingly, in one case, another operational staff member working in law enforcement (more specifically in the legal department in charge of legal surveillance through cameras and drones) not only was aware of the inspections by the DPA, but believed that these are 'not as frequent as they should be'.

In one Member State, the DPA has developed guidelines to detail the procedure of investigating competent authorities. In this guidance, the DPA is instructed not to address the DPO, in order to protect its independence. This was viewed positively by the DPO staff interviewed by FRA.

> **The [national] DPA has published a kind of guidance on their cooperation with the DPO. It explicitly states that in the case of specific enforcement requests, the DPO will be informed, but will be kept at a greater distance, because the DPO must remain independent if the DPA and the data controller communicate with each other. We are very pleased with this, because otherwise, it puts you in a difficult position – if there is a formal request for information and the organisation wants to respond in a certain way, but you may have a different perspective or different information, you don't want to be caught in the middle. Additionally, if you have a different perspective or different information that requires you to act, you can do so accordingly.**
>
> *A DPO at a judicial authority*

Despite the LED's clear mandate when it comes to DPAs' supervision over competent authorities, as set out in Articles 45–47 of the LED, the FRA interviews with staff working in law enforcement and judicial authorities revealed uneven (and sometimes contested) DPA supervision. While most DPOs reported regular inspections (and often described them as constructive), some operational staff assume that their authority is exempt from any DPA supervision. Several competent authorities' operational staff insisted on what they perceived as a lack of institutional knowledge of law enforcement systems from DPAs and complained about resource-intensive requests. However, positive findings (e.g. collaborative DPA–DPO relationships and post-inspection improvements) show how proactive engagement can bridge gaps. However, systemic reform is needed to avoid supervision being perceived as burdensome rather than a safeguard for lawful processing. The LED's accountability framework depends on effective, trusted enforcement.

1.3. Seeking advice and cooperation

The LED provides that data protection experts should be consulted by staff working in law enforcement and judicial authorities when these staff require advice and guidance, both internally (DPOs) and externally (DPAs).

Article 34 of the LED provides that DPOs should 'inform and advise the controller and the employees who carry out processing of their obligations' and, specifically when it comes to DPIAs, they should 'provide advice where requested as regards the data protection impact assessment and monitor its performance'.

Article 46(1) of the LED provides that DPAs should 'promote the awareness of controllers and processors of their obligations under this directive' and 'provide advice on the processing operations referred to in Article 28'. To do so, Article 47 clarifies that DPAs should have 'effective advisory powers to advise the controller'. Article 28 refers to specific cases when competent authorities should consult their DPA. These cases concern the processing of data which 'will form part of a new filing system to be created' if one of the following two conditions apply: (1) a DPIA has shown that the processing would result in a high risk to the rights and freedoms of individuals in the absence of measures taken by the controller to mitigate the risk or (2) the type of processing (in particular when using new technologies, mechanisms or procedures) involves a high risk to the rights and freedoms of individuals.

1.3.1. Seeking and receiving advice

Among 43 operational staff working in law enforcement authorities, just over half (23) reported that they experience good and fruitful cooperation with their DPOs and consult them on a regular basis. By contrast, 12 operational staff working in law enforcement authorities claimed that they are not in contact with their DPO at all or are not aware of consultations. One respondent observed that the DPO is not visible in their daily work, and the interviewee stated that they are not aware whether the DPO operates at the unit level or as a centralised function. When necessary, the interviewee contacts the lead investigator or the legal department of the police. On the other hand, another operational agent from the same Member State noted that they consult their institution's DPO and described the DPO as responsive and understanding of their operational needs. Furthermore, one respondent noted that interactions with the DPO are highly hierarchical and conducted in writing through the chain of command. Another noted that they are allowed to contact the DPO only through a superior.

> **We have a very good relationship with the data protection office. And indeed, there would be certain things that, of course, we would look for advice on. And you know, indeed, when I want to talk about even things like recent judgments, it wouldn't be just a DPO, it would also be legal, our internal legal section as well.**
>
> *An officer at a law enforcement authority*

Two operational staff working in law enforcement authorities explicitly mentioned structured consultation between data protection experts and operational staff, notably through discussions

with police services when amending regulations to specify a new processing purpose or through discussions with end users during system development to determine which data elements are truly essential. One interviewee noted that, while they consult their DPOs, there is a misalignment between the understanding of the organisation's data protection experts and that of its operational personnel (see the following quote).

> **"What also characterises these challenges in applying the LED is that we often have, on one hand, the operational law enforcement officer understanding and expertise about what type of data processing the police operationally would need. And on the other hand, we have the data protection experts' and related understanding of what the requirements are for processing according to the GDPR/LED or in national law. Somehow these two don't align. There ought to be some kind of 'dictionary' or interpreter in between or the list of data protection measures (toolkit) typically used to avoid certain types of problems in processing. When we ask the data protection side … whether such processing is allowed or possible, the default answer tends to be: 'No, it isn't.' But no guidance or advice or toolkit is given on how to modify data processing to fulfil properly the GDPR and/or LED requirements.**
>
> *An officer at a law enforcement authority*

Interviewees from law enforcement were also asked if there are any cases in which it is mandatory to consult DPOs. Eleven of them explicitly reported that they are required to consult DPOs, and 16 noted that it is not mandatory (or they are not aware of it being mandatory). Nevertheless, operational agents continue to refer to DPOs' guidance, even if it is not mandatory. One interviewee noted that, while the advice of the DPO is not legally binding, they have never seen implementation proceed without the agreement of the DPO.

As for seeking advice from DPAs, some interviewees working in competent authorities noted that contact with the DPA is facilitated by DPOs in their institutions. One operational staff member working in a law enforcement authority wished that the DPA was involved at an earlier stage in assessing the police's actions, rather than only providing guidance after the development of products, which the police would then have to implement. Several interviewees claimed that they have never sought advice from their DPA, and most respondents indicated that they are not aware or have they made use of guidelines issued by the EDPB or their DPA.

> **Basically, guidelines are the basis of our work, because of course we stick to it. It provides a clear direction, how we work, how we handle data. If we didn't have that, then everyone would do what he believes is right. There has to be a clear line and it is also a certainty of action for each individual, because he knows exactly, if I stick to that, then I'm not doing anything wrong. Yes, that is very important, that such a thing exists.**
>
> *An officer at a law enforcement authority*

In contrast, within judicial authorities, most interviewees indicated that they do not consult their DPOs, and there are no mandatory requirements obliging them to do so. Only some of them mentioned some consultations that they participated in, and only one interviewee noted that there are cases when they are obliged to consult the DPO. The same patterns are visible in cooperation with DPAs – most interviewees claimed that they do not seek advice from DPAs or are not aware of such cooperation. No interviewees referred to other types of consultations, such as external legal or IT experts, but some of the DPOs working in the judicial authorities who were interviewed claimed that they are sometimes contacted by prosecutors.

When asked about their experiences with DPIAs, a majority of interviewees from law enforcement noted that they do not have direct experience with the process and that they consider this as something that the DPOs would be involved in. Operational staff interviewed by FRA that indicated they were involved in DPIAs reported having an overall good experience in this process. Among judicial authorities, the majority of respondents stated that they were either unaware of whether a DPIA was conducted, had never conducted a DPIA or had no experience in this regard. Some of them had never heard of the term 'DPIA' or were unfamiliar with what it was.

Some interviewees in law enforcement reported challenges when it comes to implementing DPIAs. A few operational agents described DPIAs as being 'unclear', 'formalistic', 'burdensome' or 'overly rigid' and lamented the lack of methodical guidance. One interviewee described that, while in the past DPOs had participated in the development of data processing, a change in the law requiring no conflict of interest between the DPOs and the police resulted in the DPO becoming extremely cautious, providing minimal consulting support to avoid conflicts of interest. The interviewee's state police force responded to this problem by introducing 'operational data protection' services to obtain the advisory support that official DPOs were now refusing to provide.

Despite this, as reported under Section 1.1.4, according to some DPOs working in law enforcement, police officers generally focus on the operational benefits and overlook matters of

compliance or data protection. Nevertheless, for a majority of DPOs, education and training are key: police officers need to receive more guidance and assistance when it comes to data protection.

The FRA interviews reveal a fragmented approach to consulting DPOs and DPAs, with law enforcement and judicial authorities facing distinct challenges. Many operational staff in law enforcement report positive, regular engagement with DPOs, valuing their responsiveness and operational awareness, but others described hierarchical barriers and even sometimes a complete lack of interaction, revealing inconsistent integration of data protection advice. A cultural divide persists between operational needs and compliance expectations, with some practitioners still perceiving DPOs as obstructionist, despite general improvements. Judicial authorities exhibited lower engagement, with most interviewees reporting no DPO consultations, often reflecting assumptions of exemption under Article 45(2) of the LED. DPA interactions with competent authorities appeared to be limited, with some practitioners mistrusting DPAs' supportive role or being unaware of their guidance. This knowledge deficit extends to DPIAs, in relation to which law enforcement staff often defer to DPOs but criticise the process as overly rigid or unclear, while judicial actors display near-total unfamiliarity, with some of them never having heard the term. Advice seeking is key to avoiding compliance being viewed as an obstacle rather than a safeguard, yet FRA findings show that DPOs' and DPAs' expertise remain underutilised.

1.3.2. Cooperation among competent authorities

To support harmonised and effective implementation of the LED, both the European Commission and the European Union Agency for Law Enforcement Cooperation (Europol) have established networks so that DPOs of competent authorities can meet, exchange experiences and practices and discuss challenges or doubts. The European Commission's DPO Network is made up of DPOs from both law enforcement and judicial authorities, while the Europol Data Protection Experts Network (EDEN) is made up of DPOs only from law enforcement authorities. In the interviews, DPOs in law enforcement and judicial authorities were asked whether they were aware of such networks at the European and national levels and about their engagement in these networks.

While most of the DPOs interviewed by FRA confirmed that they were aware of EU networks – with some of them also confirming that they do participate in these networks – only some of them indicated that they cooperated at the national level. Some DPOs regretted the absence of forums at the national level to have discussions among experts. One interviewee, however, noted that, although no formalised network exists, the professionals in the field know each other through shared training experiences and keep collegial communications. In Member States that do have a network of experts at the national level, interviewees indicated that, given the specificity of the topic, such networks are indeed very useful (see box 'Promising practice: national network established among DPOs in the competent authorities (Belgium and Denmark)').

Promising practice: national network established among DPOs in the competent authorities (Belgium and Denmark)

The Belgian Federal Police organises regular internal network meetings that bring staff with a DPO function together. These meetings provide a forum to discuss relevant updates (e.g. concerning legislation or internal guidelines) and exchange good practices and provide a space for participants to raise questions. According to interviewees, these meetings also provide a useful moment to ensure that there is a shared understanding of key interpretations among staff and to discuss cases or projects involving several services.

The DPOs from the law enforcement authorities in Denmark are part of a national network. The Danish network has the advantage that all members refer to the same legislation and legal tradition. Discussions cover exceptions to the rights of data subjects or the use of AI and cloud solutions, for instance. Participants also have the opportunity to develop and draft memos on specific questions (e.g. on the differentiation between the LED and the GDPR), which are then shared among members of the network.

Source: FRA interviews in Belgium and Denmark.

Concerning their relationship with national DPAs, the views of the DPOs in the law enforcement and judicial authorities were contrasting. Several of them observed good cooperation with national DPAs during investigations that the authority conducts. In a few Member States, however, DPOs expressed frustration and a rather negative opinion, as they complained about their national DPA not replying when contacted, not providing training or information adapted to the work conducted by law enforcement authorities or not providing adequate support that was tailored to their work. One interviewee noted that their DPA is reluctant to provide definitive interpretations of data protection law transposing the LED, in order to retain flexibility during enforcement actions.

While EU-level networks are positively recognised as fostering cross-border dialogue, the FRA research reveals uneven and underdeveloped cooperation among law enforcement and judicial authorities at the national level. Belgium and Denmark's structured national networks (facilitating shared interpretations, case discussions and guideline development) demonstrate the value of systematic exchange. Relationships with national DPAs are mixed, ranging from constructive partnerships to frustration over a perceived lack of tailored guidance or a reluctance to clarify LED interpretations. This lack of cooperation is often a missed opportunity for harmonised, effective LED implementation.

2. Providing expertise: the key role of data protection officers

Article 32 of the LED states that all competent authorities shall designate a DPO; however, it is not mandatory for courts and other judicial authorities when acting in their judicial capacity. Article 33 introduces a broad mandate for the DPO, requiring the DPO's involvement 'in all issues which relate to the protection of personal data'. Article 34 of the LED (see box 'Article 34: tasks of the DPO') sets out a list of tasks that represent the minimum that DPOs should be doing in competent authorities.

Article 34: tasks of the DPO

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this directive and to other Union or Member State data protection provisions;

(b) to monitor compliance with this directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 27;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 28, and to consult, where appropriate, with regard to any other matter.

Despite the limited availability and awareness of practical guidance and measures to apply the LED requirements in operational staff's daily work (as identified in the first chapter of this report), most DPOs expressed that they had witnessed improvements in both the awareness of staff of data protection and the recognition of them as supportive co-workers. Several of them also raised the positive impact on their work of the national law transposing the LED, in terms of both recognition by colleagues and useful tools, notably the DPIA. This confirms what the European Commission identified in its first report published in 2022: 'This [the designation of DPOs] has

resulted in competent authorities becoming more aware of their data protection obligations as well as having a positive impact on competent authorities' compliance with data protection rules' [19] .

However, a number of issues still remain: many DPOs pointed out that they are lacking human resources to efficiently conduct their tasks. In parallel, several DPOs raised the fact that they are lacking appropriate tools, namely IT tools and expertise, LED-specific guidance and criteria (e.g. in relation to DPIAs, which were referred to by several DPOs as a useful tool) and training material adapted to law enforcement. Finally, some of them indicated that they still do not feel recognised, either by the staff or by their authority's management. This chapter will discuss these challenges in detail.

Importantly, and without ruling out the improvements identified by several DPOs as noted earlier, FRA's research did show some level of discrepancy between this positive development identified by DPOs (particularly the positive impact of awareness-raising activities, such as newsletters and guidance) and the feedback FRA received from operational staff working in law enforcement authorities and interviewed by FRA. While several interviewees were aware of (and stated that they had used) guidance that was developed by their DPO, by the national DPA or, even in one case, by the EDPB, in most cases, the operational agents interviewed by FRA were unaware of any guidance on specific data protection requirements or stated that, while they believed that some guidance existed, they had not seen or read it.

Among those who were aware of the existence of guidelines, most praised the added value of DPOs and of their work. Some interviewees working as operational staff in law enforcement had some less positive comments, referring to there being too many data protection guidelines or these being too complex or consisting 'mainly of a brief description of the provisions of the legal instrument'.

> **The colleagues from the data protection department are very active and are constantly guiding us. They actively publish information, awareness and guidance materials. Also, they have standardised certain activities (e.g. answers regarding access requests) all made available in the internal communication network for all police units.**
>
> *An officer at a law enforcement authority*

Promising practice: internal assessment on data protection

work conducted by the police's audit office (Sweden)

In August 2024, the Swedish police conducted their own assessment of how effectively the police lead, steer and control their data protection work. The objective of the assessment was to evaluate whether the police authority has an effective and appropriate governance structure for and control over managing data protection obligations. The evaluation notably identified that, while overall governance is mostly effective, there are notable areas needing improvement, namely:

- the control and follow-up of data protection work vary and are not sufficiently effective, leading to uncertainty about compliance and risking deficiencies in personal data handling going unnoticed or unaddressed;
- internal guidelines on data protection are perceived as too extensive and complex, with the organisation asking for more practical support documents;
- the networks meant to coordinate data protection work across the authority do not function as intended, which weakens steering and communication.

One of the key sections in the audit addresses the DPO function, identifying that, in practice, DPOs have spent much of their time on tasks other than auditing and compliance reviews due to internal requirements and resource shortages within the legal department.

The audit resulted in four key recommendations:

1. clarify guidelines and support documents;
2. improve internal coordination and governance forums;
3. ensure adequate control and follow-up of processing;
4. strengthen conditions for DPOs.

Finally, the report includes an action plan adopted by the authority's leadership that maps out how these recommendations will be addressed within specific units and timelines.

Source: Sweden, Police, Review of the Swedish Police Authority's Governance and Management of Data Protection Work (Granskning av olismyndighweihting tooletens ledning och styrning av dataskyddsarbetet), August 2024.

2.1. Resources

Article 33(2) of the LED provides that data controllers shall support their DPO by 'providing

resources necessary to carry out [their] tasks and access to personal data and processing operations, and to maintain [their] expert knowledge'.

FRA interviewed 42 DPOs: 28 in law enforcement (covering structures belonging to both the police and interior ministries) and 14 in prosecutors' offices. All but two DPOs indicated that they were working for one authority. One DPO working in law enforcement indicated that they were acting as the single point of contact for several law enforcement authorities on international cooperation, and one DPO working in a judicial authority indicated that they had been appointed for several 'prosecution units'. A large majority of them indicated that they had indefinite contracts, whereas only a few had fixed-term contracts.

Most DPOs clarified that they either work alone or are supported by one or two assistants and/or legal experts. Several work with a team ranging from four to seven people, and two work in large teams (of 13 and 15 people). As a general rule, DPOs working in judicial authorities mainly work alone. Despite these differences, almost all of the DPOs interviewed were either dissatisfied or moderately satisfied, indicating that their current situation was fine, but that additional resources would allow them to do more or be more efficient, given the level of resources available in their organisation. Some of them indicated that they were satisfied with the current resources allocated to them to perform their work; of these, two work alone in a judicial authority and three work in a team in a law enforcement authority. As an example, one interviewee indicated that they worked alone and part-time as a DPO but had '1300 hours of overtime'. A large majority of DPOs noticed a serious increase in workload and, as a result, some of them indicated that they had to prioritise their work, generally prioritising either specific requests that were mandatory or had clear deadlines defined in law or requests that had a political dimension and therefore needed to be treated as a priority. In general, DPOs who were 'moderately satisfied' complained of the fact that they did not have any time left to conduct deeper and/or proactive work within their authority, as their time only allowed them to focus on day-to-day tasks. Finally, some of them (all working in law enforcement authorities) stated that they are lacking technological knowledge and that they would welcome the recruitment of IT specialists.

> **We are constantly working in emergency mode.**
>
> *A DPO at a law enforcement authority*

> **Because the staff of the police is much more aware, the data protection office receives a lot more requests about different issues in connection with data protection, as well as more requests for staff training.**

A DPO at a law enforcement authority

Similar to FRA's findings in its analysis of DPAs' challenges in implementing the GDPR [20], the shortage of resources has a multilayered impact on the work conducted by data protection officials. Notably, some DPOs emphasised that the lack of human resources prevents them from conducting more internal training or providing targeted guidance, which they see as a crucial element for ensuring effective implementation of data protection requirements within their authority. A few also mentioned that, although they were aware of the necessity to conduct regular reviews of the need to keep data and the obligation to delete, the lack of resources and subsequent lack of time was preventing them from doing so on a consistent basis.

The fact that competent authorities should have a full office dedicated to data protection (and not only one DPO) was also highlighted by some DPAs' experts interviewed by FRA.

Some interviewees also mentioned that they face recruitment difficulties: competent authorities receive too few applications for positions within the DPO's office, and very often applicants do not meet the required expertise. One interviewee indicated, as an example, that the recruitment of an assistant DPO took several years and many attempts.

> **[More superficial controls] are the most serious consequence [of the DPO's insufficient resources]. Controls in the classic sense, in the sense of an audit, where you really go into depth [are now difficult] – because of course I check things, when I receive a complaint from an employee or someone, I look at what's behind it. But I can't go into that in depth and analyse it from the ground up. It's just not possible because of the lack of resources.**

A DPO at an interior ministry

Several DPOs indicated that their institution (be it the police, the prosecutor's office or the interior ministry) conducted an evaluation and/or restructuring of data protection resources. Some indicated that either the DPO function or a dedicated DPO office was set up after the entry into force of the national law transposing the LED (four in judicial authorities and nine in law enforcement authorities). Although most were positive about this, one interviewee indicated that, despite the initial restructuring prior to the adoption of the national law that led to the establishment of a dedicated data protection office consisting of 20 people, the office has now been reduced to five people.

Some DPOs indicated that Schengen evaluations had some positive impacts in the strengthening of their office, namely by supporting their stand regarding the lack of human resources, by reinforcing the importance of the independence of the DPO or by pushing the initiation of audits (internal or external) and subsequently implementing recommended measures.

Almost all of the DPOs interviewed insisted that they are facing heavy workloads. More than half of them cannot focus on tasks related to data protection and have other tasks to do. Among the 42 DPOs interviewed, 19 stated that they are full-time DPOs. While DPOs working in law enforcement authorities include both full- and part-time DPOs (eight are full-time DPOs and eight work on other tasks), most DPOs working in a prosecutor's office work on other tasks. All DPOs working in interior ministries are full-time DPOs. In most cases, additional tasks are related to other legal questions. A few of them conduct IT or cybersecurity-related tasks, and one of them stated that they are also the archivist of the authority (dedicating only 10 % of their time to DPO-related tasks).

Despite the workload, several DPOs pointed to some requirements of the LED as proving to be helpful in supporting their work. The DPIA was notably referred to as very useful for identifying at a very early stage any potential misprocessing of data that, eventually, would have caused more time-consuming and difficult issues for the authority as a whole and for their function in particular. Even though DPIAs were often referred to as being a complex and challenging exercise, the ultimate benefits of conducting timely, detailed and appropriate DPIAs were highlighted by several interviewees. Most of them, however, indicated that they mainly have to navigate the process of the creation of a DPIA template alone and that detailed and case-specific guidance should be developed at the EU or national level to support and guide them.

> **"The DPIA is not a paper tiger, it is useful and regularly used.**
>
> *A DPO at a law enforcement authority*

> **We've tried certain prefabricated [DPIA] forms or even programmes on offer, but they were not suitable. So now we always customise these DPIAs, depending on the application. But this takes a long time, sometimes an extremely long time.**
>
> *A DPO at an interior ministry*

Promising practice: systemising the assessment of the need to conduct a DPIA (the Netherlands)

In the Netherlands, more than 250 DPIAs have been carried out by the Public Prosecution Service (Openbaar Ministerie). The necessity for a DPIA is assessed using QuickScan, a weighting tool introduced in 2018–2019. A list of assessment criteria supports data controllers in assessing cases coherently and objectively to determine if a DPIA would not be necessary, would be useful or is mandatory (when a certain threshold score is exceeded). If data processing is considered to have a higher risk, a DPIA has to be conducted. This assessment takes more time and requires a more in-depth analysis. To determine if this step must be taken, it has to be clear when data processing constitutes a high risk. It can be ambiguous in practice to determine what is considered 'high risk'. Lists were made to provide indications of when it is necessary to conduct a DPIA, but considering that not all employees have in-depth knowledge of privacy laws, it was considered helpful to introduce a weighting tool. The tool is able to conclude which element in data processing constitutes a risk and thus needs to be subject to an in-depth assessment. Not all types of processing require an in-depth analysis, but certain elements of processing and/or several elements together could. The scoring criteria indicate the steps that need to be taken, if no more action needs to be taken or if an in-depth analysis is needed in order to properly assess the risk(s) of data processing.

Source: Ministry of Interior and Kingdom Relations (Ministerie van Binnenlandse Zaken en Koninksrijkrelaties), *Guidance document Pre-scan DPIA. Version 2.0* (Handreiking Pre-scan DPIA. Versie 2.0), 2024.

FRA research reveals important resource constraints that can undermine DPOs' ability to fulfil their mandate. While most of the DPOs interviewed by FRA indicated that they have indefinite

contracts, they operate with inadequate staffing (often working alone or with minimal support) and face rising workloads that force reactive, firefighting approaches rather than proactive compliance. Law enforcement DPOs fare slightly better than judicial counterparts, yet both groups report dissatisfaction, citing insufficient time for training, audits or strategic initiatives. The recruitment crisis, exacerbated by public-sector pay gaps and LED-specific expertise shortages, further hampers capacity, with some vacancies remaining unfilled for years. However, DPOs are key to the effective and comprehensive enforcement of the LED.

2.2. Training and expertise

Article 32(2) of the LED provides that 'the data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law'.

DPOs in competent authorities mainly indicated that they have legal backgrounds (some did not clarify their background, and only one DPO (working in a judicial authority) had an IT profile). Recital 63 of the LED clarifies that a DPO can be 'a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field'. Indeed, almost all of them indicated that they were already working within the authority and were appointed as DPO either based on personal interest or because they worked on a related topic (some of them were recruited after 2018 directly as DPOs). A few indicated that they were part of the team that prepared for the transposition and/or entry into force of the national law transposing the LED and, therefore, already had substantial knowledge.

Many of the DPOs interviewed reported having not been provided with specific LED training. A recurring complaint relates to the fact that only GDPR-based training is available, but that this training is not adequate for data processing within law enforcement or judicial authorities. As a result, several DPOs indicated that they taught themselves and continue to train themselves regularly. A few DPOs also mentioned the meetings organised by the European Commission's DPO Network or the Europol Data Protection Experts Network (EDEN) as 'a source of training'. Several mentioned that they learned a lot by attending these meetings and that exchanging experiences with peers working in similar situations is very helpful (see Section 1.3.2). The ways that interviewees indicated that they self-train include desk research, consulting guidance, memos and attending external lectures. However, regarding external training or conferences, many interviewees reported that these generally focused on the GDPR and not on the LED. A few interviewees mentioned that they attended training organised by Interpol, which proved useful when it comes to cases related to concrete law enforcement, but was not always relevant given that the legal framework used as a reference is different.

> **One area where we believe we are lagging behind is that we have not received the necessary training. The training we have received is very basic. Our knowledge of the directive and the regulation is derived from our own experience and study.**

A DPO at a law enforcement authority

DPOs working in judicial authorities also indicated that there was an absence of training that was adapted to the specificities of the legal framework applying to their colleagues and to their work.

> **[B]ut we have the LED now for three years or so, and I have been working in this data protection regime for about three years or so, and there has not yet been a specific training event, no handout, no information material; the judiciary has obviously had to work this out on its own, and that is my biggest challenge. So, it would have been better, from the beginning on … to actually address the issue, to network, to get many stakeholders, perhaps international ones too, on board and to manage it centrally. That would have been easier than having to work it out yourself, because for me and for many others it's trial and error and you try it and that's actually the issue.**

A DPO at a judicial authority

Promising practice: training through simulation exercises (France)

In France, to train data controllers on potential practical issues, a competent authority under the LED simulated an audit by the DPA on a processing operation that presented certain difficulties. To avoid positioning itself as an enforcer, the competent authority proposed a simulation in collaboration with the teams responsible for designing and managing the data processing operation. During

this exercise, the competent authority examined the data and its accuracy, retention periods and so forth. The DPO considers this a good practice, as it allowed improvements to be made, helped raise awareness of the regulations and enhanced the visibility of the DPO's office and its role.

Source: Interview in France.

Finally, a few interviewees in the DPAs raised as an issue the fact that some DPOs were nominated when they did not have the relevant expertise, making the relationship difficult. One interviewee from a DPA stated that some DPOs were appointed as a mere 'formality' (see Section 3.2.2). DPA experts also mentioned the lack of appropriate training and education for DPOs, with one expert explaining that they (the DPA experts) 'do the education of the DPOs', which, in the view of the interviewee, should not be their responsibility. While a majority of them praised the key role that DPOs are playing within law enforcement and judicial authorities to ensure effective implementation of the LED principles, some interviewees raised concerns about, on one side, the expertise and understanding of LED legal principles and, on the other side, the exact scope and tasks of their role.

> **Sometimes it seems that they do not have enough understanding of what their mandate is and what they have to do, because most often, they appoint as a data protection officer someone who has to combine these positions, well, unless you count some very large organisations, but insofar as they are staff members and they are also probably state officials, special service officials, they have, of course, also this hierarchical command and subordination, which perhaps does not always promote their independence and autonomy in carrying out their tasks.**
>
> *An officer at a DPA*

> **DPOs in public authorities fail to comply with their duty and do not have the appropriate knowledge. Our DPA in fact frequently ends up performing DPOs' duties just because public administration DPOs say the topic is complex and they don't understand it and they don't perform their duties as they should.**
>
> *An officer at a DPA*

The interviews reveal critical gaps in the training and expertise of DPOs in law enforcement and judicial authorities, despite the LED's requirement for specialised knowledge (Article 32(2)). While most DPOs transitioned from existing roles (often with legal backgrounds), their preparation has largely been self-directed, with formal LED training scarce or non-existent. Many rely on GDPR-focused courses, which fail to address law enforcement specifics, or EU-level DPO networks for practical insights. However, despite the significant efforts of DPOs to ensure expertise and efficiency, the absence of tailored programmes can undermine operational staff's confidence and consistency in applying the LED.

2.3. Data protection officers' relationships and recognition within the organisation

Recital 63 of the LED clarifies that 'data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law'.

When asked about how their role is perceived by their colleagues in the authority, several of the DPOs indicated that their role was initially perceived negatively, but through continuous education and information this perception has changed.

> **[Y]our role in the organisation, your relationship with the colleagues, is one of the most essential things as DPO. In the police context, people are sceptical to everything data protection, something that is hindering them, something that is stopping them from doing what they want … But I do have to say that one of the things I'm actually most proud of here is that I managed to install data protection culture in the sense that people are now thinking about data protection … By being able to give solutions to colleagues, they perceive my role as more positive, it's an evolution. It's something that takes time and you must convince them of it. But it is working.**
>
> *A DPO at a law enforcement authority*

The interviews show that, when DPOs are located at the top of the hierarchy, they generally report that their role is perceived positively by the organisation and that the relationship with the hierarchy is fluid and easy. By contrast, DPOs who are not positioned at the managerial level say that they perceive some resistance from their colleagues when it comes to recalling appropriate data protection procedures to be followed, either because they are seen to be precluding the efficiency of their work or because they are considered internal auditors or controllers. However, in both cases, most DPOs reported having witnessed a positive evolution in the way they are perceived within their organisation, and several of them stated that they actively worked to reinforce cooperation and build trust to develop a positive attitude towards data protection.

A recurring complaint from DPOs relates to the false perceptions that some colleagues have regarding their job: for example, one DPO located at the top level and who considers that his job is respected complained that 'a disadvantage is that everything is taken as an instruction, while giving instructions is not the job of a DPO'. Indeed, almost all of the DPOs interviewed believe that their role is almost exclusively of an advisory nature when it comes to their relationship with operational agents acting as data controllers. Several of them complained that operational agents sometimes expect them to conduct assessments or take decisions on their behalf.

Despite this, most DPOs emphasised that they found their colleagues to be quite cooperative and solution oriented when a concrete data protection issue or challenge was identified. Indeed, most operational agents interviewed by FRA stated that they consult their DPO not on a systematic basis, but on a case-by-case basis. From the controllers' perspective, some interviewees showed a clear understanding that, as operational or investigating agents, they must always be prepared to explain and justify their actions and that the DPO is a key ally to ensure this.

> **I quickly understood that we would make more progress by working collaboratively rather than having the DPO position themselves as a supervisory body. We already have so much work that the control phase will have to come later.**
>
> *A DPO at an interior ministry*

Finally, several operational agents interviewed by FRA showed a lack of awareness of tools developed by their DPOs. While all DPOs state they provide regular oral guidance to their colleagues when requested, several of them also referred to written guidelines. A few of them stated that these are published on their intranet, and one of them stated that they regularly send guidance to all staff per email. However, when asked whether they know of internal guidelines to address specific data protection requirements, most operational agents did not know of any written guidelines. This lack of awareness of the rules is confirmed by the fact that some DPOs knew of cases in which they should have been consulted, but were not.

Only one DPO interviewee flagged that they lacked effective independence within their organisation, stating that the issues they report can be blocked by their management. Although the interviewee noted that, after the adoption of the LED, this situation has improved from a formal perspective, they stated that, in practice, they still have a lack of independence with regard to their decisions.

Despite being reported by only one DPO, the crucial importance of the independence of DPOs was also emphasised by experts working in DPAs. One interviewee, for instance, highlighted that they do notice a difference in their relationships with DPOs depending on how independent they are from their management (see the following quote).

> **When the data protection officers are not in a subordinate relationship, they have more experience in data protection issues, it's easier to work with them, it's quicker, well, we are more or less on the same page, and they are also able to identify those potential problems internally in advance and perhaps consult with us beforehand to find the right solution to address one or the other issue.**

> *An officer at a DPA*

The interviews reveal a shift in perception, from scepticism to cautious acceptance, of DPOs within law enforcement and judicial authorities. Many DPOs have actively reframed their role, with some of them adopting a 'service provider' approach with the aim of building trust. However, DPOs reported that challenges persist in embedding their role effectively. Operational staff increasingly recognise DPOs as allies in justifying actions, but the awareness of tools (e.g. intranet guidelines and email updates) remains worryingly low, suggesting either communication failures or a lack of interest from operational staff. While DPOs who are positioned higher hierarchically report smoother integration, those at lower levels may still face resistance and be perceived as obstructive 'auditors' rather than enablers of compliance. DPAs' observations confirm this, noting that independent DPOs (free from hierarchical pressure) collaborate more effectively and flag risks proactively, aligning with supervisory expectations.

3. Supervising the Law Enforcement Directive: the views and experiences of data protection authorities

To further assess the practices and challenges involved in implementing the LED framework, FRA conducted interviews with the DPAs of all 27 Member States, which are referred to in the LED as 'supervisory authorities'. The interviews were conducted with officials in the national DPA who were in charge of investigations and complaints related to the LED. While all DPAs responded positively to FRA's request to conduct interviews, not all of the officials interviewed were dedicated experts on the LED. In eight Member States, FRA interviewed representatives of DPAs who indicated that they were not experts on questions related to the national provisions transposing the LED, but that they had worked on related cases or questions. In one case, the person interviewed was working in the international department, and not on LED-related cases.

Article 41 of the LED requires Member States to make sure that 'one or more independent public authorities' are entrusted with the monitoring of the application of the LED's requirements. Their tasks are listed in Article 46 (see box 'Article 46: tasks') and their powers are listed in Article 47 (see Section 3.2). Article 45 of the LED excludes from this supervision 'processing operations of courts when acting in their judicial capacity' and allows Member States to decide on whether to also exclude 'processing operations of other independent judicial authorities when acting in their judicial capacity'. Following the transposition of the LED into national laws, nine Member States decided to exclude 'other judicial authorities' from the supervisory scope of their DPA [21]. This exception seems to have created some confusion among respondents, as some experts in prosecutors' offices who were interviewed by FRA believed that this exception exempted them not only from the supervision of their DPA, but also from the whole scope of the LED – or at least that the national law transposing the LED is subordinate to the national criminal procedural code, which is their main legal reference. This is one of the reasons why those who proved the most difficult to recruit for the interviews were employees of prosecutors' offices (see Annex 1).

Article 46: tasks

1. Each Member State shall provide, on its territory, for each supervisory authority to:

(a) monitor and enforce the application of the provisions adopted pursuant to this directive and its implementing measures;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(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;

(d) promote the awareness of controllers and processors of their obligations under this directive;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, 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;

(g) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this directive;

(i) conduct investigations on the application of this directive, including on the basis of information received from another supervisory authority or other public authority;

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(k) provide advice on the processing operations referred to in Article 28; and

(l) contribute to the activities of the Board.

3.1. Enforcing the Law Enforcement Directive: data protection authorities' dedicated resources and expertise

In a majority of Member States, one supervisory institution is tasked with the supervision of both the GDPR and the LED (in Belgium, the oversight of data processing under the LED is mandated to a separate authority; in Spain, a separate authority is tasked with the supervision of data

processing by judicial authorities; and, in Sweden, the supervision of the police is the responsibility of both the national DPA and another authority). In these Member States, the FRA findings highlight that the Commission's observation that 'the overall increase in the data protection supervisory authorities' staff in recent years does not seem to concern LED-related tasks' [22] is still valid: GDPR-related complaints and investigations represent a very large part of the authority's work and, therefore, resources are largely focused on these. Several interviewees refer to this as a general issue of chronic understaffing. This situation was indeed already highlighted by FRA in its 2023 report related to the implementation of the GDPR [23].

Resources allocated to LED-related issues are generally deemed to be sufficient to respond to complaints (i.e. for the most pressing issues). However, a majority of respondents highlighted that their work would benefit from additional resources, notably in order to:

- conduct regular investigations on their own initiative;
- recruit IT specialists to complement their team;
- prepare for future EU regulations that may fall under their supervision, such as the AI Act, the Regulation Establishing the Entry/Exit System [24] or the Screening Regulation [25].

Many respondents from DPAs highlighted that there are several areas in which the LED applies in parallel with sector-specific EU regulations, for example in the context of large-scale EU information systems (e.g. the SIS Regulation [26], the Regulation Establishing the Entry/Exit System, the Visa Information System Regulation [27] and the Regulation Establishing an Interoperability Framework [28]. This adds further complexity and increases the workload of supervisory authorities. Although the volume of LED-related complaints to the supervisory authorities may not be high [29], the range of tasks under Article 46 of the LED is broad. Beyond handling complaints, supervisory authorities also have responsibilities related to monitoring the application of the national provisions transposing the LED, to raising awareness and providing advice to public institutions (including on legislative measures), to cooperation and mutual assistance with other supervisory authorities, and to prior consultation. Therefore, more thorough and frequent monitoring of law enforcement data processing is needed to ensure effective supervision of the LED. FRA's findings clearly show that the overall scope and importance of the tasks performed by competent authorities that may have LED-related implications clearly indicate a need for increased (and specialised) human resources for DPAs across Member States. Increasing resources would support them in supervising these authorities more frequently and more effectively, including by extending their tasks beyond addressing complaints to conducting regular ad hoc inspections.

> **Despite a significant overall increase in the DPA's office's resources, there is a notable shortage of personnel for LED-related tasks, particularly given the new responsibilities of supervising EU information systems such as SIS, VIS [visa information system], EES [entry/exit system], and ETIAS [European travel information and authorisation system], which require substantial resources … LED-related tasks are under-resourced, necessitating strict prioritisation. Inspections, an essential aspect of the work, have been particularly impacted. The number of inspections conducted has decreased significantly, negatively affecting operations' efficiency and effectiveness. With sufficient staff, it would be possible to conduct more inspections, including more extensive monitoring of the information systems used by security authorities.**
>
> *An officer at a DPA*

Most interviewees in these institutions, from 20 Member States, declared that the dual enforcement of both the GDPR and the LED by one institution was a strength rather than a limitation, as it provides comprehensive and nuanced data protection oversight and it enables easier identification of which legal framework applies to a specific case. Some mentioned the lack of law enforcement expertise as a potential limitation. Among the DPAs interviewed, those with a dedicated sector or unit for LED-related cases declared that this enabled them to devote focused time and resources to such cases.

In one Member State, oversight of police processing is entrusted to a dedicated authority specialised in law enforcement data protection. According to one interviewee, this set-up is seen as a strength because it concentrates expertise and supports a strong understanding of policing practices and systems. At the same time, the DPA noted that this does not remove resource constraints and that investigative work remains largely reactive due to limited capacity.

Echoing FRA's previous conclusions on the implementation of the GDPR, this research exposes a general under-resourcing of DPAs for LED-specific supervision, despite their broad mandate under Article 46. While most Member States task a single authority with overseeing compliance with both the GDPR and the LED, prioritisation skews heavily towards the GDPR, a trend that is exacerbated by chronic understaffing. Although complaint-driven work is manageable, proactive enforcement (e.g. unannounced inspections and thematic reviews) suffers, with DPAs lacking the capacity to regularly monitor law enforcement processing. Dedicated LED units, where they exist, fare better, demonstrating that LED-designated resources enable more effective oversight. Robust

oversight can foster not only better LED implementation, but also a culture of awareness and understanding of data protection principles within competent authorities.

3.2. Investigating competent authorities

As described above, DPAs are tasked with investigating competent authorities, either on their own initiative or following a complaint. To do so, the LED clarifies that Member States should provide them with supervisory powers, which should include at least 'the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks'.

3.2.1. Resources and investigatory powers

When asked to describe whether they were satisfied with investigatory powers as granted to them by law, most of the DPA staff interviewed by FRA considered these powers to be sufficient. Several respondents acknowledged, however, that this statement was based on a low number of investigations conducted: given resource shortages, most investigations are reactive (based on a complaint or on notifications of breaches).

Some respondents from DPAs highlighted that they consider it helpful to be involved at a very early stage when a data processing operation is being developed. Indeed, most of the DPA staff interviewed confirmed that they were consulted on issues or asked questions about procedures that were outside the scope of what competent authorities are required to do. Examples include the use of specific technologies, such as AI, CCTV, facial recognition, drones or biometric data, and other topics, such as issues related to seized documents, the superfluous collection of data or disclosure of third-person data during disciplinary proceedings. A few DPA employees flagged some negative effects that these unofficial requests may have, namely that DPAs cannot provide data controllers with legal advice and are already stretched under workloads stemming from official requests, complaints or investigations. A few other interviewees indeed highlighted that it may be difficult for them to assess where to draw a line between requirements to provide guidance.

Challenges related to the use of artificial intelligence and modern technologies

Most DPA experts stated that they had not investigated any cases of non-compliance with LED principles that involved modern technologies, and all but six of them stated that they did not have sufficient IT expertise in-house (however, a few of them believed that, as the use of modern technologies is not developed within their law enforcement, this is not, currently, an issue). One of the three that stated that their IT expertise was adequate emphasised the importance of

conducting DPIAs and of cooperating with competent authorities when these authorities plan to use specific technologies. Another one identified as a challenge the lack of guidance on the criteria that should be used to evaluate new technologies. However, no interviewees referred to the fundamental rights impact assessment that was introduced by the AI Act. Some solutions identified by interviewees included outsourcing, recruiting (one interviewee stated that they are 'actively recruiting ICT [information and communications technology] technologists') and developing in-house labs or an in-house workforce to develop their understanding.

Many interviewees referred to (some well-known) cases involving facial recognition technologies, public surveillance or the use of biometric data for identification purposes. No specific difficulties were identified, however, in the course of the discussion; some interviewees stated that they do anticipate investigations becoming more challenging because of the volume of data becoming greater. One interviewee, however, considered that their authority had not identified data protection challenges in the use of new technologies by law enforcement because they lack the human resources and the expertise to assess such technologies. In this context, several interviewees from DPAs, at the time of the fieldwork, were aware that their authority would be granted additional powers with respect to the supervision of fundamental rights protection from AI through Article 77 of the AI Act. They confirmed that they are in the process of preparing for this new role, mainly through training, recruitment and restructuring.

Challenges related to accessing data during investigations

Almost all interviewees indicated that they had not faced any issues in accessing documents, even when these were classified, as, in most cases, interviewees declared that DPA staff involved in the investigations have security clearance. In Member States where the DPA has no or very limited competence to investigate or access classified information, this was identified as a challenging factor to effectively investigate competent authorities.

Interviewees did report that, in some cases, police authorities have been reluctant to hand over documents, and this stems, in the opinion of one interview, 'from the abstract language of the LED, which leaves room for interpretation regarding what constitutes "necessary" data, especially since "personal data" is oftentimes spread over a variety of documents'. There was some disagreement between the supervisory and competent authorities about what constitute necessary data for the purpose of an investigation. One interviewee mentioned that there have been cases in which the third-party rule (which prohibits law enforcement from sharing information received from a foreign authority to another authority without prior consent) prevented law enforcement from providing information, and this was deemed not satisfactory for the DPA, adding that such cases are not uncommon. One interviewee from a DPA mentioned some cases in which the police referred to the national security exemption of Article 10 of the LED, while, in the view of the interviewee, 'the nature of the data and the context [were] not supporting such a claim'. Some DPA experts called for a legal basis to make cooperation and document submission mandatory, highlighting that such a legal basis does exist in some Member States, with one interviewee calling for a legal

clarification aiming at also making confidential data fully accessible to the DPA.

Challenges related to data protection authorities' expertise in cases related to the Law Enforcement Directive

Echoing what some operational agents identified as a challenge in their exchanges with data protection experts, the lack of in-house expertise was mentioned as potentially problematic by some interviewees from DPAs, notably when it comes to assessing the grounds under which a data subject's rights may be limited. One interviewee stated that, in most cases, the DPA can only assess whether the argument put forward by the police is reasonable.

> **Cases [on information to be given to the data subject] that involve a police assessment of whether to withhold information for the sake of protecting the investigation can be difficult to scrutinise because we lack the police expertise. Of course, we need to look at whether [the police] have a reasonable argument – and whether we understand the argument – but otherwise, we can't do much more than trust that it is correct.**
>
> *An officer at a DPA*

Promising practice: standardisation of processes governing inspections and investigations (Germany)

In Germany, mandatory inspections were standardised in one procedure. Routine inspections follow a step-by-step process, involving (1) gathering information through questionnaires and document requests, (2) an on-site appointment consisting of an opening meeting, an investigation of the facts and a final meeting, (3) a legal assessment and, finally, (4) the preparation of the inspection report.

Source: FRA interview in Germany.

3.2.2. Data protection authorities' cooperation with competent authorities and

data protection officers

Some respondents from DPAs emphasised that investigations benefited from good cooperation with competent authorities, and several insisted on the essential role of DPOs during their investigations. Similarly, many interviewees confirmed that their DPA maintains a list of LED DPOs at the national level, although some experts interviewed by FRA stated that they do not have or require such a list, as they know DPOs in law enforcement. FRA also asked about whether, to their knowledge, DPA officials were contacted in confidence by DPOs from law enforcement or the judicial authorities to raise issues confidentially. Several of them stated that this was the case: in some cases, this related to processing of data that the DPO saw as potentially problematic and, in other cases, it related to DPOs' opinions not being taken on board. In one Member State, the DPA interviewee explained that they know it is difficult for DPOs to be heard by police chiefs and for a balance to be found between operational necessity and data protection, referring to this as being 'a daily battle'. In another case, a DPA interviewee stated that, 'while not strictly whistleblowing', DPOs contacted them to raise issues related to resources and institutional capacities.

> **[Having the DPO as the main point of contact] is very beneficial, as they are knowledgeable, understand the issues, and know what needs to be done.**
>
> *An officer at a DPA*

Some interviewees from the DPAs indicated, however, that they do not systematically turn to DPOs when there is an investigation and instead contact them only on a 'needs basis'. They consider that only data controllers should be approached during an investigation and that the DPOs should be approached only if they played an active role in the data processing under investigation. Indeed, FRA's findings also identified some dissonant perceptions in the appreciation of the role of the DPOs: while a majority consider DPOs as their direct interlocutors, one interviewee considered them as being 'part of their institution' and, therefore, not independent enough to be trusted interlocutors of the DPA. Another interviewee considered the DPO to be an 'internal supervisor'.

Several DPA interviewees identified what they considered to be a serious lack of expertise and understanding of LED requirements within law enforcement and judicial authorities and, remarkably in a few cases, by DPOs. One example of this can be found in challenges identified by DPAs when it comes to notifications of personal data breaches. Some respondents highlighted to FRA that they believe there is 'little awareness in law enforcement authorities' of when data breaches should be reported. Two issues were identified: the first was related to the seriousness

threshold (one interviewee clarified that competent authorities would only report breaches that pose 'great risk', which, in their view, could potentially contradict Articles 10 and 17 of the LED) and the second was in regard to the differentiation between potential and confirmed breaches. The thresholds of the seriousness of the breach were indeed identified as lacking clarity for **both** operational staff and DPAs by a number of experts interviewed.

> **One challenge the DPA faces is that the thresholds for identifying data breaches are not as stringent under the LED as they are under the GDPR.**
>
> *An officer at a DPA*

3.2.3. Enforcement and corrective powers

For their supervisory mandate to be effective, the LED provides that DPAs should be entrusted with corrective powers, such as issuing warnings, ordering controllers to bring processing operations into compliance or imposing temporary or definitive limitation – including bans – on processing (Article 47(2) of the LED). DPAs were asked whether they faced any enforcement issues and, in particular, whether the application of criminal procedural law prevented them from using these corrective powers in practice, given the independence and secrecy of criminal investigations.

A majority of DPAs stated that they did not face any resistance stemming specifically from the national criminal procedural law in the application of corrective powers; several of them mentioned that there had been no or very few cases that ended in corrective powers being applied under the LED. Several DPAs insisted that they were very aware of the limited scope of their investigations when it comes to criminal investigations, also recalling that, de facto, this limits the cases in which corrective powers can be applied.

In the few interviews in which respondents identified limitations linked to the application of the criminal procedural law, the following issues were raised.

- In one case, the DPA expressed concerns that the code of criminal procedure could impair data protection in a way that is not justifiable, as it is considered by law enforcement authorities as excluding the DPA from applying both investigatory and corrective powers.

> **The [law enforcement authorities, including corresponding ministries] are of course also bound by law and order. They therefore ensure that the law is observed, including in their subordinate authority. However, [they believe that] no independent third body such as the [DPA] should come in and presume to know better and exercise legal supervision … I would now counter that with 'Yes, but that's how it's intended by the European legislator' … [W]e, as the DPA, have special legal supervision over the law enforcement authorities in the duty area, namely for data protection law.**
>
> *An officer at a DPA*

- In another case, the DPA stated, that they have no possibility to prevent the disclosure of personal data after a seizure by the prosecution or by the national bureau of investigation, as it is mandated by criminal procedural law. The interviewee believes that competent authorities perceive this as a case in which a specific law overrides general rules: 'we were unable to have the names of the other … victims or the defendant's criminal record removed from the indictment because the … court ruled that the Criminal Procedure Code explicitly allows such disclosure'.
- In a few cases, interviewees reported that their investigations must be stopped when data processing is related to criminal investigations, that is, for secrecy reasons, for reasons related to the protection of the evidence or when an administrative misdemeanour is classified as a criminal offence at a later stage.

While not specifically related to the application of the criminal procedural law itself, some interviewees identified further challenges when it comes to the enforcement of the LED legal regimes, including corrective powers. One interviewee noted that the legislator specified cases when a fine cannot be imposed for violations under the LED legal regime, which has created 'a skewed relationship between the competent authorities under the LED', namely those that may receive fines and those that are exempt from the application of such corrections. One interviewee stated that the main challenge stems from the fact that 'sanctioning public authorities and paralyzing data processing [by these institutions] would have a significant political influence'.

Finally, to ensure its consistent application, the LED sets out that DPAs should provide each other with mutual assistance. In its first evaluation, the Commission reported that mutual assistance had been very rarely utilised to date. FRA's research confirms this finding: for a majority of the DPAs interviewed, cooperation with other EU DPAs mostly takes place under the GDPR regime.

Some of the cases mentioned by the DPAs referred to inquiries asking about the interpretation of provisions of the LED. However, in general, the mutual assistance regime is not seen as valuable or relevant for LED-related matters. A few DPAs also noted that cross-border cases can be dealt with under the Europol Regulation [30]. Similarly, almost all of the DPAs stated that their authority did not investigate transfers of personal data to non-EU countries or international organisations, as, in their view, this would fall outside the scope of the LED or would fall under the national security exemption.

The findings reveal systemic obstacles to DPAs' effective investigation of law enforcement and judicial authorities. While most DPAs consider their legal powers sufficient, resource constraints relegate enforcement to reactive, complaint-driven actions, leaving proactive oversight neglected. Early engagement with authorities on topics such as AI, biometrics or surveillance technology is valuable but informal, creating blurred boundaries between guidance and enforcement. The lack of in-house IT expertise further hampers the scrutiny of modern technologies, with DPAs struggling to assess risks in facial recognition, drones or big data analytics. Although some outsource or recruit specialists, most lack the capacity to keep pace with technological advances.

Access to data emerges as a recurring friction point. While security clearances generally facilitate access, classified materials and national security exemptions (Article 10 of the LED) create deadlocks, with some interviewees noticing that authorities may invoke procedural laws to withhold information. Disputes over what constitute 'necessary' data may further delay investigations, as police push back on disclosure requests.

Expertise gaps can reinforce these challenges. Some DPAs indicated that they struggle with scrutinising law enforcement justifications due to a lack of operational insight. DPOs' variable competence (from highly skilled to underprepared) adds inconsistency, with some DPAs being contacted in a 'whistleblowing' capacity by DPOs who are frustrated by their advice being ignored. Breach notifications also exemplified this, as some respondents indicated that they believe that there is little awareness within law enforcement authorities regarding when data breaches should be reported, leading to misjudged thresholds of only 'high-risk' incidents being reported.

Enforcement powers can also face legal and political hurdles. While most DPAs report no resistance from criminal procedural laws, exemptions for 'ongoing investigations' shield authorities from corrective actions. Sanctions are rare, with political sensitivities deterring fines or processing bans against public bodies. Mutual assistance (Article 50 of the LED) is largely unused, hindered by divergent national implementations and a cultural reluctance to collaborate.

Conclusion

The LED was designed to ensure that legitimate law enforcement activities are conducted with appropriate fundamental rights safeguards in place, in an era when personal data are central to effective criminal investigations. However, as this report demonstrates, the implementation of laws transposing the LED remains uneven across the EU, with significant challenges related to awareness, resources and practical application. While progress has been made since the LED's adoption, and recent CJEU case-law has further clarified important aspects of its interpretation, gaps in understanding and resource constraints risk undermining its effectiveness.

One of the key issues identified is the need for better awareness and understanding of the LED's core principles and requirements among law enforcement and judicial authorities. As the report has shown, there are still operational staff who do not have a clear understanding of its principles, such as purpose limitation and data minimisation, or of the conditions governing international data transfers. This may undermine the effective and consistent application of the LED's requirements in practice, with real-world consequences. These include the risk of unlawful data processing or public trust in law enforcement being eroded.

Another critical challenge is the shortage of resources available to DPOs and DPAs. DPOs, who play a vital role in ensuring compliance within law enforcement authorities, often work alone or with minimal support, lacking the time, expertise and/or independence needed to fulfil their mandates effectively. As this report shows, many were appointed internally without prior specialised knowledge of the LED, forcing them to rely on self-learning or GDPR-centric training that does not fully apply to their work. At the supervisory level, DPAs also face significant capacity constraints, including chronic underfunding and the prioritisation of GDPR-related tasks over proactive LED enforcement. This resource gap limits their ability to conduct regular inspections, develop expertise in new technologies or provide timely advice to law enforcement agencies.

The rapid advancement of technology presents another significant hurdle. The LED was designed before the widespread adoption of AI and cloud-based investigations, leaving many authorities uncertain about how to apply its principles to these new contexts. For example, the use of AI in criminal investigations raises questions about, among other things, lawfulness, data quality, bias, transparency and accountability. Similarly, the storage of data in third-country clouds, particularly in the United States, creates legal uncertainties, as authorities struggle to define what constitutes 'appropriate safeguards' in the absence of EU adequacy decisions.

Beyond these structural issues, data protection is still sometimes perceived as an obstacle to effective policing rather than as an integral part of it. This mindset can lead to practices such as the indiscriminate collection and processing of data 'just in case' it becomes useful for potential future investigations, or frustration with what are seen as bureaucratic requirements, such as responding to data subjects' requests.

The effective implementation of the LED is not just a legal obligation; it is a cornerstone of a

justice system that respects fundamental rights while combating crime. The findings of this report highlight both the progress made and the work that remains to be done. By acting on these, Member States and EU institutions can ensure that the LED achieves its dual goals of enabling effective law enforcement and protecting the privacy rights of all individuals. The evaluation of the LED by the European Commission published in 2026 presented an opportunity to address these issues comprehensively, ensuring that the LED remains fit for purpose in a rapidly evolving digital landscape.

Annex 1: Methodology

To collect first-hand experiences of the understanding of, and potential challenges related to, the application of data protection principles, FRA identified two entities to be interviewed: competent authorities and DPAs (or 'supervisory authorities' as they are referred to in the LED). Competent authorities are defined in the LED as 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' and therefore include, principally, law enforcement authorities and prosecutors' offices.

The target group for the interviews to be conducted was therefore defined as follows, for each of the 27 Member States:

- one DPO from a competent authority;
- two officials in charge of data-driven investigations (e.g. cybercrime or digital forensics) from an operational police department;
- one member of the national prosecutor's office and/or an investigating judge experienced in dealing with LED-related cases;
- one official in charge of investigations and complaints related to the LED in the national DPA.

In December 2024, FRA contracted Franet to identify the five interviewees per Member State and to conduct the interviews in the national language. This fieldwork phase took place from January to July 2025.

In cooperation with the European Commission and Europol, FRA developed three questionnaires, building on the data protection principles and requirements of the LED: one for operational agents in competent authorities, one for DPOs in competent authorities and one for DPA staff members.

The questionnaire for competent authorities (operational staff members and DPOs) covered six areas:

- institutional capacities;
- the implementation of the LED (including questions on the lawfulness of processing, purpose limitation, data minimisation, data storage, data quality, data security, the distinction between different categories of data subjects, data subjects' rights and breaches);
- being investigated;
- requesting advice;
- the transfer of personal data to non-EU countries or international organisations;
- cooperation and networks.

Albeit similar in scope, questions were differentiated and adapted to fit with DPOs' and operational staff's roles.

The questionnaire for DPAs covered eight areas:

- institutional capacities;
- investigatory powers and investigations;
- consultations and providing advice;
- modern technological challenges;
- personal data breaches;
- corrective powers;
- the transfer of personal data to non-EU countries or international organisations;
- cooperation with other Member States' DPAs.

During the identification and recruitment of interviewees, most national authorities responded positively.

- DPAs from all 27 Member States accepted the invitation to participate in the project.
- Competent authorities' DPOs also all accepted the invitation to participate in the project. In eight Member States, Franet conducted interviews with two DPOs.
- Operational staff from law enforcement and judicial authorities were more difficult to recruit in four Member States:
  - Denmark (only one interview could be conducted with the police),
  - France (no interview could be conducted with members of the police or judicial authorities),
  - Ireland (only one interview could be conducted with the police),
  - Italy (no interview with the police could be conducted).

In general terms, however, FRA research benefited from a very high rate of and positive participation among operational staff working in both law enforcement and judicial authorities. Operational staff from competent authorities were cooperative and showed a willingness to share their experiences and understanding related to the protection of personal data in their day-to-day work.

In the police, interviews were mainly conducted with officers working as criminal investigators, some with a cybercrime specialisation and some with a specialisation in the assessment of digital evidence. In judicial authorities, interviews were mostly with public prosecutors specialising in cybercrime, digital investigations, international cooperation and data protection. Given the difficulties mentioned earlier, while FRA specifically requested that operational agents with no data protection mandate be interviewed (in order to test the level of awareness and understanding of data controllers), in some cases, the authorities nominated their data protection expert to participate in the interview. This was the case in 8 of the 26 interviews conducted in prosecutors'

offices.

In total, FRA conducted face-to-face interviews with 132 experts (Table 1).

Table 1 – Breakdown of interviews conducted by FRA

DPOs in competent authorities	Operational staff in law enforcement authorities	Operational staff in judicial authorities	Staff members in DPAs
19 in the police **14** in prosecutors' offices **8** in law enforcement departments of interior ministries **1** in a correctional authority	**16** in criminal investigations **15** in cybercrime **4** in border management and border criminal investigations **3** in data protection / privacy / legal positions (other than DPOs) **2** in data analysis **2** in international law enforcement cooperation **1** in staff management	**12** prosecutors **3** judges **2** state attorneys **1** investigator	**1** interview per Member State, and in **2** cases an additional interview was conducted with a different staff member
Total: 42	**Total: 43**	**Total: 18**	**Total: 29**

FRA's questionnaire was broad, ensuring that different areas of expertise could be covered in relation to the LED. In some cases, this resulted in long interviews in which participants shared detailed aspects of their work. Assurance of the confidentiality of exchanges played a key role in ensuring a positive response to the invitation to participate in interviews.

All interviews were conducted face-to-face by Franet [31] in the language of the Member State. With the consent of the interviewees, interviews were audio-recorded 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, see the data protection notice published on FRA's website.

Interviews were conducted anonymously to obtain the most open insights into experiences, as this allowed interviewees to speak more freely. Quotes and promising practices were sent back to interviewees, who checked them for accuracy, while ensuring that their anonymity was upheld in

the information reported. Where available and useful, interviewees provided FRA with public sources of information, which were integrated into the report as official references. On a few occasions, the interviewee did not, and could not, provide FRA with further references, and in these instances the source of the practice is identified as stemming from the interviews FRA conducted with one or several interviewees.

FRA analysed the fieldwork data using Maxqda software to support the identification of patterns and common challenges. It also compared the data with previous evidence that FRA has collected on challenges evidenced by DPAs in the implementation of the GDPR, published in 2024.

Note: The results presented in the report are based – as outlined – on a qualitative research methodology. This is an established methodological approach. However, by their very nature and scale, these qualitative research findings cannot claim (and do not claim) to be representative of the whole professional group(s) to which interviewees belong. At the same time, the response rate and number of people covered were broad and the information provided allows a comprehensive picture to be gained of issues of relevance for the topics covered in the report. Where the report refers 'one' respondent, these are illustrative examples of views that were held by more than one respondent and should not be interpreted as 'atypical' responses from a single respondent in the research. Given the good responses and large number of interviews, patterns in responses were identified based on the number of interviewees mentioning a practice or a challenge, clarifying in the text the group to which they belong (i.e. DPOs, staff working in law enforcement authorities, staff working in judicial authorities or staff working in DPAs).

Endnotes

[1] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

[2] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Roadmap for lawful and effective access to data for law enforcement, COM(2025) 349 final of 24 June 2025.

[5] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

[6] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

[7] See Kosta, E. and Boehm, F. (eds), The EU Law Enforcement Directive (LED): A commentary, Oxford University Press, Oxford, 2024; and Communication from the Commission to the European Parliament and the Council – First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final of 25 January 2022.

[8] Judgment of the Court of Justice of 4 June 2026, CL v Prokuratura na Republika Bulgaria, C-312/24, ECLI:EU:C:2026:449, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62024CJ0312.

[9] Judgment of the Court of Justice of 19 March 2026, criminal proceedings against Ministère public, C-371/24, ECLI:EU:C:2026:219, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62024CJ0371.

[10] Judgment of the Court of Justice of 20 November 2025, JH v Policejní prezidium, C-57/23, ECLI:EU:C:2025:905, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023CJ0057.

[11] European Commission: Directorate-General Justice and Consumers, Report on the Transposition of Directive (EU) 2016/680, Brussels, 2023.

[12] Communication from the Commission to the European Parliament and the Council – First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final of 25 July 2022.

[13] European Commission, 'June infringements package: Key decisions', 4 June 2026; and European Commission, 'July infringements package: Key decisions', 8 July 2026.

[14] See Article 4(1)(b) and (c) of the LED, recital 26 of the LED and Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation', WP 203, 2 April 2013.

[15] See De Hert, P. and Sajfert, J., 'The fundamental right to personal data protection in criminal investigations and proceedings: Framing big data policing through the purpose limitation and data minimisation principles of Directive (EU) 2016/680', Brussels Privacy Hub Working Paper, Vol. 7, No 31, December 2021, p. 13.

[16] Judgment of the Court of Justice of 8 December 2022, Inspektor v Inspektorata kam Visshia sadeben savet, C-180/21, ECLI:EU:C:2022:967, paragraphs 43–44, 50–56 and 61, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0180; see also Wahl, T., 'CJEU ruled on scope and concepts of Law Enforcement Data Protection Directive', eucrim website, 10 January 2023.

[17] Austria, Data Protection Law (Datenschutzgesetz – DSG), Section 42, paragraph 8.

[18] Judgment of the Court of Justice of 16 November 2023, Ligue des droits humains ASBL and BA v Organe de contrôle de l'information policière (OCIP), C-333/22, ECLI :EU:C:2023:874, paragraphs 41-42 and 55.

[19] Communication from the Commission to the European Parliament and the Council – First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final of 25 July 2022, p. 19.

[20] FRA, GDPR in Practice – Experiences of data protection authorities, Publications Office of the European Union, Luxembourg, 2024, Chapter 1, Section 1.1.

[21] See Sajfert, J., 'National implementations', in: Kosta, E. and Boehm, F. (eds), The EU Law Enforcement Directive (LED): A commentary, Oxford University Press, Oxford, 2024, pp. 39–48.

[22] Communication from the Commission to the European Parliament and the Council – First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final of 25 July 2022.

[23] FRA, GDPR in Practice – Experiences of data protection authorities, Publications Office of the European Union, Luxembourg, 2024.

[24] 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, ELI: http://data.europa.eu/eli/reg/2017/2226/oj).

[25] 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, ELI: http://data.europa.eu/eli/reg/2024/1356/oj).

[26] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen information system (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj).

[27] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the visa information system (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60, ELI: http://data.europa.eu/eli/reg/2008/767/oj).

[28] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj).

[29] Communication from the Commission to the European Parliament and the Council – First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final of 25 July 2022, Section 3.4.1 (stating that individual complaints are 'far fewer in number than for the GDPR').

[30] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj).

[31] For more information, see FRA's web page on Franet, the agency's multidisciplinary research network: Franet.

About this publication

© European Union Agency for Fundamental Rights, 2026

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, 2026

HTML:

- ISBN: 978-92-9489-825-8
- doi:10.2811/1281573
- TK-01-26-026-EN-Q

PDF:

- ISBN: 978-92-9489-836-4
- doi:10.2811/4200067
- TK-01-26-026-EN-N

Photo credits (cover):

- Cover: © Who is Danny/Adobe Stock

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS Rennweg 12 – 1030 Vienna – Austria

Contact FRA

- Website
- LinkedIn
- Instagram
- Facebook
- YouTube
- X