Council of the
European Union

Brussels, 25 July 2022
(OR. en)

11583/22

DATAPROTECT 229
JAI 1070
DIGIT 149
MI 595
FREMP 164

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 July 2022
To:	General Secretariat of the Council
No. Cion doc.:	COM(2022) 364 final
Subject:	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')

Delegations will find attached document COM(2022) 364 final.

Encl.: COM(2022) 364 final

EUROPEAN
COMMISSION

Brussels, 25.7.2022
COM(2022) 364 final

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')

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

First report on the application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')

Table of contents

1 THE LED AS THE MAIN INSTRUMENT TO ENSURE DATA PROTECTION IN THE EUROPEAN UNION'S SECURITY POLICY

This Communication sets out the European Commission's first report on the evaluation and review of the Data Protection Law Enforcement Directive (EU) 2016/680[1] ('the LED'), pursuant to Article 62(1) LED.

The report examines, in particular, the application and functioning of the LED's rules on the transfer of personal data to third countries and international organisations as required by the LED, but it also takes a broader approach. It situates the LED within the frameworks of EU law on the protection of personal data and EU law regulating the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties, including safeguarding against and prevention of threats to public security ('criminal law enforcement')[2]. The report provides an overview of the Member States' transposition of the LED into their national laws, presents the first lessons drawn from the LED's application and functioning, and outlines the way forward.

1.1 A key element of a consistent European Union data protection framework

The LED is one of the three pillars of the EU framework guaranteeing the fundamental right to the protection of personal data. The other two are the General Data Protection Regulation ('the GDPR')[3] and the Regulation on Data Protection for EU institutions and bodies ('the EUDPR')[4]. The fundamental right of data protection is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter')[5] and in Article 16 of the Treaty on the Functioning of the European Union ('the TFEU')[6].

---

[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).

[2] Article 1(1) LED.

[3] 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 (OJ L 119, 4.5.2016, p. 1).

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[5] The Charter of Fundamental Rights of the European Union (OJ C 202, 7.6.2016, p. 389).

[6] A consolidated version of the Treaty on the Functioning of the European Union (OJ C 202, 7.6.2016, p. 47).

The LED entered into force on 6 May 2016 and Member States were required to transpose it by 6 May 2018[7].

The LED is the first EU legislative act that takes a comprehensive approach to the protection of personal data by competent authorities (i.e. judicial authorities, police and other criminal law enforcement authorities as provided for by Article 3(7) LED) for criminal law enforcement purposes. By comparison with the Council Framework Decision 2008/977/JHA[8], which it repealed and replaced, the LED is a major advance in ensuring the consistent application of data protection rules across the EU. Firstly, the LED provides a complete set of rules to both cross-border and domestic processing of personal data for criminal law enforcement purposes, while the Council Framework Decision only covered cross-border processing . Secondly, the LED provides a comprehensive and horizontal set of rules, whereas under the previous approach, each EU sectoral act that provided for the processing of personal data in the criminal law enforcement context was governed by its own data protection rules[9].

The GDPR, the EUDPR and the LED are based on similar concepts and principles[10], resulting in the consistent interpretation and application of EU data protection rules. They share common definitions and contain similar obligations for data controllers and processors. However, the LED also specifically addresses risks linked to the processing of personal data in the criminal law enforcement context. The corresponding provisions include obligations to (i) distinguish between different categories of data subjects, (ii) distinguish between personal data based on facts and data based on a personal assessment, (iii) keep a log about the use of personal data, and comply with specific security requirements[11].

Given the specific nature of judicial cooperation in the fields of criminal matters and police cooperation, it was considered necessary to adopt specific rules in these fields for the protection of personal data and the free movement of personal data[12]. The sensitivity of the area of judicial cooperation in criminal matters and police cooperation, together with the complexity of the national legal frameworks that regulate criminal law enforcement, led to a directive being considered the best instrument for achieving a high level of data protection in this field. A

[7] Article 63(1) LED.
[8] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).
[9] For example, legal acts regulating the Schengen Information System and other Schengen acquis instruments contained specific provisions regulating matters such as data subject rights.
[10] These include lawfulness and fairness; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 4 LED).
[11] Articles 6, 7, 25 and 29 LED respectively.
[12] Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon. (OJ C 115, 9.5.2008, p. 345–345).

directive also leaves Member States the necessary flexibility when implementing the principles, rules and exemptions at national level[13].

The Commission published its first report on the implementation of the GDPR on 24 June 2020[14]. It concluded that the general view was that the GDPR met its objectives, in particular by providing citizens with a strong set of enforceable rights and by creating a new EU system of governance and enforcement. The report set out a list of actions to be taken to further facilitate the application of the GDPR by all stakeholders and to promote and further develop a data protection culture in the EU, along with vigorous enforcement.

This report follows on from the review of legal acts adopted by the EU which regulate data processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The purpose of that review was to assess the need to align the legal acts in question with the LED[15]. On 24 June 2020, the Commission met that obligation by adopting a Communication on a way forward on aligning the former third pillar acquis with data protection rules[16]. It identified 10 legal acts that should be aligned with the LED and set out a timetable for this work.

Finally, this report was prepared in parallel with the Commission's report on the application of the EUDPR. An important element of the latter is the review of its rules, set out in Chapter IX, on the processing of operational personal data by EU bodies, offices or agencies when carrying out activities that fall within the scope of police cooperation and judicial cooperation in criminal matters[17] ('JHA agencies'). The rules in question are largely based on the LED. Article 98 EUDPR requires the Commission to review legal acts regulating the processing of operational personal data by JHA agencies and allows it to submit appropriate legislative proposals, in particular with a view to applying the Chapter IX rules to Europol[18] and the European Public Prosecutor's Office as well as to propose any necessary changes to this Chapter.

1.2 An essential contribution to ensure a robust security policy within the European Union

---

[13] Explanatory memorandum to the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25 January 2012.

[14] Communication from the Commission to the European Parliament and the Council 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020) 264 final, 24 June 2020'.

[15] Article 62(6) LED required the Commission to review, by 6 May 2019, other EU legal acts that regulate the processing of personal data for law enforcement purposes, in order to assess the need for alignment with the LED and, where appropriate, propose amendments to those other EU legal acts in order to ensure a consistent approach to the protection of personal data within the scope of the LED.

[16] Communication from the Commission to the European Parliament and the Council 'Way forward on aligning the former third pillar acquis with data protection rules', COM(2020) 262 final, 24 June 2020.

[17] Chapters 4 and 5 of Title V of Part Three of the TFEU.

[18] This has already been addressed by the 2020 Commission proposal on amending the Europol Regulation.

The Commission has consistently stressed that an effective and genuinely secure EU can only be built on the basis of full compliance with the fundamental rights enshrined in the Charter and secondary EU legislation. The LED makes a key contribution to the EU's security policy by ensuring that the personal data of victims, witnesses and suspects of crime are duly protected. Furthermore, by harmonising the rules on the protection of personal data processed by competent authorities in EU and Schengen countries, the LED contributes to increased trust and the security of data exchanged between authorities for criminal law enforcement purposes, and thereby facilitating cross-border cooperation in the fight against crime and terrorism[19]. The LED also plays a key role in promoting a culture of data protection compliance among competent authorities.

The Security Union Strategy[20] further stresses that new technology such as artificial intelligence could be used as a powerful tool to fight crime. Realising this potential also means ensuring the highest standards of compliance for fundamental rights. Data protection legislation, including the LED, provides the basis on which sectoral legislation can be built. For instance, the proposed AI Act[21] would further frame the use of personal data for remote biometric identification in public places for law enforcement purposes.

Finally, in an interconnected world, crime (and cybercrime and other cyber-enabled crime in particular) is increasingly of a cross-border nature. Even when investigating domestic cases, competent authorities increasingly find themselves in cross-border situations because information is stored electronically in a third country. This increases the need for international cooperation in criminal investigations, both on the part of the Member States' authorities and on the part of EU bodies such as Europol and Eurojust. Such cooperation, and in particular the collection and exchange of electronic evidence,[22] often involves the transfer of personal data. Strong data-protection safeguards are therefore essential. Such safeguards also help to build confidence between law enforcement authorities, ensuring faster and more effective information exchange and strengthening legal certainty when information is then used in criminal proceedings. In this respect, the LED provides an updated set of tools for facilitating such

[19] Communication from the Commission to the European Parliament and to the Council - First Progress Report on the EU Security Union Strategy, COM(2020) 797 final, 9 December 2020.
[20] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM (2020) 605 final, 24 July 2020.
[21] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, 21 April 2021.
[22] Electronic information and evidence is needed in about 85% of investigations into serious crimes, and 65% of the total number of requests are made to providers based in another jurisdiction. See the Commission Staff Working Document ('Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings'), SWD(2018) 118 final.

transfers of personal data from the EU to a third country or international organisation (for instance Interpol[23]), while also ensuring that the personal data continues to benefit from a high level of protection. The Commission and Member States have made use of the whole range of the LED's tools since its entry into force, thus confirming that it is broad and flexible enough to make effective international police and judicial cooperation possible.

1.3 Important considerations regarding the preparation of the report

In preparing this report, the Commission gathered information and feedback from a variety of sources and targeted consultation activities. Further to Article 62 LED, the Commission took into account the contributions and positions of the European Parliament[24], the Council[25], the European Data Protection Board ('the EDPB')[26] and national data protection supervisory authorities. Additional feedback was obtained through a questionnaire addressed to civil society organisations (through the European Union Agency for Fundamental Rights)[27] and from responses to a public call for evidence[28]. The Commission also considered observations from the Member States Expert Group on the GDPR and LED[29], and observations of the German Presidency of the Council[30]. It also took into account the analysis of national transposition measures and a small number of complaints it had received in this regard.

While the LED applies to all Member States and all Schengen countries (because it constitutes a development of the Schengen acquis[31]), this report only covers EU Member States.

Three factors impacted the preparation of this report. Firstly, two thirds of Member States failed to meet the May 2018 deadline for transposing the LED into national law. Nevertheless, most Member States transposed the LED by 2019 after the Commission had launched infringement

---

[23] See also recital 25 LED.
[24] Contribution by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs to the European Commission's upcoming report on the evaluation and review of the LED, 7 February 2022.
[25] Council position and findings on the application of the LED (Council document 13943/21 of 18 November 2021 https://www.consilium.europa.eu/media/54304/st_13943_2021_init_en.pdf).
[26] Contribution of the EDPB to the European Commission's evaluation of the LED under Article 62 LED, adopted on 14 December 2021 ('EDPB contribution to the evaluation of the LED'). https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.
[27] Out of the 804 civil society organisations approached by the European Union Agency for Fundamental Rights (FRA), 88 replied. However, only 17 of the *contributions could be considered on account of the fact that 61 contributions were not related to the LED,* or indicated that the organisation concerned do not work on fundamental rights protection in the area of criminal law enforcement or *is* not at all familiar with the LED.
[28] Call for Evidence, data protection in law enforcement – report on the Law Enforcement Directive, 24 January 2022. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13288-Data-protection-in-law-enforcement-report-on-the-Law-Enforcement-Directive_en.
[29] Commission expert group on Regulation (EU) 2016/679 and Directive (EU) 2016/680 (E03461); https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461
[30] Report by the Presidency of the Council of the European Union on the exchange of police data with third countries - experiences in the application of Article 37 of the Law Enforcement Directive, December 2020.
[31] See recitals 101-103 LED.

procedures. Therefore, there is rather limited experience on its application, a point which the EDPB[32] and the Council[33] also stress. Secondly, it proved more difficult to compile statistics on the application of the LED, as compared to the GDPR. Some data protection supervisory authorities do not collect statistics on their supervisory activities separately for the LED and the GDPR. This is the case, for example, in relation to data breach notifications[34] and complaints made under the LED[35], sometimes making it difficult to gain an accurate overview of these provisions under the LED[36].

Thirdly, it is important to consider that case law is only starting to be developed regarding on the application of the LED. Several cases are currently pending before the Court of Justice of the European Union ('the CJEU') concerning the interpretation of key LED provisions such as data subjects' right of access and the right to an effective judicial remedy. These judgments will provide more clarity and will contribute to a more harmonised approach amongst Member States.

2 A SATISFACTORY TRANSPOSITION, BUT A NUMBER OF OUTSTANDING ISSUES REMAIN

The Commission has set up a Member States Expert Group[37] to help the Member States incorporate the LED into national law. The group facilitates discussions and the sharing of experiences between Member States and the Commission on data protection rules. It met regularly between the adoption of the LED in 2016 and the transposition deadline of May 2018 and its work resumed in 2021.

The transposition overview presented below focuses on the main issues identified so far. It is primarily based on the Commission's analysis of the information Member States provided when notifying the Commission of the national measures they have taken to transpose the LED into national law. This analysis was supported by an external study carried out by an external contractor. The Commission also engaged in bilateral exchanges with several Member States.

2.1 A complete transposition overall, but with some issues on specific provisions

The Commission initiated infringement procedures against 19 Member States in July 2018 for failing to adopt laws transposing the LED by the May 2018 deadline and to duly notify the Commission of their transposition. Another procedure for partial non-transposition was initiated

[32] EDPB contribution to the evaluation of the LED, paragraph 4.
[33] Council position and findings on the application of the LED, paragraph 7.
[34] For example, the authorities in Denmark, Lithuania, Norway, Austria and several authorities in Germany do not keep separate statistics on LED data breaches. Six authorities have also reported that they received no breach notifications under the LED.
[35] For example, the authorities in Denmark and Austria and several of the authorities in Germany do not keep separate statistics for LED complaints.
[36] EDPB contribution to the evaluation of the LED, paragraph 43.
[37] See footnote 29.

in July 2019 against another Member State. As a result, most of the Member States subsequently notified the Commission of their national transposing legislation and the Commission gradually closed the infringement procedures against them in 2019 (2020 for one Member State). In 2021, the Commission referred its infringement action against Spain to the CJEU because it had still failed to transpose the LED and notify the Commission of its transposition measures. Given the seriousness and duration of the infringement, the CJEU, for the first time, imposed both a lump sum and a penalty payment on Spain[38].

The Commission also launched – in April 2022 – an infringement procedure against Germany after detecting a gap in the transposition of the LED in relation to the activities of Germany's federal police.

The Commission will continue to assess the transposition of the LED within the Member States and will take the necessary measures to remedy any gaps.

2.2 Priorities for assessing compliance

The Commission is also checking that the Member States' national provisions correctly transposed the requirements of the LED (compliance check).

When transposing the LED, Member States either amended their previous legislation on data protection or repealed and replaced it with a new horizontal data protection act(s). In many instances, the national laws transpose the LED by referring to the same or equivalent provision of the GDPR (e.g. as regards definitions, notifications of data breaches, the appointment of the data protection officer and provisions on the organisation, status, competences, tasks and powers of the national data protection supervisory authorities). A number of the LED's provisions were also transposed through new provisions in, for instance, general administrative law, administrative procedural law or criminal procedure. Some Member States also transposed a number of the LED's provisions in sectoral legislation regulating the operation and powers of specific competent authorities. A variety of national legal acts may therefore have to be considered when determining whether or not the LED has been correctly transposed in a particular Member State. Overall, the national laws largely reflect the LED's principles and core provisions. However, a number of issues have been identified, the most important of which are set out in the following sections. The Commission has already launched a number of infringement procedures against Member States[39]. The review process remains ongoing and the

[38] Judgment of 25 February 2021, *European Commission v Kingdom of Spain*, C-658/19, EU:C:2017:548.

[39] In April 2022 the Commission launched infringement procedures against Greece, Finland and Sweden on the grounds that their national transposing laws are not in conformity with the LED. The case against Greece relates to *a number of points, including, inter alia*, the non-application of the national law transposing the LED to the processing of personal data by judicial-prosecutorial authorities and by authorities acting under their supervision for the majority of criminal offences; the transposition of provisions on data storage and review (Article 5); the legal basis for data processing (Article 8); and safeguards in the context of automated decision-making (Article 11). The infringement procedures against Finland and Sweden were launched because their laws do not provide data subjects with access to an effective remedy before a court or a tribunal. The Commission opened an infringement procedure

Commission will continue to use all available tools, including infringements, when a national transposing measure lacks conformity with the LED.

The case law on the LED is still in its infancy. The CJEU has started to deliver judgments on the interpretation of the LED, including *in* the cases *WS v Bundesrepublik Deutschland*[40] and *B v Latvijas Republikas Saeima*[41]. At the time of writing this report, a number of preliminary rulings are pending before the CJEU (as indicated in the following sections).

2.2.1 Scope of the LED

The difficulty of delineating between the scope of application of the LED and the GDPR was raised as an issue of concern both by the Member States Expert Group on GDPR and LED[42], and by the EDPB[43]. Some data protection supervisory authorities have also noted that competent authorities can find this difficult[44].

The scope of the LED is defined[45] by two key elements: the notion of competent authority (personal scope) and the notion of criminal offence (material scope).

As regards the personal scope, data processing falls under the LED when, firstly, it is undertaken by a competent authority and, secondly, when the personal data is processed for LED purposes[46] (i.e. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security). In the Commission's view, 'competent authorities' as defined by the LED[47] are either organs of the State or private bodies, on which the law confers special powers beyond those which result from the normal rules applicable in relations between individuals and/or by the possibility of exercising the power of coercion. These authorities are competent authorities under the LED when (even if only sporadically and/or in isolated cases) they process data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or of executing criminal

---

against Germany in May 2022 because several national laws transposing the LED fail to provide effective corrective powers at federal and Länder level.

[40] Judgment of 12 May 2021, *WS v Bundesrepublik Deutschland*, C-505/19, EU:C:2021:376. The case concerned, among other issues, the lawfulness of processing personal data (Article 4(1)(a) and Article 8 LED) in the specific context of a red notice issued by Interpol. The Court did not preclude the processing of personal data appearing in a red notice issued by Interpol as being lawful until it has been established in a final judicial decision that the *ne bis in idem* principle applies in respect of the acts on which that notice is based.

[41] Judgment of 22 June 2021, *B v Latvijas Republikas Saeima,* C-439/19, EU:C:2021:504. The CJEU interpreted the definition of the competent authority under Article 3(7) and the concept of crime. See also the section below.

[42] See Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 5 May 2021 https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=25283&fromExpertGroups=true

[43] EDPB contribution to the evaluation of the LED, paragraph 7.

[44] The data protection supervision authorities of Ireland, France and Hungary raised this as a concern.

[45] Article 2(1) LED and recitals 12-14 LED.

[46] Article 1 LED.

[47] Article 3(7) LED.

penalties (including safeguarding against and preventing threats to public security). This means, for instance, that processing by such bodies of personal data for non-LED purposes (e.g. human resources or other administrative purposes such as processing by Financial Intelligence Units (FIUs) of personal data under the anti-money laundering *acquis*[48]) falls within the scope of application of the GDPR and not the LED.

The notion of a 'criminal offence' is of central importance when determining whether or not data processing falls within the LED's scope of application. According to the CJEU, three criteria are relevant when assessing whether an offence is criminal in nature: whether the offence is classified as criminal under national law, the intrinsic nature of the offence, and the degree of severity of the penalty that the person concerned is liable to incur[49]. The autonomous character of the concept of criminal offence referred to in recital 13 LED entails, among other things, that Member State law cannot determine the nature of an offence as being 'criminal' for the sole purpose of applying the LED.

The question on demarcation between the scopes of application of the GDPR and the LED arises in some Member States as regards the delineation between the domains of criminal and administrative offences. In particular, some national transposing laws refer to purposes for processing personal data that are not listed in Article 1 LED (e.g. threats to public order or public safety). The question also arises because some Member States consider that a number of administrative bodies (e.g. FIUs, as mentioned above) carry out tasks falling under the LED.

Most of the Member States' laws comprehensively cover any competent authority processing of data for LED purposes. By contrast, some Member States have chosen to exhaustively enumerate the competent authorities under the LED in their national legislation. A few Member States have also provided a derogation for processing by certain types of competent authorities or certain types of data.

The issue of the scope of the LED is the subject of a preliminary reference before the CJEU. The Landesverwaltungsgericht Tirol Court (Austria) raised the issue of the LED's scope of application where a competent authority unsuccessfully tried to access data on a seized phone (interpretation of Article 2 LED). The case also concerns the conditions of such access[50].

---

[48] Article 41 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, which regulates the operation by the Financial Intelligence Units, explicitly states that the processing of personal data under this Directive is subject to Regulation (EU) 2016/679.

[49] Judgment of 22 June 2021, *B v Latvijas Republikas Saeima,* C-439/19, EU:C:2021:504, paragraph 87.

[50] Request for a preliminary ruling in *C.G. v Bezirkshauptmannschaft Landeck*, C-548/21.

2.2.2 Governance and powers of data protection supervisory authorities

All but two Member States (Belgium and Sweden) have entrusted the enforcement of the LED to the supervisory authority that is also responsible for enforcing the GDPR. Belgium has entrusted the supervision of the police for the purposes of the LED to a different supervisory authority. In Sweden the supervision of certain competent authorities, including the police, is co-shared by the supervisory authority competent for the GDPR and another supervisory authority. Furthermore, pursuant to the LED, all data protection supervisory authorities are not competent to supervise the courts when they act in their judicial capacity.

As regards the LED's provisions on data protection supervisory authorities' independence[51], all Member States have stipulated in their transposing legislation that data protection supervisory authorities shall act independently when performing their tasks. They also require that members of their data protection supervisory authorities be free from external influence and not take nor seek instructions from anybody.

Supervision of compliance by data protection supervisory authorities is crucial and enshrined in Article 8(3) of the Charter. The LED requires Member States to provide data protection supervisory authorities with investigative, corrective and advisory powers, which must be effective. This is a prerequisite for properly enforcing data protection rules and thus achieving the LED's objective of a high level of protection of fundamental rights, in particular as regards the right to the protection of personal data, and for ensuring the free flow of data within the EU. The data protection supervisory authorities need to have equivalent powers throughout the EU, in order for them to perform their tasks as required by the LED[52].

All Member States have provided their authorities with the investigative powers specified in the LED and a majority of Member States have also provided them with other powers (e.g. to conduct audits, enter premises, make copies of data and seize objects[53]). As a consequence, almost all data protection supervisory authorities found that they have effective investigative powers.

Almost all Member States have provided for the corrective powers specified in the LED[54]. Many have done so by closely following the wording of the LED, while several have used very broad wording that might be reasonably interpreted as encompassing all the powers set out in the LED.

---

[51] Section 1 of Chapter VI LED.
[52] Recitals 7 and 82 LED.
[53] See also paragraph 23 of the EDPB's contribution to the evaluation of the LED: 24 Member States provided for the power to obtain access to any premises of the controller and the processor, and to any data processing equipment and means; 21 Member States provided for an audit process and 9 Member States provided for other powers (e.g. seizure of objects, request for a hearing before the data protection supervisory authority and request for executive assistance from the police).
[54] Points (a) to (c) of Article 47(2) LED.

In addition, the majority of Member States' laws give data protection supervisory authorities the power to impose administrative fines[55].

Not all Member States have given their data protection supervisory authorities the power to bring infringements of the national laws adopted to transpose the LED to the attention of judicial authorities and to commence or otherwise engage in legal proceedings. Such power is important and complements the other means available to the data protection supervisory authorities to effectively ensure a high level of protection of individuals' fundamental rights and in particular their right to the protection of their personal data.

2.2.3 Remedies

All Member States provided for the right to lodge a complaint with their relevant supervisory authority[56]. Most national laws provide for a time limit for initiating such a complaint. It is important that this time limit does not impede the data subjects' right in this respect.

In line with the LED[57], all Member States provide for a judicial remedy against the decisions of the supervisory authority, without prejudice to any other administrative or non-judicial remedy available in their legal systems. A judicial remedy is available in all Member States but two Member States[58] where a supervisory authority does not handle a complaint or inform the data subject within 3 months on the progress or outcome of the complaint[59].

Most Member States also provide for a judicial remedy against the data controller and the processor[60] in the case of an alleged violation of the LED. However, several national transposing laws do not provide for the right of the data subject to mandate not-for-profit bodies, organisations and associations to lodge a complaint with a supervisory authority or initiate a judicial remedy on their behalf[61].

2.2.4 Time limits for storage and review

Member States' approaches to transposing the LED's time limits for the storage and review of personal data[62] vary widely. The majority of national data protection acts that transpose the LED only meet the general requirement of Article 5 LED. This means that it is for the sectoral law to

[55] 18 Member States provided that possibility: Bulgaria, Czechia, Estonia, Greece, Croatia, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Austria, Portugal, Romania, Slovakia and Sweden. The data protection supervisory authorities in three Member States (Estonia, Latvia and Austria) may impose fines on natural persons (e.g. employees) or on private entities (i.e. private entities that are data processors).
[56] Article 52 LED.
[57] Article 53 LED.
[58] Finland and Sweden.
[59] Article 53(2) LED.
[60] Article 54 LED.
[61] Article 55 LED.
[62] Article 5 LED.

actually set time limits for the erasure of personal data, or for a periodic review of the need to store personal data. A few Member States transpose the provision by laying down the time limits in sectoral legislation.

In some Member States, however, the law leaves it for the competent authority to set up the time limits. In some instances, the law does not lay down any criteria for the periodic review nor do they require that such criteria shall be provided by other laws and/or it do not provide that procedures to ensure that the time limits are observed shall also be laid down in national law.

It is noted that the Bulgarian Supreme Administrative Court has recently requested the CJEU to reply to its preliminary request on the interpretation of Article 5 LED regarding the time limits for storing data[63].

2.2.5 Legal basis for processing, including special categories of personal data

The majority of Member States provide – using wording that often closely matches Article 8 LED – that the legal basis for processing must be laid down in EU or Member State law. However, some national data protection acts transposing the LED do not reflect the requirement that the personal data to be processed and the purposes of processing should be set down in law[64]. Other national data protection acts transposing the LED do not contain all provisions corresponding to Article 8. It is for the national legislation to provide for the basis of processing and comply with the requirements of Article 8. In addition, merely repeating the general requirements of Article 8 LED in national law cannot be considered a sufficient legal basis for a specific processing operation: national law must specify which authority is competent to process the personal data, the public tasks it performs that justify such processing, and the purpose of the processing.

As regards the processing of special categories of personal data[65], most Member States require strict necessity as a prerequisite of processing. Most Member States also provide the same legal grounds for processing sensitive data as are set out in Article 10 LED (processing authorised by law; to protect the vital interest of the data subject or of another natural person; or relate to data manifestly made public by the data subject). In a few Member States, the transposing laws provide for some additional grounds for data processing (e.g. when the processing of such data is necessary in order to avert or prevent a danger that directly threatens the life, physical integrity or assets of persons, or to protect the health or interests of the data subject or another person). When the national data protection act transposing the LED does not provide the necessary safeguards for the rights and freedoms of the data subjects (as is the case in some Member States), such safeguards must be provided by the sectoral laws.

---

[63] Request for a preliminary ruling in *NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR - Sofia*, C-118/22.
[64] Article 8(2) LED.
[65] Article 10 LED.

A few national transposing laws refer to consent in relation to processing personal data, including processing of special categories of personal data. It is important to recall that, while Member States are not precluded from providing in their national law that the data subject may agree to the processing of their personal data for LED purposes, this consent can only serve as a safeguard and cannot constitute the legal basis for such processing. The discussions on this issue indicate that it would be useful to have more guidelines on the role of consent in the context of the processing of personal data for criminal law enforcement purposes.

2.2.6 Automated decision-making

All the Member States' transposing laws include provisions prohibiting a decision based solely on automated processing, unless it is provided by law[66]. Most Member States' transposing laws require that such decisions are not based on special categories of personal data unless suitable safeguards are provided[67]. They also prohibit profiling that results in discrimination[68]. However, some national legislation does not refer to appropriate safeguards for the rights and freedoms of the data subject in cases where automated decision-making is authorised by law. More specifically, not all Member States provide for the right to obtain human intervention on the part of the controller, or do not require suitable measures to safeguard the data subject's rights and/or freedoms and legitimate interests.

2.2.7 Data subject rights

All Member States have chosen to make use of the possibility given by the LED to restrict data subjects' right of access to their personal data[69]. Most Member States also provide for restrictions of other data subject rights[70]. The national data protection acts transposing the LED often only follow the general language of the LED without further specifying the circumstances or the conditions in which the restrictions are to apply. In such cases, these circumstances and conditions have to be specified in sectoral legislation otherwise it would give data controllers discretion in applying these restrictions.

Most Member States comply with the LED requirement to enable data subjects to exercise their rights via the data protection supervisory authority[71]. Most Member States have used the option to stipulate that data subjects' rights are to be exercised in accordance with national law in the context of national criminal investigations and proceedings[72].

---

[66] Article 11(1) LED.
[67] Article 11(2) LED.
[68] Article 11(3) LED.
[69] Article 15(1) LED.
[70] Articles 13(3) and 16(4).
[71] Article 17 LED.
[72] Article 18 LED.

Several Member States' transposing laws do not reflect all the LED's specific requirements regarding the way in which data subjects' rights are to be exercised (e.g. format and communication means of the replies, absence of charge).

There is a pending preliminary ruling[73] raised by a German court concerning the interpretation of the restrictions to data subjects' right of access to their data (Article 15 LED in light of Article 54 LED), and the right to an effective judicial remedy under Article 47 of the Charter and the freedom to choose an occupation under Article 15 of the Charter.

2.2.8 Some important provisions specific to the LED

Some LED provisions are specific to the criminal law enforcement context and have no equivalent in the GDPR.

Categories of data subjects

The LED obliges Member States to require a data controller to draw a distinction, where applicable and as far as possible, between the data of different categories of data subjects, and to provide examples of those categories (e.g. a person for whom there are serious grounds for believing that they have committed or are about to commit a criminal offence (a 'suspect'))[74]. Some Member States' laws do not specify (to some extent or at all) the categories listed by the LED. When specifying the category of 'suspects', some national laws do not require that there should be 'serious grounds for believing the persons have committed or are about to commit a criminal offence'. The forthcoming CJEU ruling in the pending case *Ministerstvo na vatreshnite raboti v B.C.* will further clarify the interpretation of the LED as regards categories of data subjects, including the requirement that categorising a data subject as a suspect should be conditional upon the existence of 'serious grounds for believing that they have committed or are about to commit a criminal offence'[75].

Distinction between classes of personal data and verification of its quality

Member States have to provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments[76]. They also have to take measures to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. Where incorrect data has been transmitted, recipients should be notified without delay and in such cases the personal data is to be rectified, erased or its processing restricted. While most Member States have transposed this requirement, some of the required specific measures are not explicitly provided for under several national transposing laws.

---

[73] Request for a preliminary ruling in *TX v Bundesrepublik Deutschland*, C-481/21.
[74] Article 6 LED.
[75] Request for a preliminary ruling in *Ministerstvo na vatreshnite raboti v B.C.,* C-205/21.
[76] Article 7 LED.

Logging

A total of 12 Member States[77] have used the option to postpone bringing their automated processing system in line with the logging requirements until May 2023[78].

Most Member States provide for logs to be kept for processing operations in automated processing systems[79]. Some national laws do not require all types of operations to be logged. The LED lays down the minimum types of information that logs must contain. Some national laws have not included all the required types of information (e.g. the reason for consultation or disclosure of personal data).

3 FIRST LESSONS FROM THE APPLICATION AND FUNCTIONING OF THE LED

3.1 Complaints and positive impact on data subjects' rights

The LED ensures the protection of the fundamental rights and freedoms of individuals, and in particular, the right to data protection. It provides a comprehensive framework for the rights of the data subject and how these rights can be exercised, including their right to information, to access, rectify or erase their personal data as well as providing for the restriction of processing. The LED has increased data subjects' understanding of their rights and how they can exercise them, and this is reflected by an increase in the number of requests made to competent authorities. Practice has shown that, among the rights conferred to data subjects under the LED, it is the right of access and erasure that are the most frequently invoked with competent authorities[80].

The LED allows limits to be placed on certain rights (the right of access[81] and the right to rectification or erasure[82]) and on the information a data controller must provide to the data subject in relation to personal data that has been processed[83]. Data subjects can request data protection supervisory authorities to review a competent authority's restriction of the right in question or ask them to verify whether the restriction was carried out in accordance with the LED (indirect exercise of the right)[84].Approximately half of data protection supervisory authorities report that they have received such a request[85]. Practice shows that the number of requests received can vary significantly (e.g. one such request was received in Croatia, but more

[77] Germany has made use of the option for certain laws transposing the LED at federal and Länder level.
[78] Article 63(2) LED.
[79] Article 25 LED.
[80] Council position and findings on the application of the LED, paragraph 15.
[81] Article 15 LED.
[82] Article 16 LED.
[83] Article 13 LED.
[84] Article 17 LED.
[85] Four data protection supervisory authorities do not collect statistics on requests received under Article 17 LED.

than 1500 were received in France)[86]. While data protection supervisory authorities determined, following a verification or a review of these complaints, that the majority of requests were inadmissible, in several cases, the data controller was ordered either to rectify or erase the personal data, or to restrict the processing of personal data, thereby ensuring the proper application of the restrictions[87].

The LED provides for a not-for-profit body, organisation or association to lodge a complaint on behalf of a data subject. However, it appears to be underused (only four data protection supervisory authorities reported that they had received such a complaints from a representative body[88]). Similarly, civil society organisations reported only a small number of requests to file such a complaint[89].

Individuals are also increasingly using their right to lodge complaints with data protection supervisory authorities, including in cases where competent authorities limit the exercise of data subjects' rights. More than a third of data protection supervisory authorities reported an increase in the number of complaints received following the transposition of the LED in their Member States[90]. Some of the most frequent complaints received by data protection supervisory authorities concerned the limitation to the right of access[91], the right to rectification or erasure[92], and the right to information and the limitations thereto[93]. These were followed by complaints related to the storage limitation principle, which requires competent authorities to keep personal data for no longer than necessary, and to the right to information.

3.2 Increased awareness of data protection within competent authorities

The Member States report that the introduction of the LED has had and continues to have a major impact on competent authorities' awareness of the importance of data protection[94]. Several data protection supervisory authorities expressed their opinion that the LED's biggest impact has been to increase awareness of and focus on data protection issues and data subjects' rights[95]. This was also demonstrated by exchanges between data protection supervisory authorities and competent authorities on data subject rights and the modalities for exercising those rights[96].

---

[86] These concern requests made since the transposition of the LED until December 2021. EDPB contribution to the evaluation of the LED (individual DPA answers).
[87] EDPB contribution to the evaluation of the LED, paragraph 50.
[88] EDPB contribution to the evaluation of the LED, paragraph 33.
[89] Three organisations (in the context of the replies to the questionnaires sent to them by the Fundamental Rights Agency) reported that they had received one request and one organisation reported that it had received more than one request.
[90] EDPB contribution to the evaluation of the LED, paragraph 31.
[91] Article 15 LED.
[92] Article 16 LED.
[93] Article 13 LED.
[94] Council position and findings on the application of the LED, paragraph 21.
[95] EDPB contribution to the evaluation of the LED (individual DPA answers).
[96] EDPB contribution to the evaluation of the LED, paragraph 40 and Council position and findings on the application of the LED, p. 9.

Some competent authorities reported that they had allocated more resources to data protection as a result[97]. This included investing in the incorporation of the principle of privacy by design and by default in their IT systems, establishing data retention periods, applying the principle of data minimisation, and reporting breaches. Subsequently, the overall security of data processed is reported to have improved[98].

Training and awareness-raising activities by data protection supervisory authorities also contributes to the proper implementation of the LED, and supervisory authorities are tasked with raising awareness among data controllers and processors of their obligations under the LED[99].

Many data protection supervisory authorities raise awareness by publishing guidelines. Some of the topics covered by the different data protection supervisory authorities include: assisting the judiciary, offices of the prosecutor and police authorities in complying with the principle of accountability; exchanging personal data with the police; appointing a data protection officer; conducting a data protection impact assessment; processing data in criminal areas such as organised crime and terrorism; keeping records of processing activities and logging; performing video surveillance; providing data subjects with information; notifying data breaches; controllers' obligations; and the exercise of rights by individuals.

However, eight data protection supervisory authorities have not yet issued any guidance and/or practical tools to support competent authorities and processors to comply with their obligations.

Furthermore, 12 data protection supervisory authorities have not provided any training or carried out awareness-raising activities for competent authorities or processors under the LED[100]. Of the data protection supervisory authorities that did carry out such activities, the most frequent topics included: data processing by the police, prosecution offices, judicial and correctional authorities; definition of the respective areas of application of the GDPR and the LED; use of personal data from social media networks; processing of data in police files; video surveillance techniques and big data; handling of data subject rights; and processing of prisoners' personal data[101].

Another innovation of the LED is the requirement for data controllers to designate a data protection officer (DPO) whose duties include, among other tasks, informing and advising on data protection requirements, monitoring compliance with the LED, advising on data protection impact assessments and monitoring its performance[102]. This has resulted in competent authorities becoming more aware of their data protection obligations as well as having a positive impact on

[97] EDPB contribution to the evaluation of the LED paragraph 70.
[98] EDPB contribution to the evaluation of the LED paragraph 70.
[99] Article 46(1)(d) LED.
[100] EDPB contribution to the evaluation of the LED, (individual DPA answers).
[101] EDPB contribution to the evaluation of the LED, paragraphs 41-42.
[102] Articles 32-34 LED.

competent authorities' compliance with data protection rules, as the Council has also recognised[103].

It is important to invest in developing and maximising DPOs' expertise and knowledge in order to help competent authorities apply the LED consistently[104]. The Commission has therefore established and facilitates the Network for the Data Protection Officers of competent authorities, Justice and Home Affairs agencies and the European Public Prosecutor's Office. The Network is a permanent initiative which focuses on the application of the LED by the competent authorities of the Member States. It aims to provide a platform for cooperation and the exchange of expertise between the Member States' DPOs. The Europol Data Protection Experts Network (EDEN) and national DPO networks for competent authorities are important initiatives that help competent authorities DPOs to promote the exchange of best practices and information on the LED's application.

3.3 Improved data security but divergences in data breach notifications

The LED has improved the security of personal data by requiring competent authorities to take measures to achieve specific security objectives. For example, it requires competent authorities to carry out data protection impact assessments when a data processing activity is likely to result in a high risk to the data subjects' rights and freedoms. The impact assessments involve identifying risks and measures to mitigate them. This requirement, as well as compelling adherence to the data protection by design and default principle and data breach notification requirements brought about an improvement on the security of personal data processing[105].

The Council has also recognised this, finding that the LED has improved the level of data security including through security plans; updating of IT systems and organisational measures; data protection impact assessments; and requiring competent authorities to maintain logs for particular processing operations[106].

The LED sets out the circumstances in which data controllers must notify their data protection supervisory authority and the data subject concerned of a personal data breach[107]. Despite this obligation, there is a wide disparity in the number of data breaches that have been notified to data protection supervisory authorities since the LED was introduced[108]. Six data protection supervisory authorities reported that they had received no data breach notifications[109] and several others reported that they had received very few such notifications. For example, the Italian

[103] Council position and findings on the application of the LED, paragraph 22.
[104] Council position and findings on the application of the LED, paragraph 25.
[105] EDPB contribution to the evaluation of the LED, paragraphs 70 and 71, and individual DPA responses (Germany, Finland, France, Hungary, Malta).
[106] Council position and findings on the application of the LED, paragraph 26.
[107] Articles 30 and 31 of the LED.
[108] The figures include all the data breaches reported between the transposition of the LED and December 2021. The data was gathered from the data protection supervisory authorities in December 2021.
[109] Spain, Croatia, Lithuania, Portugal, Slovakia and Slovenia.

authority reported just three data breach notifications and the French authority reported eight, but the Dutch authority reported over 500.

This difference in the number of reported data breach notifications suggests (after taking into account factors such as population size) that there appears to be divergent practices between the Member States' competent authorities as regards what is considered a breach and when it needs to be reported to a Data Protection Supervisory Authority. The Commission also noted this in its report on the GDPR[110]. The EDPB recently published guidelines on breaches under the GDPR[111]. These guidelines while not directly applicable, are also of relevance for LED data breaches. They should therefore contribute to a more uniform approach to the handling of LED data breaches across the Member States.

3.4 Supervision by data protection supervisory authorities

3.4.1 Resources of the data protection supervisory authorities

Providing each data protection authority with the necessary human, technical and financial resources, premises and infrastructure is a prerequisite for the effective performance of their tasks and exercise of their powers, and therefore an essential condition for their independence[112]. The Commission has consistently stressed the fact that the Member States are obliged to allocate sufficient human, financial and technical resources to data protection supervisory authorities[113]. The Council has also specifically called on the Member States to allocate sufficient human, technical and financial resources to the data protection supervisory authorities[114].

However, the overall increase in the data protection supervisory authorities' staff in recent years[115] does not seem to concern LED-related tasks. The number of staff working on the LED has remained the same or has even decreased in half of the data protection supervisory

---

[110] Commission Staff Working Document, Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020) 264 final.
[111] EDPB Guideline 01/2021 on examples regarding personal data breach notification, adopted on 14 December 2021. https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf
[112] Article 42(4) LED.
[113] Communication from the Commission to the European Parliament and the Council, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', COM(2020) 264 final.
[114] Council position and findings on the application of the LED, paragraph 12.
[115] Contribution of the EDPB to the evaluation of the GDPR under Article 97, 18 February 2020, pp. 26-29. https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf;
EDPB overview on resources made available by Member States to the data protection authorities and on enforcement actions by the data protection authorities ('EDPB overview on resources'), 5 August 2021, pp. 4-5. https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en.

authorities[116]. Any increase has been very modest, amounting to fewer than two persons in full-time equivalents ('FTEs') on average[117]. In almost half of the data protection supervisory authorities (including those with a total number of employees of more than 100 FTEs), between less than 1% and 7% of the total staff work on the LED[118]. In absolute numbers, around half of the data protection supervisory authorities allocate between 1 to 4 FTEs to LED tasks, and eight data protection supervisory authorities allocate between 7 and 15 FTEs to LED tasks. However, one data protection supervisory authority has 53 FTEs working on the LED[119]. Similarly, the EDPB Secretariat has dedicated fewer than 1.5 FTEs to issues entirely related to the LED.

This situation is not satisfactory, even if 10 data protection supervisory authorities have indicated that they have sufficient financial, human and technical resources[120]. On the other hand, 16 data protection supervisory authorities found that they have insufficient resources. Of these authorities, some noted that this negatively impacted their own-initiative investigations[121] , their handling of complaints[122], the inspection of large-scale IT systems (SIS, VIS) and the issuing of opinions on their own initiative[123]. Indeed, the sector's specific characteristics mean that the effective enforcement of the LED requires systematic inspection of processing activities that are often complex, and that it is not enough to rely on individual complaints (which are far fewer in number than for the GDPR)[124].

Furthermore, the data protection supervisory authorities have pointed to the lack of IT expertise to address the ever increasing complexity of IT technologies used in the law enforcement area[125].

3.4.2 Use of powers

Use of corrective powers

A total of 19 data protection supervisory authorities applied their investigative powers, either on their own initiative or on the basis of a complaint[126]. Data protection supervisory authorities

[116] EDPB contribution to the evaluation of the LED, paragraph 65 and figure on Q41, p. 20.
[117] Germany indicated a significant increase from 33 to 53 FTEs between 2017 and 2021.
[118] EDPB contribution to the evaluation of the LED, figure on Q41, p. 20. EDPB overview on resources, p. 5.
[119] EDPB contribution to the evaluation of the LED, figure on Q41, p. 19.
[120] Belgium, Denmark, Ireland, Greece, Latvia, Luxembourg, Hungary, Malta, Austria and Finland.
[121] Germany and France.
[122] France and Sweden.
[123] The Netherlands.
[124] Ireland received 135 LED-related complaints since 2018, Hungary has received 141 since 2018, and Denmark has received 223 since 2017. By contrast, there have been thousands of GDPR-related complaints (see EDPB overview on resources, p. 10.)
[125] EDPB contribution to the evaluation of the LED, paragraph 69.
[126] The data protection supervisory authorities of Ireland, Malta and the Netherlands reported that they conducted investigations on their own initiative. The data protection supervisory authorities of Greece, Spain, Lithuania and Hungary conducted investigations on the basis of complaints. The data protection supervisory authorities of Belgium, Bulgaria, Denmark, Germany, France, Italy, Luxembourg, Austria, Poland, Slovenia and Sweden conducted investigations both on their own initiative and on the basis of complaints.

reported difficulties only in very few cases (e.g. when a data controller did not provide all the relevant information or refused access to information)[127].

The same 19 data protection supervisory authorities also applied their corrective powers. By far the most frequently used power was that of issuing orders to bring the processing in compliance with the law, including orders to rectify or delete personal data or to restrict its processing. The data protection supervisory authorities used this power in 114 cases. The fact that this power to order a temporary or definitive limitation (including a ban) on processing was used in only four cases[128] shows that the data protection supervisory authorities have used these powers carefully.

Use of advisory powers

Pursuing systematically prior consultations and requesting the opinion of the data protection supervisory authorities on draft legislative and administrative measures are an effective means to ensure a high level of protection of the right to the protection of personal data and decrease the number of subsequent complaints. Prior consultation of the data protection supervisory authorities is of particular importance when using new technologies which can have a significant impact on fundamental rights.

Half of the data protection supervisory authorities reported that they had been consulted on data protection impact assessments. The number of prior consultations varies between Member States. Some authorities were consulted only once while another authority received 59 prior consultations[129]. In most of these cases the data protection supervisory authorities provided written advice and in some cases used their corrective powers in relation to the processing - in particular, they issued warnings or ordered measures to bring the data processing into compliance with the law. In one case, the data protection supervisory authority issued a negative opinion which appears to have had the same effect as a ban on processing.

In addition, it appears that the data protection supervisory authorities also deal with requests for advice, outside the prior consultation procedure. The most common type of issue on which competent authorities approached data protection supervisory authorities for advice related to specific types of processing (in particular the use of new technologies, mechanisms or procedures, closely followed by appropriate security measures, the processing of special

[127] The German and Hungarian data protection supervisory authorities stated that they had not received all the necessary information and/or that the controller denied them access to necessary information. The German authorities mentioned that a similar power to Article 58(1)(a) GDPR is not provided.
[128] EDPB contribution to the evaluation of the LED, paragraph 30, and also the individual replies of the authorities of Austria and Luxembourg.
[129] The Danish and Lithuanian data protection supervisory authorities reported that they had been consulted only once. The Belgian data protection supervisory authority received 59 prior consultations.

categories of personal data, the determination of the legal basis for the processing, the storage limitation principle and appropriate time limits[130]).

Furthermore, 22 data protection supervisory authorities issued opinions to their national parliaments and governments on legislative and administrative measures relating to the processing of personal data. Several indicated that they are occasionally consulted[131].

3.4.3 Judicial review of data protection supervisory authorities' actions

Almost half of the data protection supervisory authorities indicated that in a small number of cases, they faced judicial proceedings regarding their decisions or inaction. The proceedings were initiated mainly by data subjects and in a few cases by competent authorities[132]. Several cases had been declared inadmissible by the courts or had been withdrawn by the applicants. The court upheld the data protection supervisory authority's decision in most of the remaining cases, but overturned it in some cases (and other cases were still pending). The small number of judgments to date means that it is not yet possible to detect a clear trend.

3.4.4 EDPB guidelines

Consistency and a high level of protection among Member States is key in order to ensure effective judicial cooperation in criminal matters and police cooperation[133]. The LED provides for the EDPB to issue guidelines, recommendations and best practices (on its own initiative or at the Commission's request) in order to ensure that the Member States apply the LED consistently. The EDPB has produced LED-specific guidance relevant for Chapter V (international transfers)[134]; guidelines on the use of facial recognition technologies[135]; and (in its former capacity as the Article 29 Working Party) an opinion on some key issues of the LED[136].

Many of the EDPB's guidelines on the GDPR are also relevant for the LED to the extent that they rely on common concepts or technologies. Such guidelines include those on the concept of

---

[130] EDPB contribution to the evaluation of the LED, paragraph 39.
[131] The data protection supervisory authorities of Czechia, Greece, Croatia Latvia and Sweden reported that they did not issue opinions. The data protection supervisory authorities of Greece, Croatia, Latvia, Poland, Romania, Slovenia and Slovakia were consulted only occasionally.
[132] This observation is based on the replies received from the data protection supervisory authorities of Belgium, Bulgaria, Germany, Estonia, Ireland, Italy, Hungary, the Netherlands, Austria, Poland, Finland and Sweden.
[133] Recital 7, LED.
[134] EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted 2 February 2021.
https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.
[135] EDPB Guideline 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted on 12 May 2022, version for public consultation, available at https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
[136] Article 29 Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP 258, adopted on 29 November 2017, available at https://ec.europa.eu/newsroom/article29/items/610178/en.

data controller and processor[137], on data subject rights[138], on personal data breach notification[139], on data protection impact assessment[140], on data protection by design and by default[141], and on individual automated decision-making[142].

Producing comprehensive and practical guidelines requires significant work and resources, but guidance is essential (as the Council has also noted[143]). It is therefore very positive that the EDPB has indicated that it will soon provide additional guidance, including on the concept of the data protection supervisory authorities' effective investigative and corrective powers, and on international transfers that are subject to appropriate safeguards.

EDPB guidelines can also reduce the data protection supervisory authorities' workload (e.g. tasks such as advising data controllers or dealing with complaints). For instance, several of the issues addressed in the Article 29 Working Party's opinion on some key issues of the LED (such as appropriate time limits, the legal basis of processing, conditions for processing of special categories of data) are also some of the most frequent issues on which competent authorities have asked the data protection supervisory authorities for advice[144].

3.4.5 Mutual assistance

To ensure the consistent application of the LED, data protection supervisory authorities are required to provide mutual assistance to one another. This includes assistance in the form of information requests and requests to carry out consultations, inspections and investigations[145].

---

[137] EDPB Guideline 07/2020 on the concepts of data controller and processor in the GDPR, adopted on 7 July 2021, available at https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.
[138] EDPB Guideline 01/2022 on data subject rights - right of access, adopted on 18 January 2022, version for public consultation, available at https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[139] Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, WP 250rev.01, last revised on 6 February 2018, and endorsed by the EDPB on 25 May 2018, available at https://ec.europa.eu/newsroom/article29/items/612052/en; EDPB Guidelines 01/2021 on examples regarding personal data breach notification, adopted on 14 December 2021, available at https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.
[140] Article 29 Working Party Guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP 248rev.01, last revised on 4 October 2017, and endorsed by the EDPB on 25 May 2018, available at https://ec.europa.eu/newsroom/article29/items/611236.
[141] EDPB Guideline 4/2019 on Article 25 data protection by design and by default, adopted on 20 October 2020, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
[142] Article 29 Working Party Guideline on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP 251rev01, last revised on 6 February 2018, and endorsed by the EDPB on 25 May 2018; available at https://ec.europa.eu/newsroom/article29/items/612053/en.
[143] Council position and findings on the application of the LED, paragraph 14.
[144] EDPB contribution to the evaluation of the LED, paragraph 39.
[145] Article 50 LED.

However, mutual assistance has been very rarely utilised to date. Only six data protection supervisory authorities have used it, primarily in response to information requests received from other data protection supervisory authorities. The majority of data protection supervisory authorities indicated that they have received only one request for information. All of these data protection supervisory authorities reported that they complied with the request received. The voluntary mutual assistance exchange, which does not have a legal deadline or strict obligation to respond, has not been used either. The EDPB has stated that it will publish guidelines on the mutual assistance framework under the GDPR and the LED[146].

3.5 Flexible instrument for international data transfers

Chapter V of the LED covers transfers of personal data to competent authorities in third countries and international organisations. This chapter essentially ensures that there is continuity of protection when personal data is transferred from a Member State to a third country or international organisation for law enforcement purposes. As noted above, such continuity of protection is an important condition for rapid, effective and legally certain law enforcement cooperation between trusted partners.

In particular, under the relevant rules of the LED[147], international transfers between competent authorities within the meaning of the LED must be based on one of the various transfer tools set out in Articles 36 to 38 of the LED (where the data originates from another Member State, the transfer also requires the previous authorisation of that Member State). These tools include adequacy decisions, transfers based on appropriate safeguards and the use of derogations in specific situations. Article 39 LED also allows for direct transfers to recipients that are not criminal law enforcement authorities, that are established in third countries, in individual and specific cases, and subject to several conditions.

3.5.1 Adequacy decisions

The Commission has accelerated its work to achieve the full potential of the tools available under the LED. This included adopting, for the first time, an 'adequacy decision' covering data processing activities for law enforcement purposes under Article 36 LED, with the United Kingdom in June 2021[148]. This adequacy decision enables the safe and free flow of personal data to the competent authorities of the third country concerned, without the need for any further safeguards or specific authorisation (unless another Member State from which the data were

---

[146] EDPB Work Programme 2021 / 2022, edpb_workprogramme_2021-2022_en.pdf (europa.eu).
[147] See Article 35(3) and Recital 64 LED. As regards onward transfers, see Article 35(1)(e) and Recital 65 LED.
[148] Commission Implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf.

obtained has to authorise the transfer[149]). The adequacy decision for the United Kingdom from June 2021 is a crucial foundation for police and judicial cooperation post-Brexit, which, according to the EU-UK Trade and Cooperation Agreement, is based on 'the Parties' long-standing commitment to ensuring a high level of protection of personal data'[150]. Pursuant to Article 36(4) LED, the Commission monitors any development in the United Kingdom's legal framework that might affect this adequacy decision. This adequacy decision with the United Kingdom is set to apply for a period of 4 years from its entry into force, extendable in principle by a further 4 years if the Commission's monitoring confirms that the United Kingdom still maintains an adequate level of protection[151].

In addition, the EDPB has also contributed to the development of this instrument by clarifying the legal standard through guidance on the elements that must be considered when assessing adequacy in the law enforcement context, with the issuance of its Adequacy Referential under the LED[152]. In particular, the third country must ensure enforceable individual rights, effective judicial redress and independent supervision.

The Commission is actively promoting the possibility of adequacy findings with other key international partners, in particular with those countries with which close and swift cooperation is required in the fight against crime and terrorism and with which significant personal data exchanges are already taking place[153]. While no other adequacy decisions have been adopted so far, this is mainly because this instrument has only recently been introduced. In addition, and unlike for data processing by commercial operators, global convergence of data protection rules in the area of criminal law enforcement is only now starting to develop (driven, for instance, by multilateral arrangements such as the modernised Council of Europe Convention 108 or the Second Additional Protocol to the 'Budapest' Convention on Cybercrime). Nevertheless, the experience gained from the adoption of the adequacy decision with the United Kingdom will help to pave the way for similar initiatives in the coming years. The Commission will, as part of its international strategy, consider other possible candidates for future adequacy decisions under the LED and will do so in direct contact with the other relevant EU institutions and bodies[154]. To this end, and in accordance with Recital 68 of the LED, the Commission will pay close attention to the international commitments of the assessed countries relating to the protection of personal

[149] See Article 35(1)(c), Article 35(2) and Recital 66 LED.
[150] See Article 525, paragraph 1, of the TCA.
[151] See paragraphs 172 to 174 of the Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive, 28 June 2021, available at https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en
[152] EDPB, Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021. See also Article 36(2) and recital 67 LED.
[153] See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017), 7 final, pp. 13-14.
[154] Council position and findings on the application of the LED, paragraph 18.

data, including accession to the beforementioned multilateral arrangements or to other law enforcement instruments providing appropriate data protection safeguards.

3.5.2 Appropriate safeguards

The LED contains other transfer instruments in addition to the comprehensive solution of an adequacy decision. The flexibility of this 'toolbox' is reflected in Article 37 LED, which regulates data transfers based on 'appropriate safeguards' regarding the protection of personal data. Such appropriate safeguards may be provided either by a legally binding instrument, or when the controller, based on an assessment of all the circumstances surrounding the transfer, concludes that appropriate safeguards exist (the so-called "self-assessment" for transfers).

In the first years of the LED's application, the Commission in particular worked on binding legal instruments in the form of international agreements providing appropriate safeguards. Such agreements play an important role both in the context of 'traditional' (i.e. cooperation between competent authorities) and other forms of law enforcement cooperation (i.e. cooperation involving third parties such as private companies). They can also serve as a basis for data transfers by Europol and Eurojust under their respective legal frameworks whose rules on international transfers are very similar to the ones under the LED.

Concerning traditional forms of law enforcement cooperation, the Commission is reviewing international agreements adopted before the LED entered into force in order to ensure consistency with the EU's modernised data protection regime[155].

Firstly, the Commission is assessing the data protection provisions contained in Europol's existing cooperation agreements[156] with third countries concluded prior to 1 May 2017, as mandated by Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (hereinafter 'the Europol Regulation)[157]. In line with Article 9 of Protocol No 36 to the Treaty on European Union[158] and the TFEU (on transitional provisions), the legal effects of these agreements have been preserved until those agreements are repealed, annulled or

---

[155] In its Communication on a way forward on aligning the former third pillar acquis with data protection rules the Commission has concluded that several existing agreements do not require further alignment with the LED (e.g. the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto).

[156] For more information on the existing Europol agreements see Europol's website at: https://www.europol.europa.eu/partners-collaboration/agreements.

[157] See Article 25(4) of the 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.53-114.

[158] Consolidated version of the Teary on European Union, OJ C 202, 7.6.2016, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016M%2FTXT-20200301.

amended[159]. The Commission will inform the European Parliament and the Council of the outcome of this assessment and will, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations to amend the respective agreement(s) in accordance with Article 218 TFEU. This is a complex task which involves the assessment of 18 agreements and was delayed by the disruptions caused by the Covid-19 pandemic. The Commission expects to complete its assessment in the second half of 2022.

Consistency of all law enforcement cooperation mechanisms with the rules of the LED is a guiding principle that the Commission also follows when negotiating new agreements for the transfer of personal data by Europol to third countries or international organisations. Since the current Europol Regulation entered into force in 2017, Article 218 TFEU has been the legal basis for such international agreements ensuring adequate safeguards. In 2018 and 2019, the Council adopted nine mandates for the Commission to start negotiations with third countries on behalf of the Union. The Commission has also been authorised to start negotiations on a cooperation agreement with Interpol to cover the exchange of data with several EU bodies and agencies. In all these cases, the Council has addressed negotiating directives to the Commission with a view to ensuring that the necessary safeguards for the protection of personal data and other fundamental rights and freedoms of individuals are included. On this basis, the Commission has already concluded the negotiations with New Zealand, leading to the signing of a cooperation agreement on 30 June 2022. In addition, progress has been achieved in the negotiations with Israel. As regards Turkey, the negotiations are at an advanced stage, but cannot be concluded until Turkey adopts the necessary reforms in its data protection legislation. Similar authorisations were granted in March 2021 for the negotiation of cooperation agreements to allow the exchange of data by Eurojust with 13 third countries.

Secondly, the Commission is conducting the first joint review of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (the Umbrella Agreement). The Umbrella Agreement, which entered into force in February 2017, contains a comprehensive and harmonised set of data protection rules that apply to all transatlantic exchanges between competent authorities. It complements existing EU-US and EU Member State-US agreements between law enforcement authorities, sets a standard of high level of protection for future agreements in this field, and strengthens law enforcement cooperation by facilitating the exchange of information. The joint review seeks to assess the effective implementation of the Umbrella Agreement, in particular as regards the provisions on onward transfer, individual rights and judicial redress. The timeline for the joint review was affected by the disruptions linked to the Covid-19 pandemic, as well as the parallel negotiations on the

[159] Recital 35 of the Europol Regulation.

Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime[160]. The Commission expects that it will be completed in the second half of 2022.

As the first bilateral international agreement with a comprehensive catalogue of data protection rights and obligations, the Umbrella Agreement a reference point for negotiating similar framework agreements with important criminal law enforcement partners[161]. In doing so, the Commission will also take into account relevant developments, including EDPB guidance, case law from the CJEU and the outcome of international negotiations on data protection safeguards in this area (such as, for instance, the Second Additional Protocol to the Budapest Convention on Cybercrime or the Europol agreement with New Zealand[162]).

Thirdly, the Commission has identified the Agreement between the European Union and Japan on mutual legal assistance in criminal matters (the EU-Japan MLAT)[163] as an EU act regulating data processing (transfers) for criminal law enforcement purposes that needs to be amended to ensure appropriate data protection safeguards in line with the LED. Following the Council's adoption of a decision[164] authorising the opening of negotiations to amend the EU-Japan MLAT, the Commission continues to engage with the Japanese authorities with a view to starting negotiations as soon as possible.

Moreover, other forms of cooperation adapted to the specific challenges and needs of criminal investigations in today's digital economy are now also increasingly relied upon. These mainly concern enhanced cooperation in the field of cybercrime and for the collection of evidence in electronic form concerning criminal offences. This cooperation, including direct cooperation with private parties for access to electronic evidence.

The Commission has also engaged with international partners with a view to ensure that these other (important) forms of cooperation can take place based on appropriate data protection safeguards.

---

[160] The Commission, on behalf of the European Union, and the United States were heavily engaged in these negotiations, including in the dedicated data protection subgroup (data protection being one of the most intensely discussed topics).

[161] See the Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017), 7 final, p. 14.

[162] Agreement between the European Union, of the one part, and New Zealand, of the other part, on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of New Zealand competent for fighting serious crime and terrorism.

[163] Agreement between the European Union and Japan on mutual legal assistance in criminal matters (OJ L 39, 12.2.2010, p. 20).https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22010A0212%2801%29.

[164] Council Decision authorising the opening of negotiations with Japan for the amendment of the Agreement between the European Union and Japan on mutual legal assistance matters (document LT 223/21).

Firstly, the Commission represented the EU during the negotiations[165] within the framework of the Council of Europe on a Second Additional Protocol to the 'Budapest' Convention on Cybercrime[166].The Protocol, which was approved by the Council of Europe's Committee of Ministers on 17 November 2021, contains strong safeguards for the protection of fundamental rights, including an article[167] containing detailed provisions on the protection of personal data transferred under the Protocol. These provisions cover all the essential data protection principles, rights and obligations recognised in EU law. These guarantees are complemented by a monitoring provision and by the possibility to suspend transfers in the event of a systematic or material breach of the safeguards contained in the Protocol, for instance, the absence of effective judicial remedies. Through these provisions, it provides appropriate safeguards in line with the requirements of Article 37(1)(a) LED[168]. This is a significant achievement, given the diverse membership of the Budapest Convention, which currently has 66 state parties representing different legal backgrounds and traditions. It will allow Member States' competent authorities to benefit from effective cross-border cooperation in the fight against cybercrime, while ensuring respect for EU values as reflected in the EU Charter of Fundamental Rights, the EU Treaties and EU secondary law. Given the large number of parties to the Budapest Convention, which currently includes countries from around the world, the Protocol will also help to promote high data protection standards for data processing in the area of criminal law enforcement at a global level. The Protocol was opened for signature on 12 May 2022, with a total of 22 Parties to the Budapest Convention (including 13 EU Member States) already signing it.

Secondly, the Commission has initiated negotiations on a bilateral agreement with the United States on cross-border access to electronic evidence for judicial cooperation in criminal matters.[169] This agreement seeks to cover electronic evidence in the form of both non-personal and personal data, including traffic and content data. Importantly, the negotiations also aim at the inclusion of additional data protection safeguards that would complement those in the Umbrella Agreement, taking into account, in particular, the sensitivity of the categories of data concerned

---

[165] Following the approval of a mandate by the Council of the European Union on 6 June 2019. The mandate is available at https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[166] The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was approved by the Council of Europe's Committee of Ministers on 17 November 2021. It was prepared by the Cybercrime Convention Committee (T-CY) between September 2017 and May 2021. The text of the Protocol (certified copy) is available at https://rm.coe.int/1680a4b2e1. The explanatory report to the Protocol is also available at https://rm.coe.int/1680a49c9d

[167] See Article 14 of the Additional Protocol, together with paragraphs 220-287 of the explanatory report.

[168] In its Opinion 1/2022 of 20 January 2022 on the draft Council decisions authorising signature and ratification of the Additional Protocol, the EDPS 'notes positively the many safeguards that have been included in the Protocol.'

[169] Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters. The mandate is available at the following link: https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf.

as well as the requirements of the transfer of electronic evidence directly by service providers. Progress on these negotiations will largely depend on the progress of the ongoing legislative process on the EU's e-evidence package[170].

These various initiatives by the Commission to develop international instruments facilitating law enforcement cooperation with international partners while also ensuring appropriate data protection safeguards have been supported by the work of the EDPB and the EDPS. This work includes the EDPB's statement on the draft Second Additional Protocol to the Budapest Convention[171] and the EDPS's opinions on the draft negotiating mandates for international agreements under Article 218 TFEU that would allow Europol and Eurojust to exchange personal data with third countries or international organisations[172]. The EDPB also issued a statement inviting Member States to assess and, where necessary, review international agreements involving international transfers of personal data[173]. This statement concerns agreements that were concluded prior to before 6 May 2016, including in the area of criminal law enforcement), and invites Member States to determine whether further alignment with EU data protection legislation and case law is required.

Article 37 of the LED also permits international data transfers based on self-assessment by a competent authority as to whether a third country (or an international organisation) has appropriate data protection safeguards. In these cases, the authority has to document the transfer (including its date and time, information on the receiving authority, justification of the transfer and the personal data transferred) and the documentation must be made available to the supervisory authority on request (Article 37(3) LED). Feedback provided by Member States[174] indicates that this tool has rarely been used.

---

[170] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018)225 final, and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018)226 final.

[171] EDPB, Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), adopted on 2 February 2021, available at https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

[172] EDPS, Opinion 04/2021 on the review of Europol's mandate, adopted on 8 March 2021, available at https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-europol-regulation_en.

[173] EDPB, Statement 04/2021 on international agreements including transfers, adopted on 13 April 2021. It is available at https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf

[174] See the Council Presidency Report on the Exchange of police data with third countries - Experiences in the application of Article 37 of Law Enforcement Directive, The EDPB has announced that it will include the conclusions from the Presidency report along with further information and comments from the Member States in its efforts to develop guidance on Article 37 of the Directive. See the letter from the Chair of the EDPB to the

To allow Member States to make full use of the LED's transfer toolbox, it is important that the EDPB intensifies its ongoing work on the various transfer mechanisms. Among other things it should provide guidance on the mechanisms included in Article 37(1) LED, notably on the transfers based on self-assessments by competent authorities. The Council has also stressed this need[175].

3.5.3 Use of derogations

Finally, the so-called 'derogations' provide an important ground for transfers under certain conditions, laid down in Article 38 of the LED. These conditions strike a balance between privacy considerations and the operational needs of competent authorities. In particular, Article 38(1) allows for transfers, and even categories of transfers, of personal data where this is necessary for the prevention of an immediate and serious threat to public security[176] or, in individual cases, for the prevention, investigation, detection or prosecution of criminal offences[177]. In contrast to derogations under Article 49 of the GDPR, no guidance currently exists for derogations under Article 38 of the LED.

3.5.4 Effective police and judicial cooperation across borders

The LED has become an international reference point for data protection in the law enforcement context and has acted as a catalyst for countries around the world to consider introducing modern privacy rules in this area. This is a very positive development that brings new opportunities to better protect individuals in the EU when their data is transferred abroad for law enforcement purposes while, at the same time, facilitating data flows that can help fighting against crime.

More generally, it is important to ensure that when companies active in the European market receive direct cooperation requests to share data for law enforcement purposes, they can do so without facing conflicts of law and in full respect of EU fundamental rights[178]. To improve such transfers, the Commission is committed to developing appropriate legal frameworks with its international partners to avoid conflicts of law and support effective forms of cooperation, notably by providing for the necessary data protection safeguards and thereby contributing to a more effective fight against crime.

Permanent Representation of the Federal Republic of Germany to the European Union of 26 February 2021 (document 13555/1/20).

[175] See the Council position and findings on the application of the LED, paragraph 20.

[176] Article 38(1)(c) LED.

[177] Article 38(1)(d) LED.

[178] As an example, the Second Additional Protocol to the Budapest Convention could be considered as an international agreement for the purposes of Article 48 GDPR.

Against this backdrop, the Commission has engaged in bilateral, regional and multilateral settings to actively promote international convergence in data protection standards for criminal law enforcement cooperation. During its dialogues with several foreign partner countries on ongoing reforms of data protection laws, the Commission's services have engaged in different ways (e.g. submissions in response to public consultations, participation in parliamentary hearings, and dedicated meetings with government representatives and policy-makers) on the development of rules on the processing of personal data by competent authorities.

In a regional and multilateral setting, the Commission, for example, supports capacity-building projects in the context of the implementation of the Council of Europe's Budapest Convention on Cybercrime[179] These projects include the GLACY+ programme to strengthen states' capacity to apply legislation on cybercrime and to enhance their ability for effective international cooperation in line with the Budapest Convention and its additional protocols. This also involves developing data protection legislation for data processing in this area. The programme currently supports 17 priority and hub countries in Africa, the Asia-Pacific, Latin America and the Caribbean region.

The Commission has also engaged with Ameripol, a police cooperation organisation bringing together 18 countries of Latin America, in the context of the development a data protection framework for the exchange of information between Ameripol and its member states. This engagement is taking place through EL PAcCTO: Support to Ameripol, a project whose purpose is to improve the level of international cooperation between the police, judicial and prosecutor bodies of the partner countries in the fight against organised crime.

The Commission also promotes the modernised Convention 108 (known as Convention 108+)[180], which is also applicable to data processing activities for criminal law enforcement purposes. This Convention, which is also open to non-members of the Council of Europe, is important not only because it is the only multilateral binding agreement on data protection, but also because through its Convention Committee it provides a forum for the exchange of best practices and the setting of global standards[181]. As part of its international strategy on data flows, the Commission encourages accession by third countries to Convention 108+.

Lastly, the Commission encourages greater convergence at international level by sharing our experience with partners on the data protection aspects of criminal law enforcement cooperation. The Commission's "Data Protection Academy", a part of the project "International Digital

---

[179] See: https://www.coe.int/en/web/cybercrime/glacyplus.

[180] Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018 (Convention 108+), available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[181] See, for example, the Practical guide on the use of personal data in the police sector, available at https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

Cooperation - Enhanced Data Protection and Data Flows", financed by the Foreign Policy Instrument, is a key tool in this endeavour. The Academy was established to foster exchanges between European and third country regulators and to improve cooperation on the ground. The academy's activities cover all aspects of data protection supervision, including in the field of law enforcement.

4 THE WAY FORWARD

In order to ensure an efficient EU security policy that fully respects the fundamental right to the protection of personal data, the Commission will continue to check that the Member States have correctly transposed the LED and to monitor the application of its provisions.

The LED has significantly contributed to a more harmonised and higher level of protection of individuals' rights and a more coherent legal framework for competent authorities.

The LED has generally been transposed in a satisfactory manner, but a number of issues have been identified. The Commission has already launched infringement procedures regarding both the non-transposition and the non-conformity of national laws with the LED. It will continue to work to ensure full and correct transposition.

The LED has resulted in a higher level of awareness and attention on data protection by national competent authorities, also as regards the security of processing.

Active supervision by data protection supervisory authorities is pivotal to ensure that the objectives of the LED are met in practice. The authorities therefore need to be given all the types of powers required by the LED, together with adequate resources.

At this stage, the focus should be on realising the full potential of the LED. In this context, and given the limited experience with these new rules, the Commission believes that it is too early to consider revising the LED.

The Commission will continue to actively work with all relevant parties in the perspective of the next evaluation due by 2026. It will in the meantime continue to work on ensuring consistency with other EU legislation that is relevant to the processing of personal data for criminal law enforcement purposes.

Legal framework

The Commission will:

- continue to assess the Member States' transposition of the LED and take appropriate action when necessary (including launching infringement procedures);
- pursue bilateral exchanges with Member States;
- ensure that future legislative proposals are consistent with the LED.

Member States should:

- ensure the full and correct transposition of the LED at national level including by specifying the necessary LED requirements when the national data protection acts transposing the LED does not do so.

Supervision by data protection supervisory authorities

Member States should:

- provide data protection supervisory authorities sufficient resources to perform their LED-enforcement tasks;
- ensure that data protection supervisory authorities can exercise all the types of powers set out in the LED;
- systematically consult their data protection supervisory authorities on draft legislation and administrative measures of general application that relate to the protection of personal data, and take due account of their opinions (particularly in the case of new technologies).

Data protection supervisory authorities are invited to:

- make full use of their investigative powers, including by conducting own-initiative inspections;
- collect specific statistics relating to their supervisory activities under the LED;
- make use of the mutual assistance tools and develop practical measures to facilitate requests for assistance, including through the planned EDPB guidelines.

The EDPB is invited to:

- expand the Support Pool of Experts[182] for LED-related tasks.

Supporting competent authorities

The Commission will:

- facilitate discussions and the sharing of experience between Member States and the Commission in the LED Member States Expert Group;
- facilitate the exchange of views between data protection officers through the Network of Data Protection Officers.

Member States are invited to:

- continue efforts to provide training on data protection requirements to competent authorities, including in relation to new technologies.

The EDPB and the data protection supervisory authorities are invited to:

- strengthen their efforts to adopt relevant guidelines (e.g. on the role of consent in the context of processing personal data for criminal law enforcement purposes, and on data subjects'

[182] EDPB Document on Terms of Reference of the EDPB Support Pool of Experts, adopted on 15 December 2020.

rights including their possible limitations), either by adopting new self-standing guidelines or by supplementing the guidelines already adopted for the GDPR.

Cross-border data transfers

The Commission intends to:

- actively promote possible new adequacy decisions with key international partners;
- negotiate new cooperation agreements between Europol and Eurojust, on the one hand, and third countries, on the other hand. Where necessary, it will seek to renegotiate existing Europol cooperation agreements to ensure that they include appropriate data protection safeguards;
- engage in negotiations with Japan with a view to amend the existing EU-Japan Mutual Legal Assistance Agreement to ensure appropriate data protection safeguards;
- pursue and conclude the negotiation of a bilateral agreement with the United States on cross-border access to electronic evidence for judicial cooperation in criminal matters, including by complementing the data protection safeguards guaranteed by the EU-US Umbrella Agreement to reflect the specific context of direct cooperation between law enforcement authorities and service providers;
- explore the possibility of concluding data protection framework agreements for data processing in the area of criminal law enforcement with important criminal law enforcement partners, building on the example of the EU-US Umbrella Agreement.

The EDPB is invited to:

- adopt guidelines in order to further clarify the notion and content of 'appropriate safeguards' (Article 37 of the LED) as well as the use of derogations (Article 38 of the LED).

Promoting convergence and developing international cooperation

The Commission will:

- expand its engagement with international partners with a view to strengthen convergence of data protection rules in the area of criminal law enforcement, including by promoting accession to Convention 108+ as the only binding global agreement on data protection;
- promote bilateral, regional and multilateral cooperation and support capacity-building projects in the field of data protection and police cooperation. This will include training and the exchange of knowledge and best practices through the Data Protection Academy.

The Member States are invited to:

- swiftly ratify the Second Additional Protocol to the Council of Europe's 'Budapest' Convention on Cybercrime, as soon as they are authorised by a Council Decision to do so.