Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (''LED'') under Article 62 LED

Adopted on 15 January 2026

Table of Contents

The European Data Protection Board

Having regard to Articles 51(1)(a)(b) and (h) of the 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., (hereinafter 'the Law Enforcement Directive' or 'the LED'),

Having regard to Article 12(1) and Article 22 of its Rules of Procedure,

Has adopted the following contribution to the European Commission's evaluation of the Data Protection Law Enforcement Directive ('LED') under Article 62 LED:

1 General EDPB policy messages

1 The Law Enforcement Directive ('LED')[1], together with the General Data Protection Regulation ('GDPR')[2] and the Regulation on personal data protection by Union institutions and bodies ('EU DPR'),[3] forms a fundamental part of the EU's data protection framework. The LED, as a Europe-wide legal instrument specifically addressing data protection in national law enforcement activities marks a significant advancement in safeguarding individuals' personal data in the criminal justice context. The EDPB underlines the added value of the LED in providing a unified and coherent framework for data protection in the field of law enforcement, establishing a high standard for the protection of personal data.

2 The European Commission is required to present a report on the evaluation and review of the LED every four years and delivered its first report in 2022.[4] In this context, the EDPB contributed to the report by providing a consolidated contribution of the individual replies from the EU national data protection supervisory authorities ('SAs') to the questionnaire sent by the European Commission.

3 The European Commission intends to present its second report in May 2026.[5] To this end, on 2 July 2025, the Commission circulated a questionnaire to the SAs requesting their contributions to the second report on the LED evaluation for the reporting period from January 2022 to 31 August 2025.

4 The EDPB welcomes that the EU legislature provided for the European Commission's regular evaluations of the application of the LED. The EDPB is committed to providing its expertise and input during these evaluations to ensure that the LED continues to serve its purpose in promoting robust data protection standards in law enforcement.

5 Since the last evaluation of the LED, there has been an increase in case law related to the law enforcement context.[6] This is only the beginning of a gradual development towards a clarification of practical issues of interpretation relating to the LED by the courts, at both national and EU levels. The referral of more cases by national courts could contribute to clarification in this context. The EDPB recognises that lessons from national implementation can provide valuable insights into the effective application of the LED. On the basis of these

[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, pp. 89–131) The LED entered into force on 5 May 2016 and had to be transposed into national law by 6 May 2018, according to Article 63(1) LED.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, pp. 1–88).

[3] 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, pp. 39–98)

[4] 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'), 25.7.2022 COM(2022) 364, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0364

[5] Following the review, the Commission shall, if necessary, submit appropriate proposals for amendments, in particular considering of developments in information technology and in the light of the state of progress in technology and in the light of the state of progress in the information society.

[6] In particular, there have been a number of preliminary rulings by the CJEU. Of particular note are decisions relating to the processing of special categories of personal data, access to data in terminal equipment and the indirect right of access. Further decisions by the CJEU on the subject of data retention, which indirectly affects the area of the LED, have also been made since the last evaluation report. The following case law is just a few examples and is not exhaustive: Judgment of 26 January 2023, *Ministerstvo na vatreshnite raboti* (Recording of biometric and genetic data by the police), C-205/21, EU:C:2023:49; Judgment of 16 November 2023, *Ligue des droits humains (Vérification du traitement des données par l'autorité de contrôle)*, C-333/22, ECLI:EU:C:2023:874; Judgment of 4 October 2024, *Bezirkshauptmannschaft Landeck (Tentative d'accès aux données personnelles stockées sur un téléphone portable)*, Case C-548/21, ECLI:EU:C:2024:830; Judgment of 28 November 2024, *Ministerstvo na vatreshnite raboti () and génétiques II)*, C-80/23, ECLI:EU:C:2024:991.'

observations, the EDPB considers it essential to further strengthen the implementation of the LED.[7]

6 The EDPB takes note of the request from DPAs to get more clarification on the scope of application of the LED, in particular regarding the delineation between the LED and the GDPR (notably with regard to EU Large-Scale IT Systems [8]), as well as the interplay between the LED and other sector-specific legislation. The EDPB acknowledges the growing role of new technologies, such as artificial intelligence (AI) and big data analytics, in modern criminal investigations. While these technologies can enhance the effectiveness of law enforcement, they also introduce significant risks to individuals' privacy and other fundamental rights. The EDPB highlights the need for law enforcement authorities to use these tools in strict compliance with the LED, ensuring that their use is necessary, proportionate, and subject to adequate safeguards. The EDPB will continue to develop and issue guidelines on the LED to ensure that the processing of personal data in a law enforcement context, for instance where these technologies are deployed, is carried out in a way that respects data protection principles and the rights guaranteed by the Charter of Fundamental Rights.

7 The EDPB observes that the growing number of EU Large- Scale IT Systems and increasing cooperation between law enforcement authorities may create challenges for the exercise of data subjects' rights. Notably, the EDPB highlights that the cooperation between LED competent authorities may often involve the transfer of personal data, both across national and EU borders, as well as outside of the EEA. It is therefore important that LED competent authorities have expertise in international cooperation in criminal matters.

8 Furthermore, the role of Data Protection Officers ('DPOs') in the operational sector is of essence. While DPOs perform crucial advisory functions within law enforcement and judicial authorities, their effectiveness may be hindered where DPOs have limited access to operational information or insufficient dedicated training.

9 In addition, cooperation among law enforcement authorities, as well as their compliance with the relevant LED obligations towards SAs require appropriate technological tools and secure platforms to exchange information.

10 The supervision of data processing activities in the law enforcement sector requires expertise in both data protection and international cooperation. In addition, a good understanding of the legal, technical, and operational context in which law enforcement authorities operate is also essential. Against this background, the current financial and human resources in most SAs, are still insufficient. Therefore, it is of the utmost importance that all SAs are provided with sufficient resources by the Member States to carry out their tasks effectively.

11 The EDPB, meanwhile, is also entrusted with new tasks under new legal acts and its tasks under the GDPR and in the context of the Coordinated Supervision Committee[9] operating

[7] This represents current understanding and is without prejudice to any ongoing and upcoming amendments due to any legislative changes.
[8] This would in particular concern EU Large-Scale IT systems, where the purpose of processing is twofold (related, for instance to border and immigration control, as well as to law enforcement purposes). In this regard, further examination of the legal consequences for applying different legal frameworks to data processing carried out through the same information system, such as the GDPR and the LED respectively may be needed (CJEU, C-180/21, Judgment of 8 December 2022 Inspektor v Inspektorata kam Visshia sadeben savet (Finalités du traitement de données - Enquête pénale, ECLI:EU:C:2022:967).
[9] The Coordinated Supervision Committee (CSC) is a group of national supervisory authorities and the European Data Protection Supervisor (EDPS) to ensure coordinated supervision of EU Large-Scale IT Systems and of EU bodies, offices and agencies, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency. More information is available at: https://www.edpb.europa.eu/csc/about-csc/who-we-are-coordinated-supervision-committee_en

within its framework, continue at an increased intensity. In light of all the responsibilities entrusted to the EDPB, including on other legal frameworks than the LED, it is also essential to ensure that the EDPB Secretariat is provided with sufficient resources in order to support the EDPB members also in relation to the LED, and thus in harmonising the guidance, procedures, enforcement processes and practices of SAs across Member States.

2 EDPB's work according to the tasks listed under Article 51 LED

12 In terms of the EDPB's tasks as listed under Article 51 LED, for the reporting period from January 2022 to the end of August 2025, the EDPB has published two Opinions, one on the technical extension[10] and one on the renewal of the European Commission's adequacy decision for the United Kingdom ('UK')[11]. Furthermore, the Board has published guidelines on transfers subject to appropriate safeguards (on Article 37 LED)[12], as well as on the use of facial recognition in the field of law enforcement.[13]

13 The EDPB has also issued statements, contributions and guidance on EU instruments other than the LED governing the processing of data by competent authorities via specific frameworks and police and judicial cooperation, on matters such as the Second Additional Protocol of the Convention on Cybercrime14, access to data for law enforcement[15] and on the implications of the CJEU's judgement on Passenger Name Records ('PNR')[16].

14 One of the main tasks of the EDPB under the LED is to promote cooperation and the exchange of information and best practices among its members.[17] Under that framework, but as well under Article 62 of Regulation (EU) 2018/1725, the EDPB Secretariat also supports the Coordinated Supervision Committee ('CSC') which ensures coordinated supervision of large-scale IT systems and EU bodies and agencies. Since the last LED evaluation report, the activity of the CSC was considerably extended to the supervision of, for instance, the Visa Information System (VIS), Prüm II, Customs Information System (CIS-JHA), Entry Exist System (EES), which come in addition to the Schengen Information System (SIS), Europol, the EPPO, Eurojust and IMI that were already falling under the framework of the CSC activities. As part of its work on the reporting period, the CSC issued, inter alia, guides for exercising data subjects' rights[18].

[10] EDPB Opinion 06/2025 regarding the extension of the European Commission Implementing Decisions under the GDPR and the LED on the adequate protection of personal data in the United Kingdom, adopted on 5 May 2025, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-062025-regarding-extension-european-commission_en

[11] EDPB Opinion 27/2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom, adopted on 16 October 2025, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en .

[12] Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted on 19 June 2024, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012023-article-37-law-enforcement-directive_en .

[13] EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted on 26 April 2023, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

[14] EDPB letter in response to a request for an opinion from the LIBE Committee on the 2nd Additional Protocol to the Budapest Convention, available here: https://www.edpb.europa.eu/system/files/2022-02/edpb_letter_on_2nd_additionalprotocolcybercrimeconvention_out2022-0008.pdf

[15] EDPB statement on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, adopted on 4 November 2024, available here: https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf

[16] EDPB statement on the implications of the CJEU judgement C-817/19 regarding the implementation of Directive (EU) 2016/681 on the use of PNR in Member States, adopted on 13 December 2022, available here: https://www.edpb.europa.eu/system/files/2022-12/edpb_statement_20221213_on_the_pnr_judgement_en.pdf; EDPB statement on the Implementation of the PNR Directive in light of CJEU Judgement C-817/19, adopted on 13 March 2025, available here: https://www.edpb.europa.eu/system/files/2025-03/edpb_statement_20250313_implementation-of-the-pnr-directive-in-light-of-the-cjeu-judgment_en.pdf

[17] Article 51(1)(h) LED.

[18] The Schengen Information System - a guide for exercising data subjects' rights: the right of access rectification and erasure, April 2023, available at https://www.edpb.europa.eu/system/files/2023-04/csc_guide_right_of_access_rectification_and_erasure_20230403_en.pdf; as well as Europol's information systems - a guide for exercising data subjects' rights: the right of access rectification and erasure, July 2023, available at https://www.edpb.europa.eu/system/files/2023-9/20230725_europol_guide_for_exercising_the_rights_draft_version_sec_fv.pdf.

3 EDPB's synthesis of replies to the questionnaire

15 As indicated above, as part of its review and evaluation of the Law Enforcement Directive ('LED') under Article 62 LED, the European Commission circulated a questionnaire to the EDPB and SAs. The purpose of this questionnaire was to gather the views of the SAs on the application and functioning of the LED for the reporting period from January 2022 to 31 August 2025. In particular, the European Commission sought feedback on how the SAs handled complaints from data subjects, carried out their consultation and advisory roles, promoted awareness and training, and managed international data transfers. The questionnaire also examined the issues of cooperation among SAs, both bilaterally and within the EDPB framework and assessed the resources available to them for supervising the competent authorities in terms of their obligations under data protection law in the area of law enforcement, given that the effective fulfilment of their mandate largely depends on these resources. Additionally, the SAs were invited to share their views on how the LED has been implemented in their respective EU Member States and what challenges they have faced.

16 In addition to the general policy messages and based on the responses received from the SAs, the EDPB provided a synthesis of its members' contributions to each question included in the European Commission's LED evaluation questionnaire. This synthesis draws on information provided by the EDPB members responsible for LED-related matters, which include the national SAs of the 27 EU Member States[19] and considers the consolidated replies provided at national level[20].

[19] The European Commission decided to only address the questionnaire to the 27 EU Member States. The questionnaire was not addressed to the European Data Protection Supervisor (EDPS), since the LED does not apply to the processing of personal data by the EU institutions, bodies, offices and agencies that the EDPS supervises, in accordance with Article 2(3)(b) LED.
[20] However, due to a federal structure and/or internal division of labour, the SAs competent for LED-related matters in some EU Member States, such as Germany and Belgium, have had diverse experiences in applying different national legislations while implementing the LED.

Questionnaire on the application of the LED under Article 62 LED

Contribution of the European Data Protection Board[21]

17 In addition to the general policy messages above, the EDPB would like to provide a synthesis of the contributions and replies provided by 27 EU Members States to the questionnaire sent by the European Commission. Please note that whenever an SA has not provided data for a specific question, that SA is not depicted in the corresponding graph.

1 Scope

1.1 Have you ever raised a query/issued a decision relating to a competent authority's determination that a processing activity falls outside the scope of Union law (such as on the basis of national security) in accordance with Article 2(3)(a) LED?

18 23 SAs have not raised a query or issued a decision relating to a competent authority's determination that a processing activity falls outside the scope of Union law in accordance with Article 2(3)(a) LED. However, one SA reported having issued such a query relating to a competent authority's determination that a processing activity falls outside the scope of EU law, during the modification of a database, in which the SA issued an opinion clarifying the compliance of personal data processing partly implemented within an activity falling outside the scope of EU law and thus governed by multiple legal frameworks.

2 Exercise of data subjects' rights through the DPA

2.1 Has Article 17 LED been implemented into your national law?

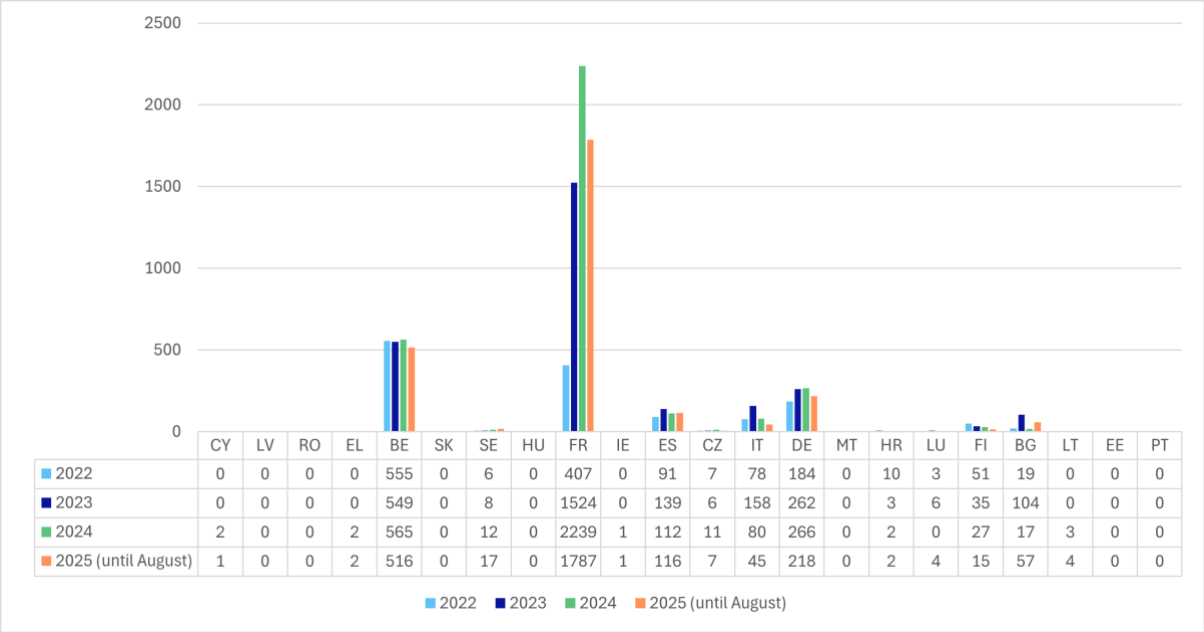
19 23 SAs reported that their Member States have implemented Article 17 LED into their national laws, while 4 SAs reported that it was not the case in their country.

2.1.a Please indicate per year how many requests under Article 17 LED have you received from January 2022 to 31 August 2025? (Please also include complaints lodged under Article 52 LED which your DPA decided to subsequently handle as an Article 17 LED request).

20 The graph below shows the number of requests received by the SAs under Article 17 LED, including complaints lodged under Article 52 LED that the SA subsequently decided to handle

[21] With regard to Section 3 of the EDPB Contribution, it reflects the input provided by the national SAs. Section 3 reflects the replies provided by the national SAs to the questionnaire sent by the European Commission. Some SAs could not gather certain statistics requested in the questionnaire. Thus, when specific data was not provided by the SA or is not available, those SAs are not reflected in the tables. With respect to Germany, the data provided by the different German SAs has been compiled and presented as a single set of information as "DE SA"; it does not always contain the figures from all German SA as some SAs could not gather certain statistics requested in the questionnaire With respect to the Greek SA, it is referred to as "EL" or "GR" indistinctively throughout the document. With respect to the LU SA, the data submitted from the CNDP and the ACJ have been added.

as Article 17 LED requests, on an annual basis during the reporting period from January 2022 to 31 August 2025.



	CY	LV	RO	EL	BE	SK	SE	HU	FR	IE	ES	CZ	IT	DE	MT	HR	LU	FI	BG	LT	EE	PT
2022	0	0	0	0	555	0	6	0	407	0	91	7	78	184	0	10	3	51	19	0	0	0
2023	0	0	0	0	549	0	8	0	1524	0	139	6	158	262	0	3	6	35	104	0	0	0
2024	2	0	0	2	565	0	12	0	2239	1	112	11	80	266	0	2	0	27	17	3	0	0
2025 (until August)	1	0	0	2	516	0	17	0	1787	1	116	7	45	218	0	2	4	15	57	4	0	0

2.2 Is there an increase / decrease since the last review?

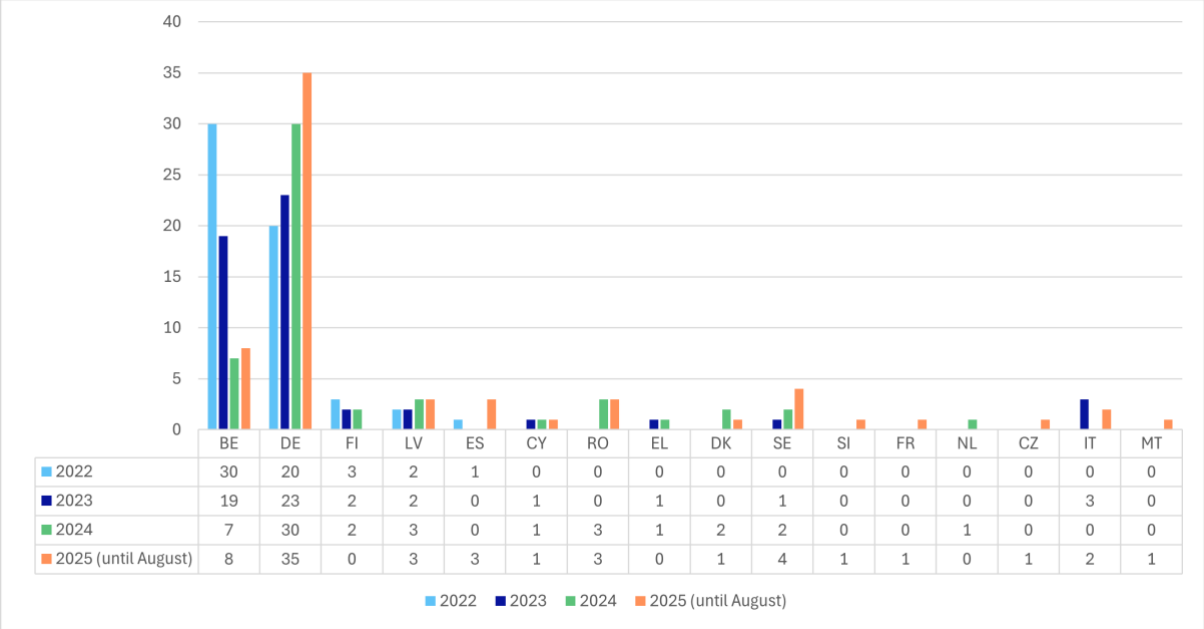
21 9 SAs reported an increase in requests under Article 17 LED since the last review, while 9 SAs noted a decrease (6 SAs did not provide numbers).

3 Consultations and advisory powers

3.1 Have competent authorities utilised the prior consultation procedure in accordance with Article 28 (1)(a) or (b) LED from January 2022 to 31 August 2025? In this context, did you provide written advice and/or use your corrective powers pursuant to Article 28(5) LED?

22 16 SAs used the prior consultation procedure in accordance with Article 28(1)(a) or (b) LED during the reporting period, while 11 SAs did not.

23 The graph below depicts the number of such procedures, per year during the reporting period from January 2022 to 31 August 2025.



	BE	DE	FI	LV	ES	CY	RO	EL	DK	SE	SI	FR	NL	CZ	IT	MT
2022	30	20	3	2	1	0	0	0	0	0	0	0	0	0	0	0
2023	19	23	2	2	0	1	0	1	0	1	0	0	0	0	3	0
2024	7	30	2	3	0	1	3	1	2	2	0	0	1	0	0	0
2025 (until August)	8	35	0	3	3	1	3	0	1	4	1	1	0	1	2	1

3.2 From January 2022 to 31 August 2025, have you established a list of processing operations that are subject to prior consultation pursuant to Article 28(3) LED or have you updated your previous list?

24 19 SAs have not established a list of processing operations subject to prior consultation, pursuant to Article 28(3) LED, while 8 SAs have established such a list.

3.3 With respect to the requirements set down in Article 28(2) LED, has your DPA been consulted systematically, from January 2022 to 31 August 2025?

25 16 SAs have been systematically consulted regarding the requirements provided in Article 28(2) LED, while 11 SAs reported they had not been consulted in this regard.

3.4 a Please indicate the types of issues/topics on which you have been approached for advice thereby distinguishing between Article 28(1) LED and Article 28(2) LED (e.g. deployment of facial recognition cameras during identity checks based on existing laws, draft of legislative/regulatory measure for the deployment of facial recognition for a purpose under the LED, access to data in criminal investigations etc.)?

26 Regarding the consultation of the SAs prior to processing, which will form part of a new filing system to be created under Article 28 LED, most (9 SAs) reported that they had been consulted on issues concerning the use of new technologies, such as artificial intelligence, as well as biometrics and facial recognition cameras for law enforcement purposes. Many (6 SAs) reported having been consulted on the deployment of police fixed cameras, police body cameras and the use of electronic surveillance, such as data processing related to public surveillance cameras. A few (3 SAs) have been consulted on the use of Automatic Number Plate Recognition (ANPR) cameras in the law enforcement context. Some SAs (2 SAs) reported having been consulted on issues relating to the restriction of data subjects' rights and

on matters concerning different databases. One SA replied that it had not been approached for advice based on Article 28(1) LED.

27 Regarding consultations of the SAs during the preparation of legislative measures, according to Article 28(2)(b) LED, most (8 SAs) reported having been consulted on issues relating to the use of new technologies, such as artificial intelligence, biometrics, the installation and operation of cameras (i.e. Automatic Number Plate Recognition ('ANPR'), security cameras for traffic violation vehicles, police body cameras, video surveillance systems), recording devices for law enforcement purposes, drones, and CCTV). Additionally, many SAs (10 SAs) have been consulted on sector-specific legislation, such as combating crime in athletic stadiums, the collection, storage and use of suspects' and convicted persons' photographs, fingerprints and DNA, criminal procedure for minors, data retention, and issues relating to access to data for the purposes of criminal investigations in relation to national and other large-scale databases (e.g. automated fingerprints database, ECRIS-TCN, etc.). Some (4 SAs) reported having provided advice on issues related to the collection, storage and further processing of data.

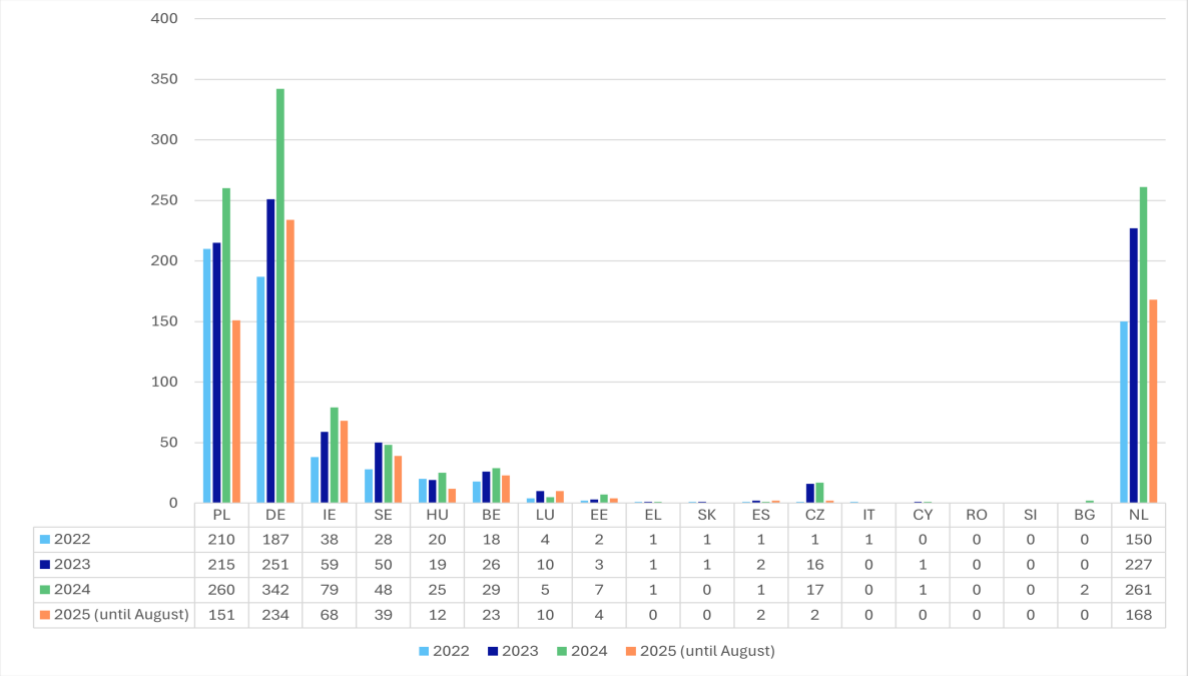
4 Data breach notifications

4.1 Does your DPA make a distinction between what constitutes a breach under the LED and a breach under the GDPR?

28 18 SAs distinguish between what constitutes a breach under the LED and a breach under the GDPR, while 9 SAs replied negatively.

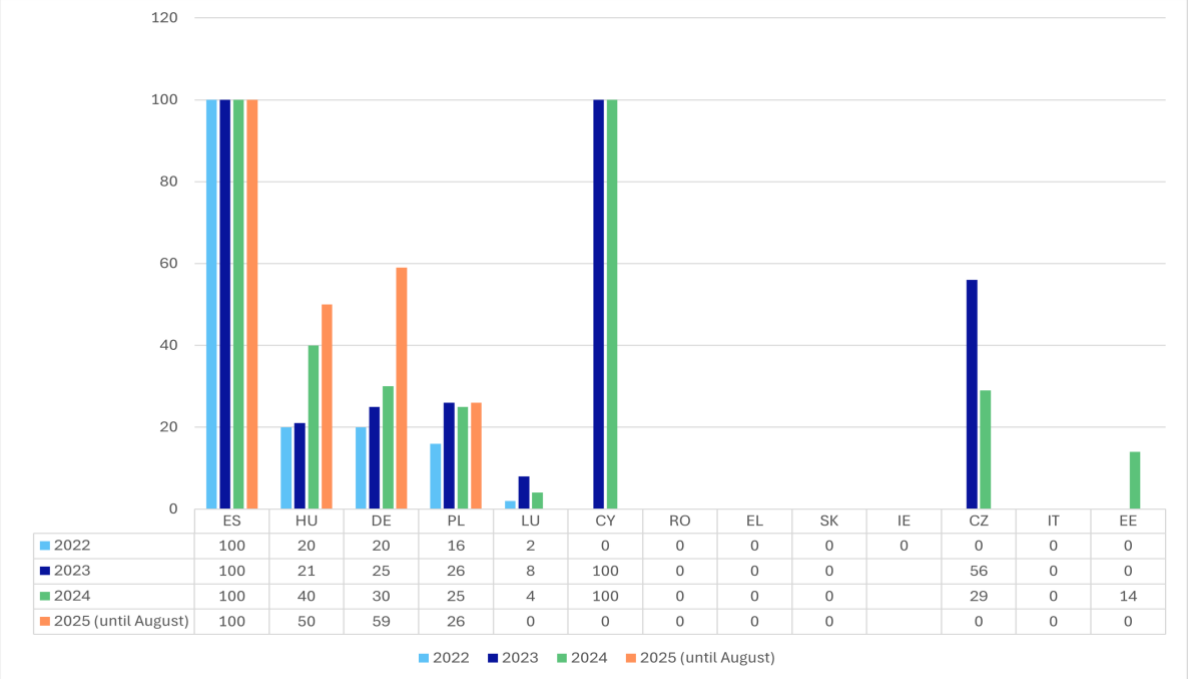
4.1.a From January 2022 to 31 August 2025, indicate per year how many data breach notifications under the LED have you received and in what percentage you advised or ordered competent authorities to take any necessary measures to either mitigate the risk posed or bring the processing into compliance with the LED?

29 The graph below depicts the number of data breach notifications received under the LED by the SAs, on an annual basis for the reporting period from January 2022 to 31 August 2025.



	PL	DE	IE	SE	HU	BE	LU	EE	EL	SK	ES	CZ	IT	CY	RO	SI	BG	NL
2022	210	187	38	28	20	18	4	2	1	1	1	1	1	0	0	0	0	150
2023	215	251	59	50	19	26	10	3	1	1	2	16	0	1	0	0	0	227
2024	260	342	79	48	25	29	5	7	1	0	1	17	0	1	0	0	2	261
2025 (until August)	151	234	68	39	12	23	10	4	0	0	2	2	0	0	0	0	0	168

30 The graph below depicts the percentage in which the SAs advised or ordered competent authorities to take necessary measures to mitigate the risk posed or to bring the processing into compliance with the LED.



	ES	HU	DE	PL	LU	CY	RO	EL	SK	IE	CZ	IT	EE
2022	100	20	20	16	2	0	0	0	0	0	0	0	0
2023	100	21	25	26	8	100	0	0	0		56	0	0
2024	100	40	30	25	4	100	0	0	0		29	0	14
2025 (until August)	100	50	59	26	0	0	0	0	0		0	0	0

5 International transfers

5.1 Have you encountered cases where a controller transferred personal data pursuant to Article 37(1)(a) LED?

31 21 SAs did not encounter cases where a controller transferred personal data pursuant to Article 37(1)(a) LED. 6 SAs reported such cases. Concerning the latter, the data transfer was based on bilateral agreements.

5.2 Have you encountered cases where a controller transferred personal data based on a 'self-assessment' pursuant to Article 37(1)(b) LED?

32 22 SAs did not encounter cases where a controller transferred personal data based on a 'self-assessment' under Article 37(1)(b) LED, while 5 SAs did.

5.2.a What kind of "categories of transfers" did the controller communicate (Article 37(2) LED)? Have there been cases where you requested documentation pursuant to Article 37(3) LED? In such cases, were you satisfied with the assessment carried out by the controller and, if not, what enforcement measures were taken? Did you encounter cases where Article 37(1)(b) LED transfers were used inappropriately?

33 One SA reported that data controllers are obliged under their national law to provide information about transfers under Article 37(1)(b) LED to the SA and that this obligation has been fulfilled by the controller. In one case, a different SA reported that it was satisfied with the assessment carried out by the controller; that the transfers were necessary for system support in the context of police assistance for specific criminal cases and it had not requested documentation pursuant to Article 37(3) LED. Another SA reported that transfers among competent authorities for civil or criminal purposes are central to the activities of the judiciary and it did not specifically control the transfers that took place and that however, court members and staff are trained on issues related to data transfers by internal DPOs and can consult them with any questions regarding data transfers between competent authorities within the EU, third countries or international organisations.

5.3 Have you carried out any investigations into data transfers based on derogations, in particular those set out in Article 38(1)(c) LED and Article 38(1)(d) LED?

34 26 SAs did not conduct any investigations into data transfers based on derogations, particularly those set out in Article 38(1)(c) and Article 38(1)(d) LED. In the one case where such an investigation was conducted, no violations were detected, but deficiencies in the documentation were identified.

5.4 Have you carried out activities to promote the awareness of controllers/processors (specifically) with respect to their obligations under Chapter V of the LED?

35 13 SAs have undertaken activities to raise awareness among controllers and processors about their obligations under Chapter V of the LED. Most of these activities, particularly those

concerning the obligations under Chapter V of the LED, involve publishing relevant information on the SAs' websites, responding to individual requests and consultations, and holding meetings with the relevant authorities. Many of these SAs have provided training sessions and seminars, while others have issued press releases, guidelines and opinions. Some have offered consultations on a case-by-case basis. Of the SAs that did not carry out such activities (namely 14 SAs), two reported that this was due to the absence of complaints received in this regard, while internal training was provided to the DPOs. Another SA cited other priorities, while a few (4 SAs) stated that a lack of resources was the reason. A few (2 SAs) reported that their awareness-raising activities have so far focused on broader data protection obligations under the LED and national implementing legislation, or on Chapter V of the GDPR, targeting a wider audience.

5.5 Have you advised law enforcement competent authorities about their obligations with respect to data transfers under Chapter V (Articles 35-40) of the LED, for instance as regards the appropriate safeguards required under Article 37(1)(a), (b) LED? Have you issued any guidelines, recommendations and/or best practices in this regard?

36 15 SAs have not advised law enforcement competent authorities of their obligations regarding data transfers under Chapter V (Articles 35-40) LED. 12 SAs reported positively, with one stating it has advised them in relation to international agreements but has not issued any guidelines, recommendations, or best practices on this matter.

5.6 Have you received/handled complaints (by data subjects and/or bodies, organisations or associations in accordance with Article 55 LED) specifically addressing the issue of data transfers?

37 25 SAs have not received or handled complaints from data subjects or bodies, organisations, or associations in accordance with Article 55 LED, specifically regarding data transfers, while 2 SAs replied positively.

5.7 Have you exercised your investigative and/or enforcement powers with respect to data transfers? In particular, have you ever imposed (temporary or definitive) limitations, including a ban, on data transfers?

38 23 SAs have not exercised their investigative or enforcement powers regarding data transfers, while 4 SAs have done so.

5.8 Have there been cases in which you have cooperated with foreign data protection authorities (for instance, exchange of information, complaint referral, mutual assistance)? Are there existing mechanisms on which you can rely for such cooperation?

39 16 SAs did not encounter cases requiring cooperation with foreign data protection authorities, although 11 SAs reported that, despite the absence of official mechanisms or channels, they cooperated with other SAs on a case-by-case basis by exchanging information and complaint referrals. Conversely, one SA reported that such a mechanism exists and that it had examined the validity of alerts issued. Another SA stated that mutual assistance was used in three cases,

although these did not concern data transfers. One SA stated that it frequently exchanges information with other SAs, mainly within the context of the EDPB or the IMI system.

6 Awareness-raising, training and guidance

6.1 From January 2022 to 31 August 2025, have you issued guidance and/or practical tools supporting competent authorities or processors to comply with their obligations?

40 While 9 SAs had not issued guidance during the reporting period, the majority provided guidance and practical tools to support competent authorities or processors in meeting their obligations (18 SAs). This guidance was addressed to both controllers and national legislators, mainly concerning the transposition of the LED into national legislation, as well as issues regarding video surveillance and the handling of data subjects' rights. Some (3 SAs) reported issuing guidelines on data security and the prevention of data breaches and security incidents. Furthermore, some SAs (3 SAs) provided guidance on personal data processing in the context of EU Large-Scale IT Systems, such as the Schengen Information System (SIS) or Eurodac and the relevant data subjects' rights, as well as on the design and implementation of data protection impact assessments. One SA reported providing guidance on the designation of the DPO under the LED.

41 Regarding methodology, most SAs stated that they have published materials (such as activity reports, guidance, newsletters, brochures, FAQs, and handbooks) either publicly (by uploading information on their websites) or bilaterally to competent authorities. A few SAs reported that such guidance is given on a case-by-case basis. Some SAs reported that ad hoc guidance is also provided in the context of prior consultations or in response to requests for prior opinions. One SA reported that advice is regularly provided during inspections, complaint handling and in response to reports. A few SAs reported that guidance is offered through regular training or conferences, while one SA stated that relevant guidance and tools from the EDPB were promoted via publication on their webpage. In two cases, SAs also reported setting up helpdesks and dedicated mailboxes to provide advice on fulfilling the obligations of controllers and processors under the LED or on other specific issues. One SA also reported using tools such as "before leaving the unit" checklists, data protection knowledge tests and templates for data processing agreements.

7 Competence

7.1 Have you faced any difficulties stemming from your national law or practical difficulties in supervising processing operations pursuant to Article 45 LED? Have you faced difficulties as regards the supervision of processing operations by courts when they do not act in their judicial capacity?

42 While 18 SAs did not face any difficulties stemming from their national laws or practical difficulties in supervising processing operations pursuant to Article 45 LED, 8 SAs reported issues regarding the interpretation of the concept of "acting in a judicial capacity", which further led to issues regarding the SAs' competence. Regarding the SAs' competence, one SA also referred to significant deficiencies in the national transposing law in terms of the LED's scope of application, the SA's competence and supervisory functions. In addition, another SA

reported that difficulties arise from the adaptation of Article 45 LED into its national legislation (i.e., processing operations of classified personal data carried out for national security activities are exempt from its competence). Another SA reported that its national transposing law does not regulate supervision of the processing of personal data by courts and prosecutors and that it does not apply to case-file documentation or registers maintained under procedural codes or specific laws. Other SAs reported difficulties only regarding public prosecutors, although these are not considered independent judicial authorities under the jurisdiction concerned. Furthermore, some authorities would deny the SA's competence to conduct proactive controls without a prior complaint on the basis that public prosecutors would be acting in their judicial capacity. In one case, an SA reported that it is not competent to carry out supervision under the law governing data protection in the field of criminal offences and for misdemeanour supervision regarding the processing of personal data in a criminal case of a court, when carried out within the framework of independent judicial decision-making or decision-making by professional associates or judicial assistants pursuant to a judge's order. That SA also reported it is not competent to supervise the processing of personal data carried out within the framework of independent judicial decision-making of the Constitutional Court in the aforementioned cases.

7.2 For which independent judicial authorities, other than courts, are you not competent pursuant to Article 45 (2) LED, to supervise their processing operations?

43 Most (12 SAs) reported that there are no independent judicial authorities, other than courts, for which they are not competent to supervise processing operations pursuant to Article 45(2) LED. Several (5 SAs) reported that they are not competent to supervise public prosecutor authorities, while others (2 SAs) reported such lack of competence regarding national security entities (i.e. internal security service and foreign intelligence services). One SA stated that this lack of competence applies to any additional authority that operates independently and has specific legal responsibilities outside the jurisdiction of the Belgian DPA in charge of police matters (the 'COC', the Supervisory Body for Police Information). Another SA reported that it is competent to supervise all other authorities processing data under the national transposing law. In one case, where the SA reported that personal data processed by the public prosecutor's office and courts are excluded from the scope of the national transposing law, the SA considered that, the Public Prosecutor's Office is neither an independent body, nor a judicial authority within the meaning of Article 45(2) LED and, therefore, should not benefit from the exemptions provided for in that provision, as the exclusion established by the law is not limited to activities performed in the exercise of judicial capacity but extends to the entire activity of these bodies.

8 Powers

8.1 With respect to your investigative powers, do you consider them effective?

44 While 23 SAs reported that they consider their investigative powers effective, 4 SAs replied negatively. In particular, one SA reported that, although its investigative powers are considered effective, it has encountered difficulties regarding the possibility to obtain access to information, as some authorities have refused to submit the requested information in certain cases, while others have insisted on allowing only on-site inspection of the necessary

information. As the provision of such information is not enforceable without court intervention, it is therefore not fully effective. Furthermore, the same SA indicated that its investigative powers are restricted as it does not have supervision power on data processing that has been subject to prior review or authorisation by a court (e. g. intrusive measures like phone tapping). The same SA also reported doubts as to whether personal data and information from ongoing investigations by competent authorities are covered by its investigative powers.

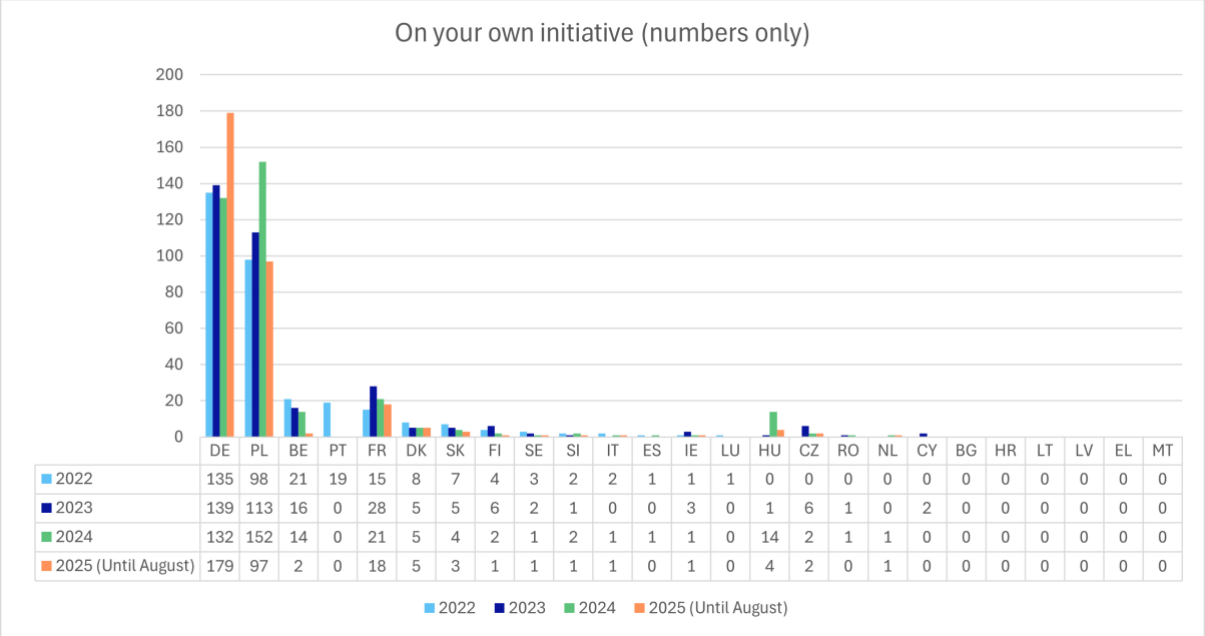
45 Another SA reported that it is not competent for processing operations of classified personal data carried out for national security activities. Another SA reported that it is not competent to carry out supervision under the law governing data protection in the field of criminal offences, nor for misdemeanour supervision regarding the processing of personal data in a criminal case of a court, when carried out within the framework of independent judicial decision-making or by professional associates or judicial assistants pursuant to a judge's order, as defined by the law governing courts, or under the provisions of other laws determining their independent functioning. It is also not competent to supervise the processing of personal data carried out within the framework of independent judicial decision-making of the Constitutional Court in such cases.

8.2 Has your answer substantially changed since the last review (from 2018-2021)?

46 24 SAs reported that their situation had not substantially changed since the last review. However, 3 SAs replied that their situation had changed, as follows: one SA reported that since the last review, it has progressively achieved more extensive direct access to all necessary tools and databases available to operational law enforcement authorities. Another SA reported that conducting complaint proceedings under the national provisions is not conducive to the amicable settlement of cases; on the contrary, the adversarial nature of such proceedings, where parties with opposing interests engage in a formal dispute, made it difficult to establish the facts and to ensure swift compliance with the LED provisions and called for the introduction of mechanisms that would allow it to operate in a non-administrative, more conciliatory and pragmatic manner.

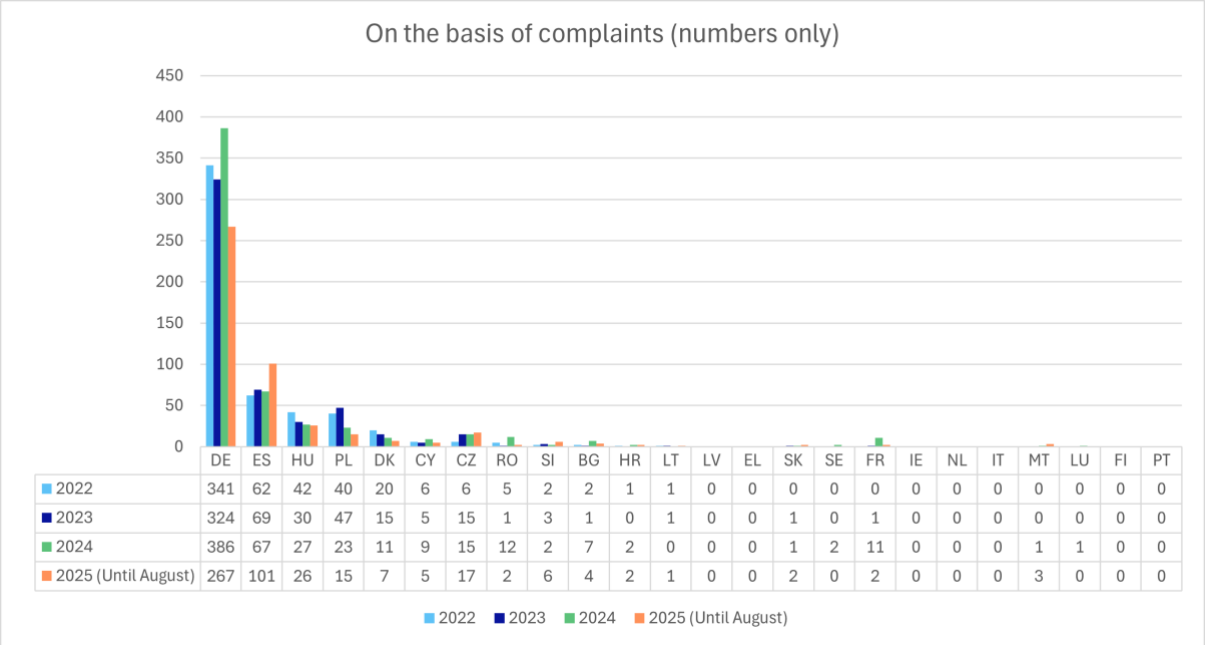
8.3 Please indicate, per year (January 2022 to 31 August 2025), how many investigations and/or inspections you have conducted.

47 The first graph below depicts the number of investigations and/or inspections conducted by the SAs, at their own initiative, each year, during the reporting period.



	DE	PL	BE	PT	FR	DK	SK	FI	SE	SI	IT	ES	IE	LU	HU	CZ	RO	NL	CY	BG	HR	LT	LV	EL	MT
2022	135	98	21	19	15	8	7	4	3	2	2	1	1	1	0	0	0	0	0	0	0	0	0	0	0
2023	139	113	16	0	28	5	5	6	2	1	0	0	3	0	1	6	1	0	2	0	0	0	0	0	0
2024	132	152	14	0	21	5	4	2	1	2	1	1	1	0	14	2	1	1	0	0	0	0	0	0	0
2025 (Until August)	179	97	2	0	18	5	3	1	1	1	1	0	1	0	4	2	0	1	0	0	0	0	0	0	0

48 The graph below depicts the number of investigations and/or inspections conducted by the SAs, on the basis of complaints, each year, during the reporting period.



	DE	ES	HU	PL	DK	CY	CZ	RO	SI	BG	HR	LT	LV	EL	SK	SE	FR	IE	NL	IT	MT	LU	FI	PT
2022	341	62	42	40	20	6	6	5	2	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0
2023	324	69	30	47	15	5	15	1	3	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0
2024	386	67	27	23	11	9	15	12	2	7	2	0	0	0	1	2	11	0	0	0	1	1	0	0
2025 (Until August)	267	101	26	15	7	5	17	2	6	4	2	1	0	0	2	0	2	0	0	0	3	0	0	0

8.4 Did you face any difficulties in exercising your investigative powers?

49 21 SAs reported not having encountered difficulties in exercising their investigative powers, while 6 SAs replied affirmatively. Among the latter, one SA reported that some parties continue to deny their obligation to provide all documents required by the SA to perform its tasks, while other competent authorities have questioned the necessity of providing certain information and some have refused to submit the requested information in specific cases. Additionally, some competent authorities have insisted on permitting only on-site inspection of the

necessary information. That SA also stated that in individual cases, it was no longer possible to use log data to investigate and clarify a past data protection violation due to deletion routines. Furthermore, some administrative offences (e.g. unauthorised data queries by police officers) become time-barred because of the lengthy duration of previous preliminary investigations by the public prosecutor's office.

50 Another two SAs reported that sometimes there is a lack of or delays in cooperation with competent authorities, while the SA's limited capacity also creates difficulties. A different SA reported that the legal framework does not provide a clear methodology or specify any technical or organisational solutions for how controllers should implement the separation of data relating to different categories of data subjects (e.g. suspects, convicted persons, victims, witnesses, third parties) and distinguish facts from personal assessments (e.g. operational information or analytical assumptions), as required by Articles 6 and 7 LED.. In addition, many competent authorities use national information systems in which data on different categories of data subjects are stored in a single file without such structural separation, which may affect data quality and compliance with the principles of proportionality and purpose limitation. In certain cases, competent authorities cannot determine the status of such data, as it depends on other data that may be obtained later in the criminal proceedings.

51 A different SA highlighted that its investigative powers are based on general national legislation which is not specifically tailored to the LED. As no dedicated investigative tools exist for supervisory authorities, the SA must apply these general provisions. In one case, another SA reported difficulties in the context of announced on-site inspections, where the data controller can change its data processing practices, while a significant number of competent authorities are located in places that are difficult to access without prior notification.

8.5 Have there been any changes since the last review with respect to your corrective powers listed under Article 47(2)(a), (b – including rectification, erasure, restriction) and (c) LED?

52 While 23 SAs reported no changes since the last review regarding their corrective powers listed under Article 47(2)(a), (b – including rectification, erasure, restriction) and (c) LED, 3 SAs reported the following changes. In particular, one SA stated that its corrective powers regarding the Federal Criminal Police and the Financial Intelligence Unit had been revised (i.e., if the SA objects to violations under the law, it may order appropriate measures if necessary to remedy a significant violation of data protection regulations. However, the limitation to significant violations of data protection regulations, as well as the obligation to object before ordering appropriate measures are not in compliance with Article 47(2) LED, as the latter has not yet been transposed with regard to the Federal Police; and that there have also been several changes at regional level). Another SA reported that since the last review, it has applied corrective powers in two cases under Article 47(2)(b) LED and Article 47 (2)(c) LED. Another SA stated that an amendment to the law had reinstated the competence of the data protection supervisory authorities for sanctioning the infringements set out in Articles 58(j) and 59(j) of its national transposing law of the LED.

8.6 Do you consider your corrective powers effective?

53 The vast majority (24 SAs) consider their corrective powers effective while 3 SAs responded negatively. In particular, two SAs reported different corrective powers at federal and state

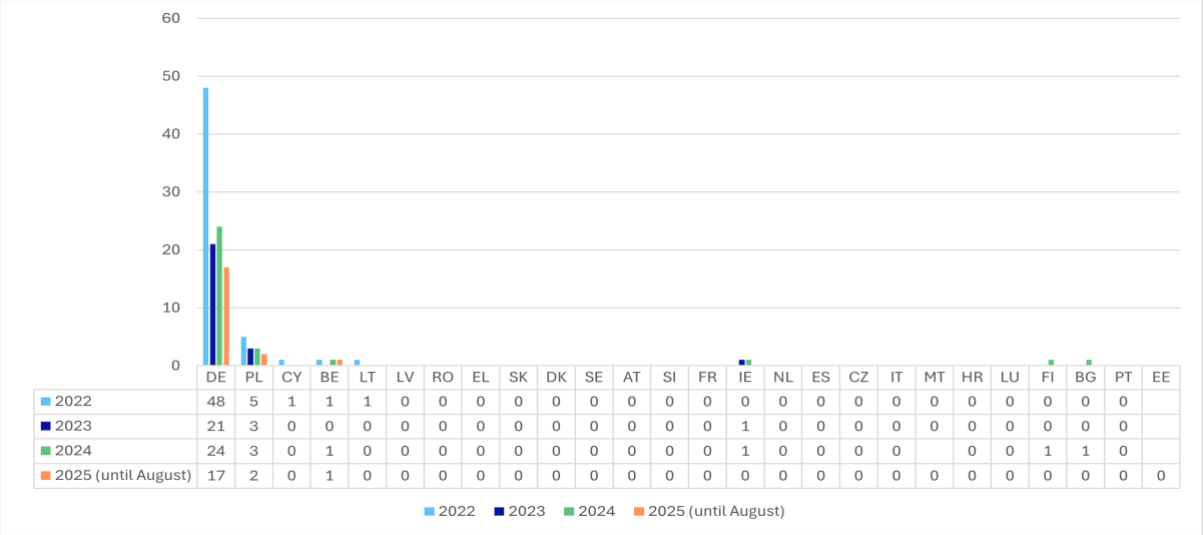
levels and that not all the powers listed in Article 47(2) LED have been implemented in national legislation, especially regarding the powers under Articles 47(2)(b) and Article 47(2)(c) LED (i.e., some SAs have additional powers and in cases where the corrective powers of Article 47(2) LED were not fully implemented, they are not considered fully effective). In one country, despite a direct reference in national law, some SAs competent for courts consider that their powers do not extend to exercising corrective powers under the LED. Another SA reported substantial discrepancies in terms of administrative fines under the GDPR and the LED and that the SA's corrective powers remain insufficient, with the maximum fine levels substantially lower for violations by the police compared to other public authorities subject to the GDPR.

8.7 With respect to the effectiveness of your corrective powers, has your answer substantially changed since the last review?

54 Almost all SAs (24) reported that their answer has not changed substantially since the last review as regards the effectiveness of their corrective powers while 3 SAs replied positively.

8.8 From January 2022 to 31 August 2025, please indicate, per year, which corrective powers you have applied and in how many cases. Please list the powers used according to Article 47(2)(a) LED (warnings). Amongst those cases, how many were related to the supervision of SIS[22] and VIS[23]?

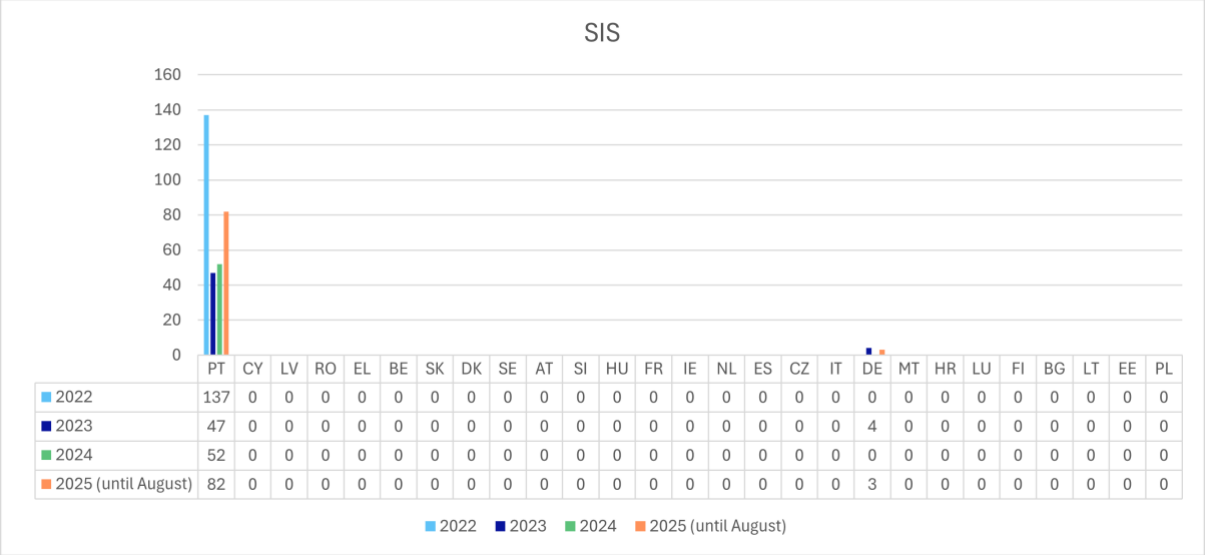
55 The graph below depicts the number of cases where the SAs have applied their corrective powers, according to Article 47(2)(a) LED (warnings), per year during the reporting period.



	DE	PL	CY	BE	LT	LV	RO	EL	SK	DK	SE	AT	SI	FR	IE	NL	ES	CZ	IT	MT	HR	LU	FI	BG	PT	EE
2022	48	5	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2023	21	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	
2024	24	3	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		0	0	1	1	0	
2025 (until August)	17	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

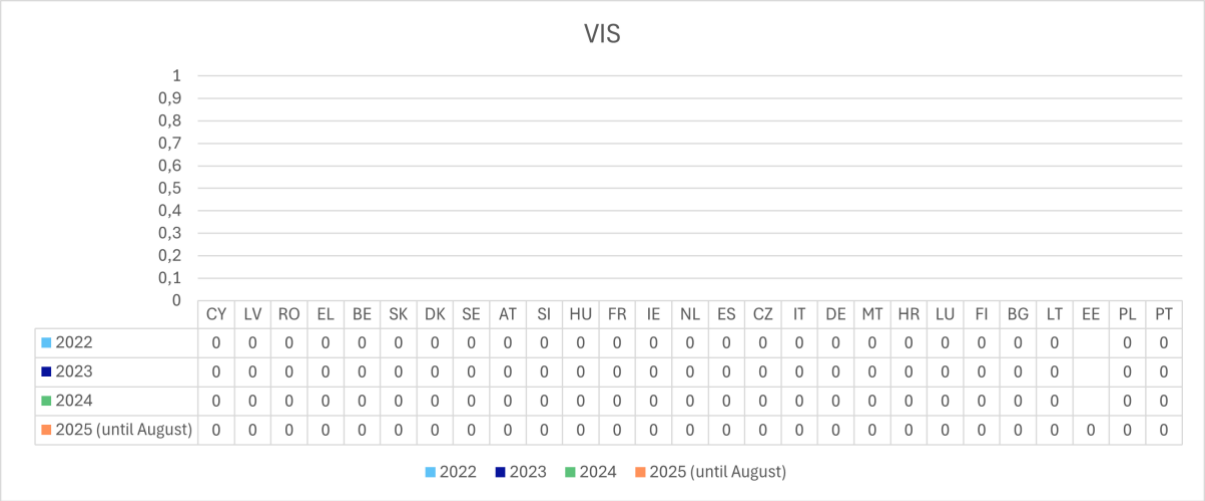
56 The graph below depicts the number of cases where the SAs have applied their corrective powers Article 47(2)(a) LED (warnings), related to the supervision of SIS, per year during the reporting period.

[22] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).
[23] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).



	PT	CY	LV	RO	EL	BE	SK	DK	SE	AT	SI	HU	FR	IE	NL	ES	CZ	IT	DE	MT	HR	LU	FI	BG	LT	EE	PL
2022	137	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0
2024	52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0

57 This graph depicts the number of cases where the SAs have applied their corrective powers Article 47(2)(a) LED (warnings), related to the supervision of VIS, per year during the reporting period.

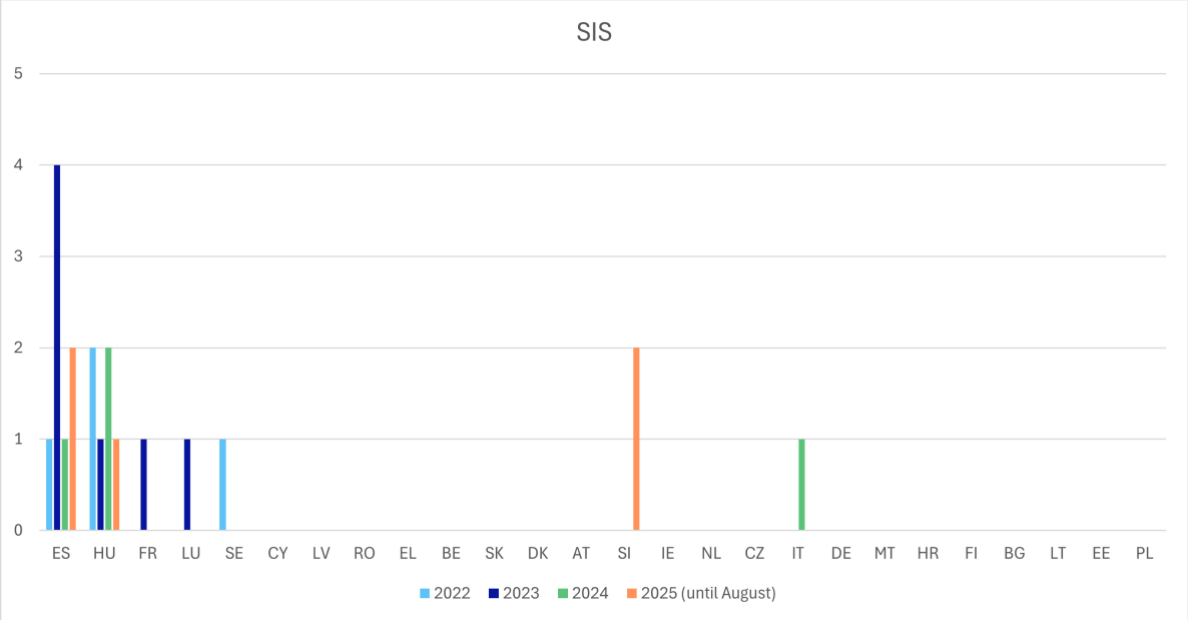


	CY	LV	RO	EL	BE	SK	DK	SE	AT	SI	HU	FR	IE	NL	ES	CZ	IT	DE	MT	HR	LU	FI	BG	LT	EE	PL	PT
2022	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0
2023	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0
2024	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0
2025 (until August)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

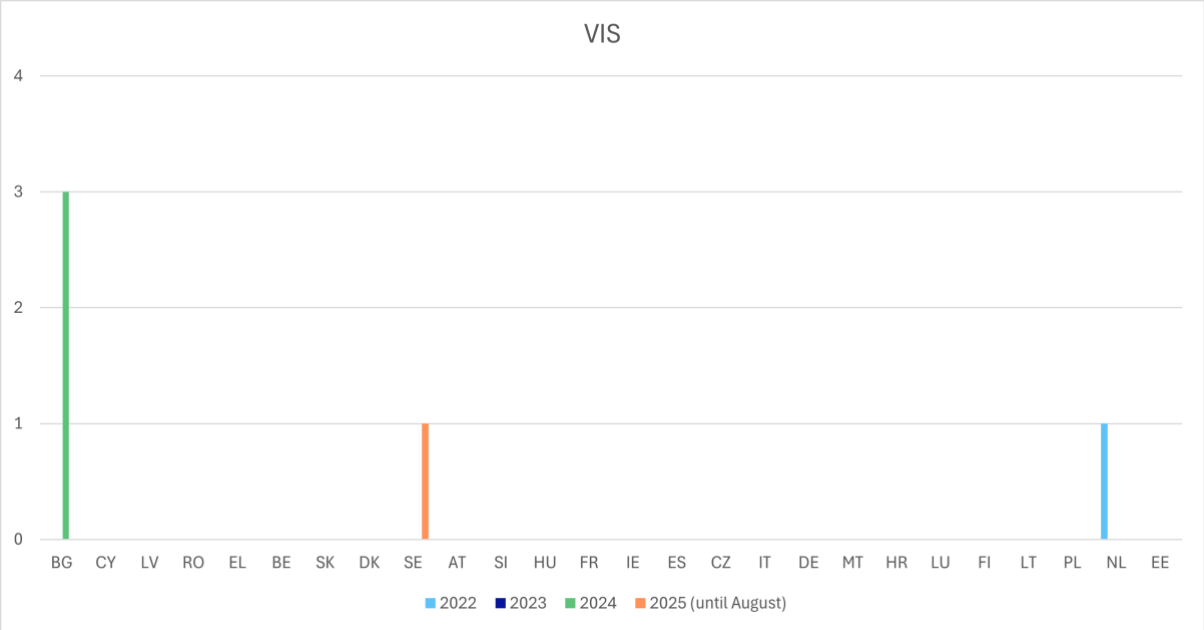
8.9 From January 2022 to 31 August 2025, please indicate, per year, which corrective powers you have applied and in how many cases. Please list the powers used according to Article 47(2)(b) LED (compliance orders). Amongst those cases, how many were related to the supervision of SIS[24] and VIS[25]?

58 The graph below depicts the number of cases where the SAs have applied their corrective powers, according to Article 47(2)(b) LED (compliance orders), related to the supervision of SIS, per year, during the reporting period.

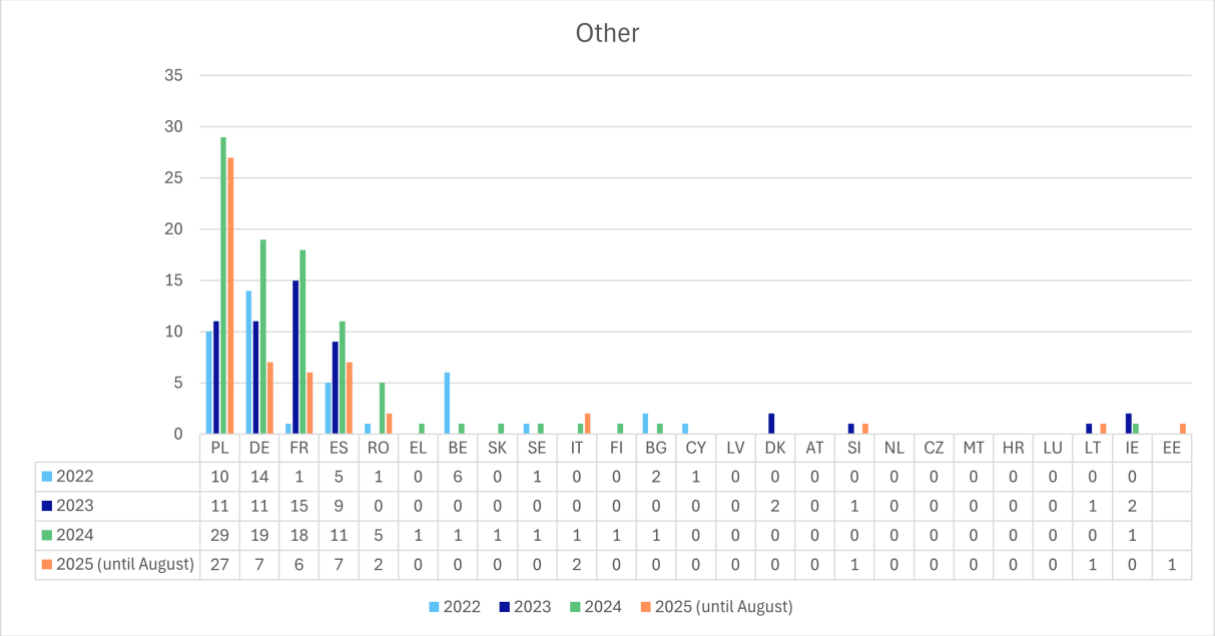
[24] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).
[25] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).



59 The graph below depicts the number of cases where the SAs have applied their corrective powers, according to Article 47(2)(b) LED (compliance orders), related to the supervision of VIS, per year, during the reporting period.



60 The graph below depicts the number of cases where the SAs have applied their corrective powers, according to Article 47(2)(b) LED (compliance orders), related to other than SIS/VIS, per year, during the reporting period.



	PL	DE	FR	ES	RO	EL	BE	SK	SE	IT	FI	BG	CY	LV	DK	AT	SI	NL	CZ	MT	HR	LU	LT	IE	EE
2022	10	14	1	5	1	0	6	0	1	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	
2023	11	11	15	9	0	0	0	0	0	0	0	0	0	0	2	0	1	0	0	0	0	0	1	2	
2024	29	19	18	11	5	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	
2025 (until August)	27	7	6	7	2	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1

8.10 From January 2022 to 31 August 2025, please indicate, per year, which corrective powers have you applied and in how many cases. Please list the powers used according to Article 47(2)(c) LED (limitation of processing). Amongst those cases, how many were related to the supervision of SIS[26] and VIS[27]?

61 The following graph depicts the number of corrective powers according to Article 47(2)(c) limitation of processing) applied by the SAs on an annual basis, for the reporting period from January 2022 to 31 August 2025, as well as cases related to the supervision of SIS, VIS and other.

[26] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).
[27] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).

	SIS				VIS				Other			
	2022	2023	2024	2025 (until August)	2022	2023	2024	2025 (until August)	2022	2023	2024	2025 (until August)
CY	0	0	0	0	0	0	0	0	1	0	0	0
LV	0	0	0	0	0	0	0	0	0	0	0	0
RO	0	0	0	0	0	0	0	0	0	0	0	0
EL	0	0	0	0	0	0	0	0	0	0	0	0
BE	0	0	0	0	0	0	0	0	8	2	1	0
SK	0	0	0	0	0	0	0	0	0	0	0	1
DK	0	0	0	0	0	0	0	0	0	0	0	0
SE	0	0	0	0	0	0	0	0	0	0	0	0
AT	0	0	0	0	0	0	0	0	0	0	0	0
SI	0	0	0	0	0	0	0	0	0	0	0	0
FR	0	0	0	0	0	0	0	0	0	0	0	0
IE	0	0	0	0	0	0	0	0	0	2	1	0
NL	0	0	0	0	0	0	0	0	0	0	0	0
ES	0	0	0	0	0	0	0	0	0	0	1	0
CZ	0	0	0	0	0	0	0	0	0	0	0	0
IT	0	0	0	0	0	0	0	0	0	0	0	0
DE	0	0	0	0	0	0	0	0	0	1	0	0
MT	0	0	0	0	0	0	0	0	0	0	0	0
HR	0	0	0	0	0	0	0	0	0	0	0	0
LU	0	0	0	0	0	0	0	0	0	0	0	0
FI	0	0	0	0	0	0	0	0	0	0	0	0
BG	0	0	0	0	0	0	0	0	0	0	0	0
LT	0	0	0	0	0	0	0	0	0	0	0	0
PL	0	0	0	0	0	0	0	0	0	0	0	0
EE	0	0	0	0	0	0	0	0	-	-	-	0
HU	0	0	0	0	0	0	0	0	-	-	-	-

8.11 Have the competent authorities or processors complied with decisions issued since the last review where you exercised your corrective powers?

62 21 SAs reported that competent authorities or processors complied with decisions issued since the last review, while 4 SAs replied negatively (2 SAs stated that this was not applicable). In particular, one SA reported that its decisions ordering compliance with the provisions were appealed to the courts, which means that the competent authorities did not comply with these decisions pending judicial review Another SA reported that in most cases, the competent authorities followed the opinion or complied with the SA's decisions and that, in general, the relevant competent authorities are formally requested to present effective measures to remedy any data protection violations, as well as preventative procedures. It also specified that in the case of larger procedures (for example, video surveillance), a follow-up inspection is often carried out on site, while in some cases, the legal matter remains unresolved and is therefore

ongoing, even though the data concerned in the specific case have been deleted by the competent authority. Another SA stated it provided a specific deadline for compliance and checks on whether measures have been taken and, in the negative, there is a procedure foreseen by law.

8.12 If you have not used any of your corrective powers since the last review, please provide reasons

63 In one case, the SA stated that it used its corrective powers, but not in the area of SIS/VIS. Another SA reported that in some cases, the technical aspects of the data processing systems used by the competent authorities do not allow for full compliance with data protection law and no measures were taken if the systems were absolutely necessary for the fulfilment of official tasks, while alternatives were agreed in some cases. In addition, corrective powers have not been used when the competent authorities changed their behaviour voluntarily after being informed by the SA, as it is sufficient to point out deficiencies and/or notify the competent authority of the SA's legal assessment (such as a reprimand under Article 58(2)(b) GDPR). Two SAs reported that their lack of use of corrective powers was due to the limited number of complaints, while one SA stated that it was because the nature of the infringement was not serious enough and another SA stated there were no grounds for using them. In another country, SAs competent for courts, consider themselves unable to exercise corrective powers in relation to the entities under their supervision, as these entities are excluded from the scope of application of the act implementing the LED. Nevertheless, this interpretation is inconsistent with the Act on the Organisation of Common Courts, which grants judicial supervisory authorities, inter alia, the power to request the controller or processor to bring data processing into compliance with the requirements of the act implementing the LED.

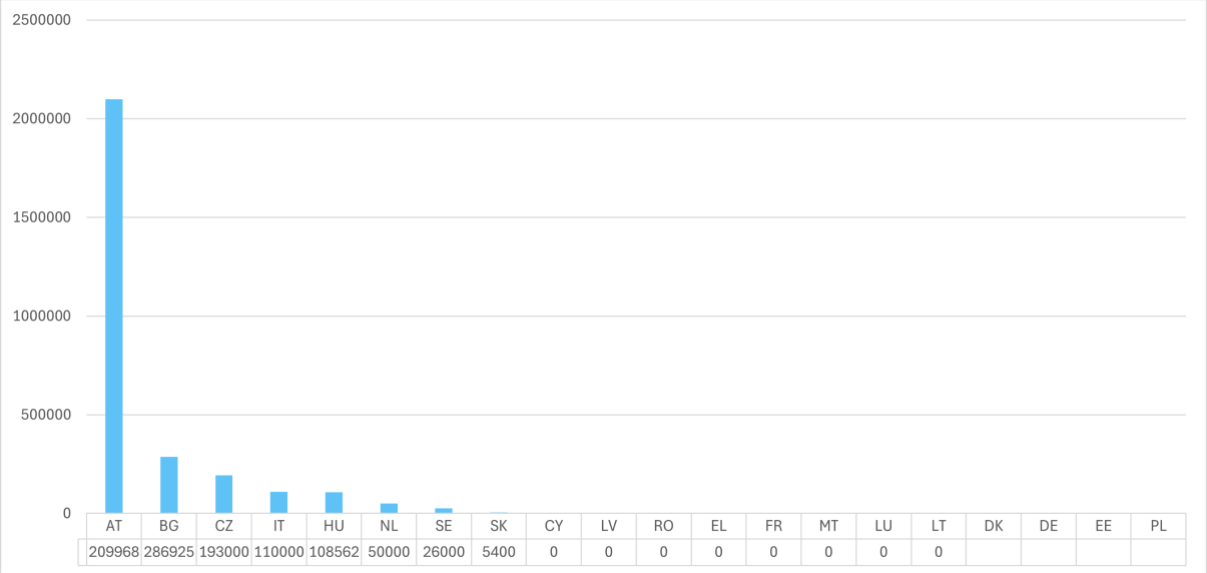
8.13 Do you have the ability to impose an administrative fine?

64 16 SAs reported that they are able to impose administrative fines, while 11 SAs replied negatively.

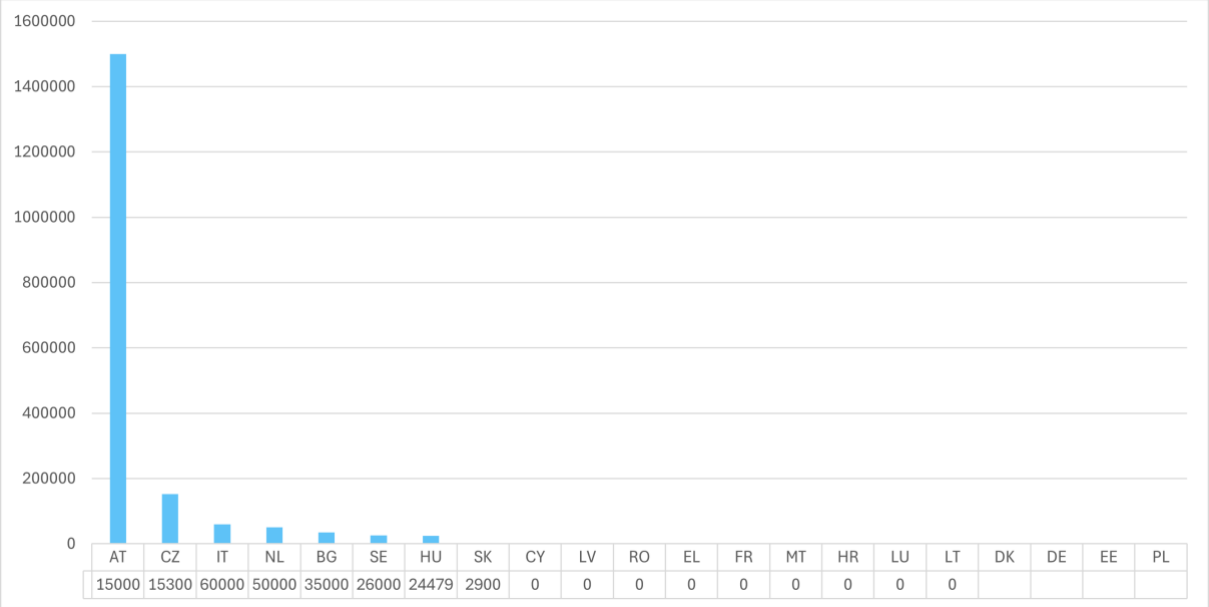
8.13.a Are there any limitations on your ability to impose an administrative fine?

65 16 SAs reported limitations on their ability to impose administrative fines. In particular, these SAs stated that such limitations concern the amount of the fines, which may arise from the law, depending on the provision infringed or the nature of the infringement. One SA reported that no administrative fine can be imposed for processing where the controller is the State (e.g. Ministries) and that however, it is possible for that SA to impose a fine where the controller is a public body distinct from the State (e.g. a municipality or a company operating a public service such as transportation). Another SA stated that this may only occur for a limited number of infringements of the LED. Another SA reported it is cannot impose fines on authorities and public bodies, as well as on bodies established under private law that act on behalf of the State and that there are also provisions on the statute of limitations in national procedural law that must be observed when imposing fines.

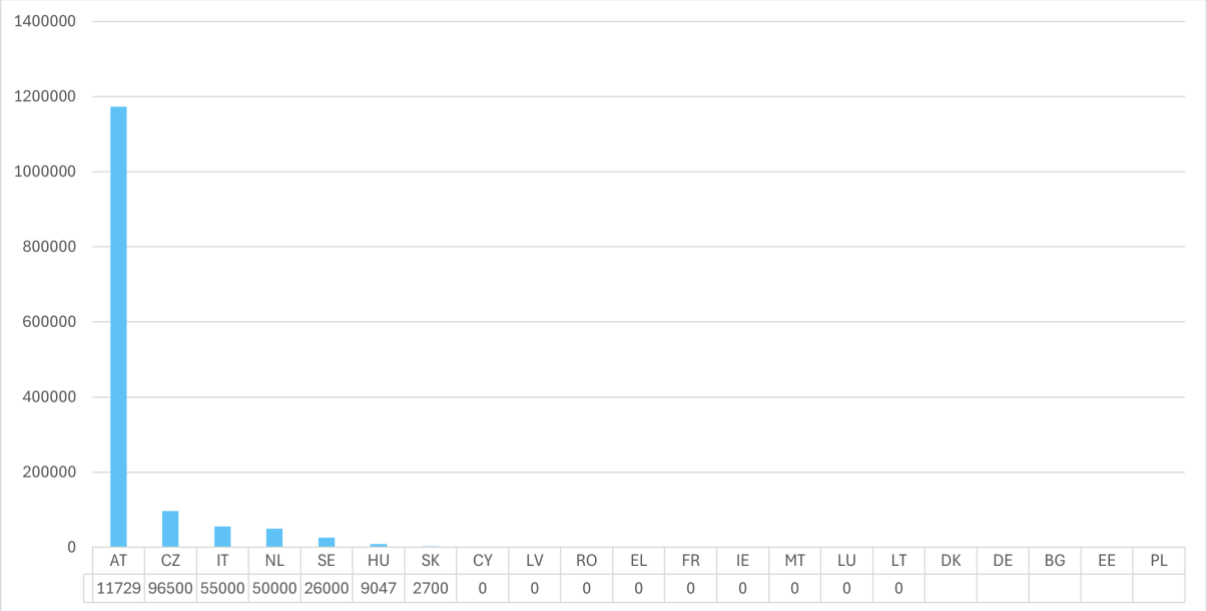
66 The first graph below showcases the total amount of fines imposed during the reporting period (in €):



67 The second graph showcases the amount of the highest fine imposed during the reporting period (in €):



68 The third graph showcases the average amount of the fines imposed during the reporting period (in €):



9 Power pursuant to Article 47(5) LED

9.1 From January 2022 to 31 August 2025, have you exercised your power to bring infringements of your national law(s) transposing the LED to the attention of judicial authorities?

69 The majority of SAs (25 SAs) have not exercised their power to bring infringements of their national law(s), while 2 SAs reported positively.

9.2 From January 2022 to 31 August 2025, have you exercised your power to commence or otherwise engage in legal proceedings?

70 The majority of SAs (23 SAs) have not exercised their power to commence or engage in legal proceedings, while 4 SAs replied positively.

9.3 Which difficulties, if any, did you face in exercising this power? (such as procedural difficulties in your national law, because it would create an outcry from your national parliament etc.) Please also state if you do not have the power to carry out either or both of these actions.

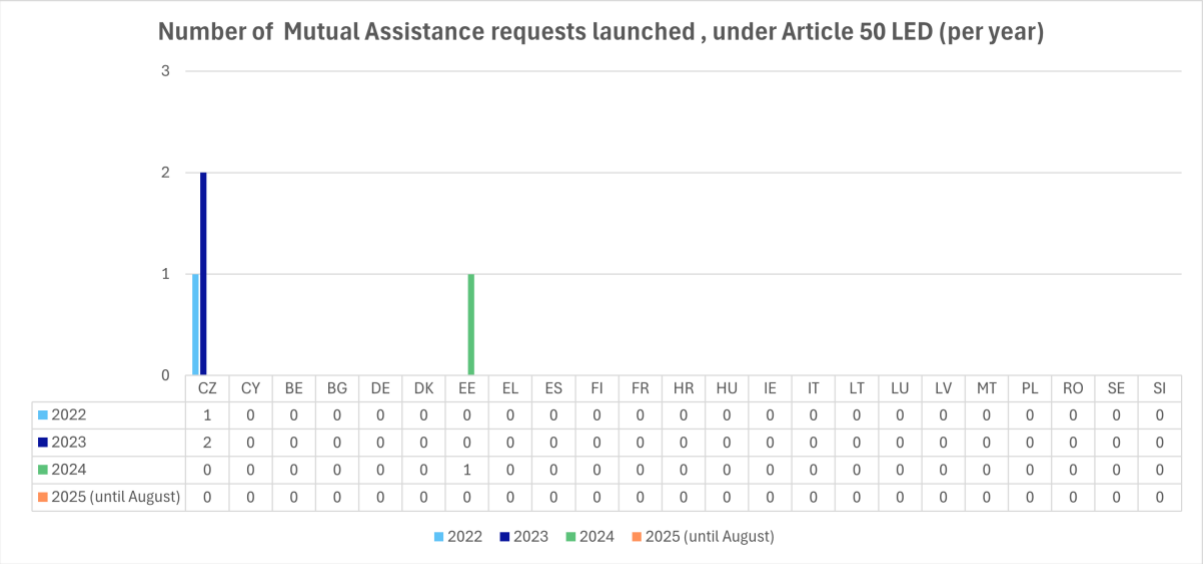
71 7 SAs reported that they did not face any difficulties in exercising their power to commence or otherwise engage in legal proceedings, while the great majority of SAs either did not provide input or reported this as not applicable (12 SAs). Three SAs reported that Article 47 (5) LED has not been transposed into their national law, while one SA stated that it does not have the power to bring infringements of the national laws transposing the LED to the attention of judicial authorities on its own initiative or to commence legal proceedings.

10 Cooperation

10.1 Please indicate the number of Mutual Assistance requests under Article 50 LED (please indicate per year)

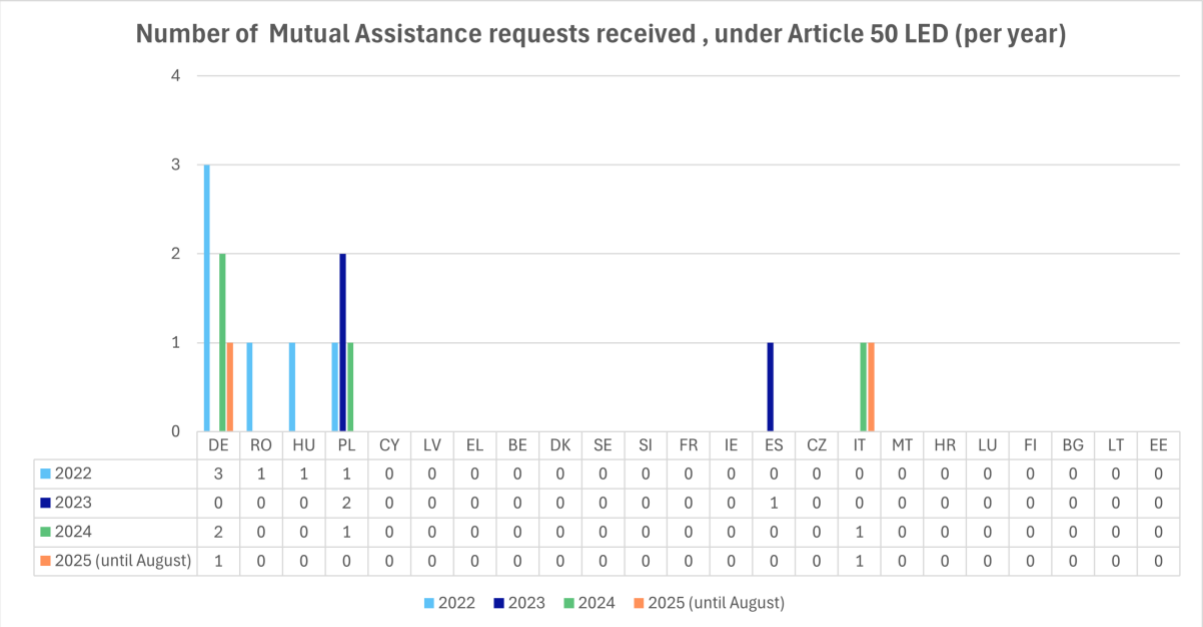
72 The graph below depicts the number of Mutual Assistance requests launched under Article 50 LED, per year, during the reporting period.

73 Please note that cooperation between EU/EEA DPAs in the form of mutual assistance is primarily embedded in the IMI system, but this system does not provide an avenue for cooperation or mutual assistance specifically tailored to Article 50 LED. It is therefore complex to gather correct statistics on this matter.



	CZ	CY	BE	BG	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IT	LT	LU	LV	MT	PL	RO	SE	SI
2022	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2024	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

74 The graph below depicts the number of Mutual Assistance requests received by the SAs each year during the reporting period.



	DE	RO	HU	PL	CY	LV	EL	BE	DK	SE	SI	FR	IE	ES	CZ	IT	MT	HR	LU	FI	BG	LT	EE
2022	3	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	0	0	0	2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
2024	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
2025 (until August)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

10.1.a Please indicate the subject matter of the requests (including the type of cooperation – e.g. request for info, to carry out an investigation, inspection etc.)

75 One SA reported that the request concerned information to facilitate communication between national competent law enforcement authorities in relation to a data subject's request. Two SAs reported that such requests concerned facial recognition carried out by the police. One SA stated that it also concerned the right to erasure of personal data, while another SA reported that it concerned the legal situation on information to be provided to data subjects and the supervisory rights of data protection authorities with regard to documents subject to secrecy, regulations for the processing of biometric data, the use of body-worn cameras in prison, the definition of automated processing systems and guidance, opinions or examples on the powers of DPAs in criminal cases. Several SAs (4 SAs) reported that such requests concerned the Schengen Information System (i.e. the validity of alerts ordering entry and stay bans, the legality of issuing those alerts, the right to access SIS data lodged with another SA etc.). In two cases, such requests concerned Article 25 LED on what constitutes 'automated processing systems'.

10.2 Have you encountered any obstacles (e.g. of an administrative nature) when requesting or providing assistance to another DPA?

76 The majority of SAs (23 SAs) have not encountered obstacles when requesting or providing assistance to another SA. 2 SAs reported obstacles related to the lack of a dedicated system for communication on Schengen-related issues. Consequently, one SA used the IMI system, which is not tailored for SIS cases. This caused confusion for the SA that received the IMI communication, as it was unclear whether such request should be classified as requests under Article 50 LED and thus whether it met the formal requirements. Another SA noted a lack of communication from the SAs contacted.

10.3 Which EDPB guidelines have proven helpful for your work under the LED and/or of the controllers?

77 The majority of SAs reported that the Guidelines on the use of facial recognition technology in law enforcement[28] were helpful to their work under the LED (15 SAs). Many SAs also indicated that the Guidelines on Article 37 LED[29] were useful (8 SAs), while a few SAs referred to the Guidelines on data subject rights: right of access[30] under the GDPR (3 SAs). In addition, a few SAs mentioned other guidelines not related to the LED as having been helpful (i.e. the Guidelines on restrictions under Article 23 GDPR[31], the EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority[32], the Guidelines on the concepts of

[28] EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adopted on 26 April 2023, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en
[29] EDPB Guidelines 01/2023 on Article 37 Law Enforcement Directive, adopted on 19 June 2024, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012023-article-37-law-enforcement-directive_en
[30] EDPB Guidelines 01/2022 on data subject rights - Right of access adopted on 28 March 2023, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en
[31] Guidelines 10/2020 on restrictions under Article 23 GDPR adopted on 13 October 2021, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en
[32] EDPB Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority adopted on 28 March 2023, available at: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202208_identifying_lsa_targeted_update_v2_en.pdf

controllers and processors[33] and the EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models).[34]

10.4 What are the topics that should be covered by future EDPB guidelines to foster the consistent application of the LED?

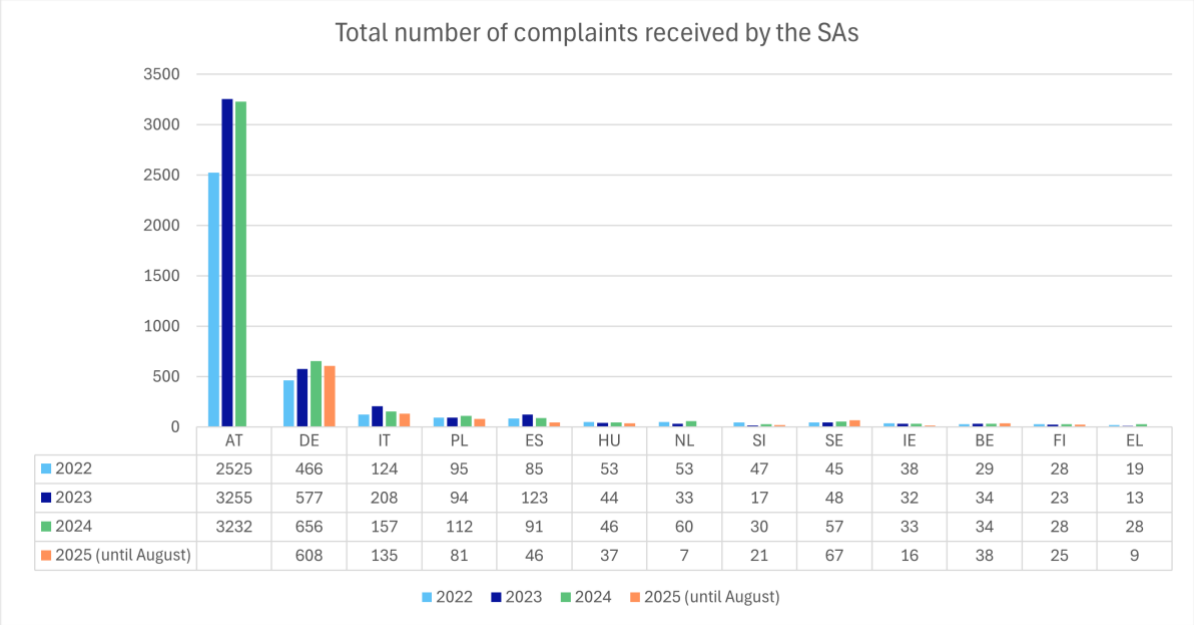
78 The majority (8 SAs) that replied, indicated that further guidance would be useful on issues related to data subjects' rights, with additional recommendations on interpreting the right of access and a focus on minors. Several (5 SAs) highlighted the need for guidance on the use of artificial intelligence in the context of law enforcement, as well as the development of criteria for data protection impact assessments ('DPIA's), considering the specific characteristics of high-risk operations such as processing biometric or sensitive data and profiling. In addition, 6 SAs indicated that clarification on the scope of the LED is required, particularly regarding the notions of competent authorities, the types of processing falling under law enforcement purposes and the scope of judicial functions. Similarly, several SAs (6) noted the need to delineate the material scope of application between the GDPR and the LED, as well as the interplay with other LED-related regulations, such as those concerning EU Large-Scale IT systems. A few SAs (2 SAs) also highlighted the need to clarify the role and responsibilities of processors in the public sector and issues of joint responsibility under the GDPR and the LED. Some SAs (4 SAs) also noted that guidance on cross-border cooperation and mutual assistance would be helpful. A few (3 SAs) indicated that guidance on processing special categories of personal data under the LED would be needed, while a few (2 SAs) referred to the need for clarification on data retention issues. In two cases, SAs referred to the need for guidance regarding data processing under the LED for research purposes, while one SA referred to the legal basis for lawful processing of personal data (Recital 33 and Article 8 LED) and on transparency obligations (Articles 12 and 13 LED). A different SA referred to the need for guidance on issues pertaining to evolving LED-related case law, another SA mentioned guidance for processing that does not require identification, and an SA noted that guidance would be helpful regarding DPOs, as well as data breach notifications.

11 Complaints

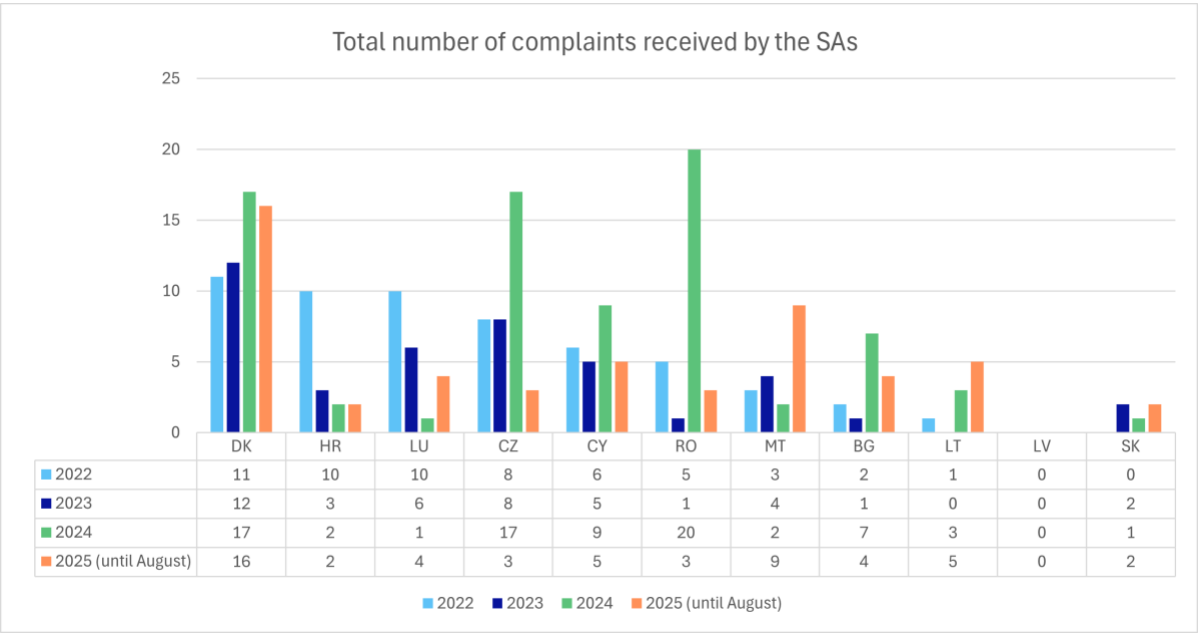
11.1 How many complaints have you received during this reporting period (i.e. from January 2022 to 31 August 2025)? Please state the number per year. How many of these were lodged by bodies, organisations or associations in accordance with Article 55 LED?

79 The two graphs below depict the number of complaints received by the SAs, per year, during the reporting period. Please note that the two tables below show information regarding 24 Member States, as some SAs did not provide information.

[33] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR adopted on 7 July 2021, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[34] Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

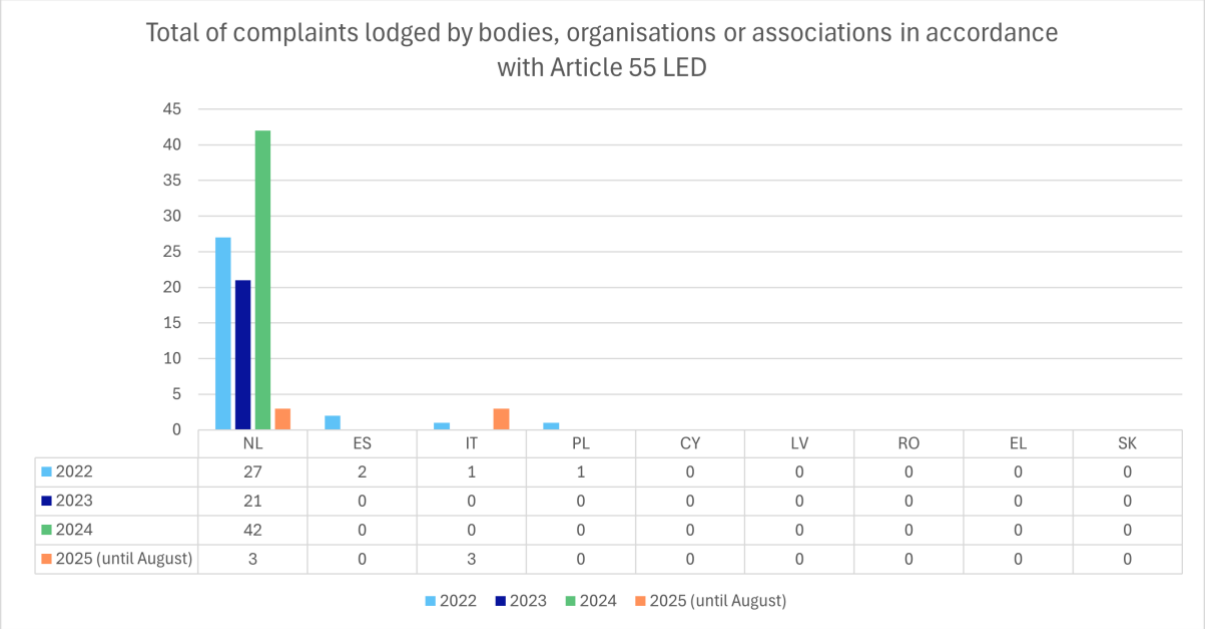


	AT	DE	IT	PL	ES	HU	NL	SI	SE	IE	BE	FI	EL
2022	2525	466	124	95	85	53	53	47	45	38	29	28	19
2023	3255	577	208	94	123	44	33	17	48	32	34	23	13
2024	3232	656	157	112	91	46	60	30	57	33	34	28	28
2025 (until August)		608	135	81	46	37	7	21	67	16	38	25	9

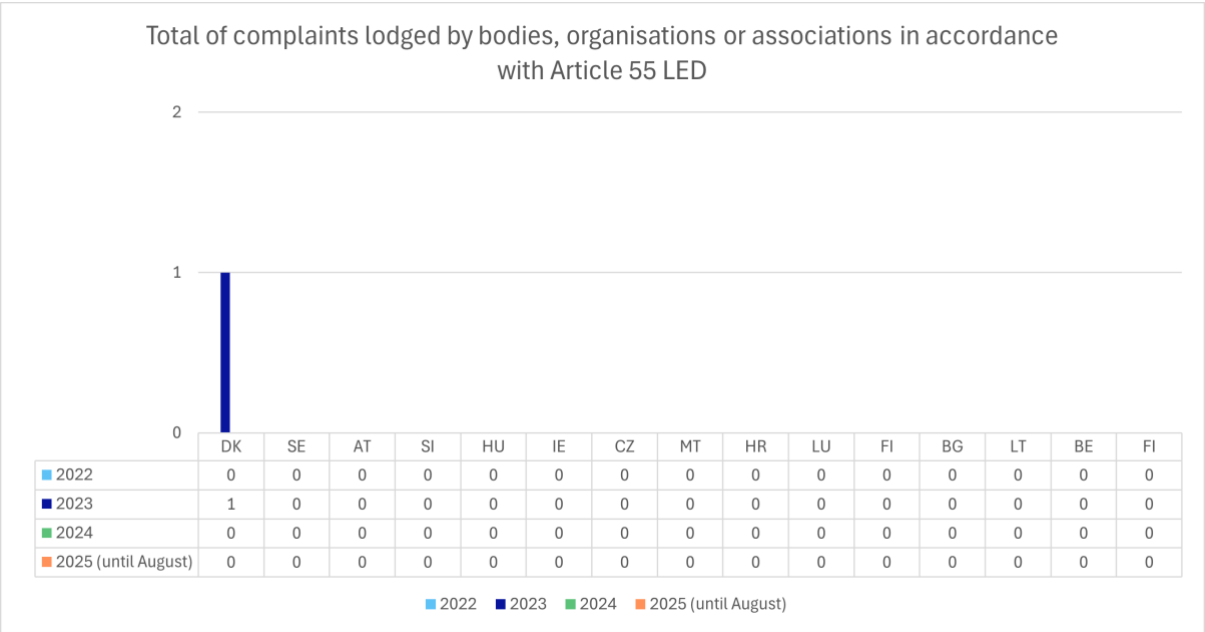


	DK	HR	LU	CZ	CY	RO	MT	BG	LT	LV	SK
2022	11	10	10	8	6	5	3	2	1	0	0
2023	12	3	6	8	5	1	4	1	0	0	2
2024	17	2	1	17	9	20	2	7	3	0	1
2025 (until August)	16	2	4	3	5	3	9	4	5	0	2

80 The following two graphs indicate the total number of complaints lodged by bodies, organisations or associations, per year, for the reporting period, in accordance with Article 55 LED. Please note that the two tables below show information regarding 24 Member States, as some SAs did not provide information.



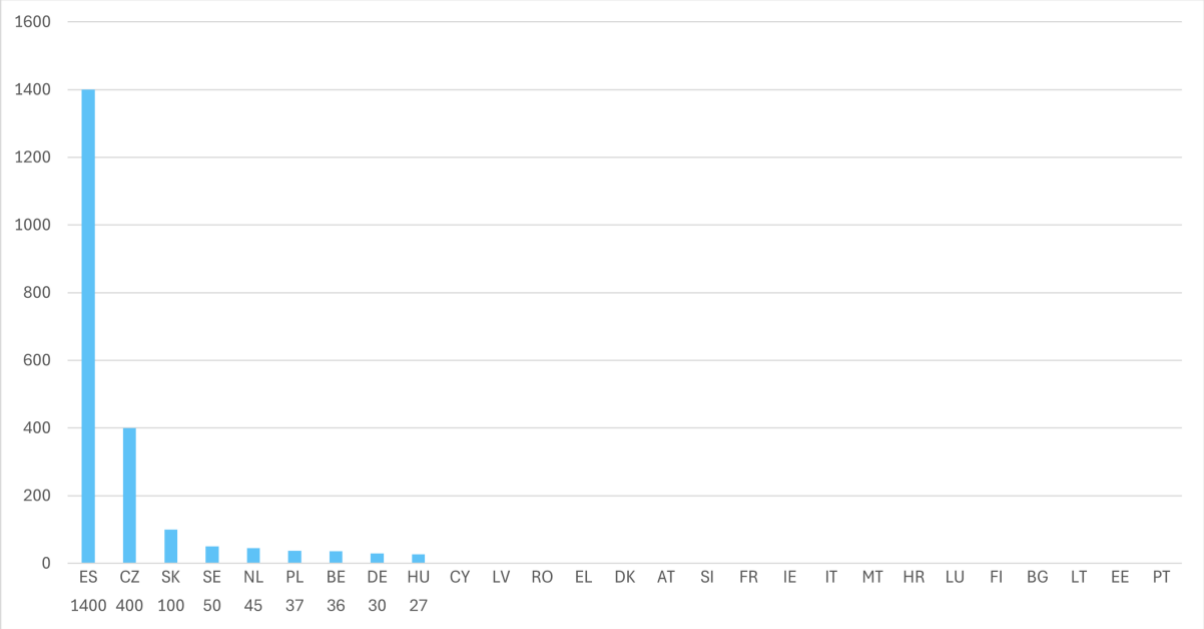
	NL	ES	IT	PL	CY	LV	RO	EL	SK
2022	27	2	1	1	0	0	0	0	0
2023	21	0	0	0	0	0	0	0	0
2024	42	0	0	0	0	0	0	0	0
2025 (until August)	3	0	3	0	0	0	0	0	0



	DK	SE	AT	SI	HU	IE	CZ	MT	HR	LU	FI	BG	LT	BE	FI
2022	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2024	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

11.2 Has there been an increase in complaints following the last review (i.e. from January 2022 to 31 August 2025) in your Member State?

81 11 SAs reported an increase in complaints following the last review, while 15 SAs stated there has been a decrease (1 SA reported not applicable). The following graph depicts the increase in percentages.



11.3 From January 2022 to 31 August 2025, please indicate the issues raised most often in these complaints (multiple choices are possible).

82 The vast majority of SAs (21 SAs) replied that the issues raised most often related to the data subjects' rights of access and rectification. In addition, many SAs (8 SAs) reported having faced issues regarding the respect for the principles of proportionality and necessity, as well as the obligation to ensure the security of processing (10 SAs). Several SAs stated that the issues regard the determination of the legal basis (8 SAs), as well as the data subjects' right to information (10 SAs). Several SAs also reported issues regarding respect for the purpose limitation (6 SAs) and data minimisation (7 SAs) principles, as well as the accuracy of the data (7 SAs) and storage limitation (6 SAs). In addition, several SAs reported issues on the accountability of the controller (7 SAs) and the modalities for exercising data subjects' rights under Article 12 LED (5 SAs), as well as the conditions related to processing special categories of personal data (6 SAs). A few SAs reported issues regarding data protection by design and by default as provided in Article 20 LED (3 SAs), and one mentioned issues relating to the obligation to keep track of the logs. One SA also reported issues about the obligation to conduct a data protection impact assessment, while several SAs reported other issues. In particular, two SAs reported that most complaints concerned data subjects' rights, with one also mentioning issues related to irregularities in the processing of personal data or the refusal by telecommunications operators or insurance companies to provide data. In some cases, data subjects' rights could only be exercised within the scope provided by specific procedural laws governing such proceedings and not on the basis of the transposing law of the LED; Another SA reported issues regarding the distinction between the right of access to criminal files and the right of access to data processed by courts, as well as the principle of minimisation. An SA reported an increase in complaints where multiple data protection issues are raised within the same complaint (e.g. access rights, alleged disclosure, alleged unfair processing), while two SAs highlighted the issue of unauthorised or unlawful use of databases.

11.4 With respect to complaints made regarding the processing of special categories of personal data, what are the main infringements you have found with respect to the

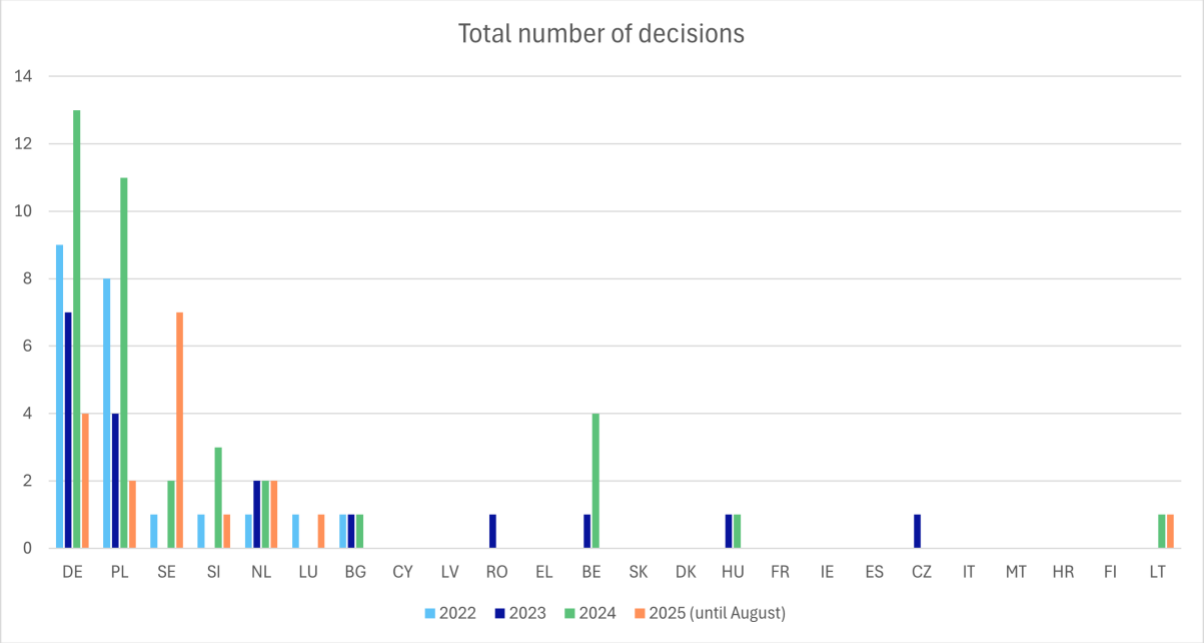
conditions set down in Article 10 LED (i.e., that the processing was not strictly necessary, including whether the competent authorities have demonstrated strict necessity, that the processing was not authorised by law, where you determined that the data hasn't been made manifestly public etc)? Has recent CJEU case-law (e.g. C-205/21, C-80/23) changed your approach?

83 Several SAs (9 SAs) reported that they did not issue decisions on complaints concerning the processing of special categories of personal data either because no such complaints were received or because the issue did not arise prominently in the cases handled. Two SAs noted that no infringements of Article 10 LED were identified during the reporting period. Among the SAs that identified issues, the main infringements of Article 10 LED concerned the absence of a legal basis or authorisation by national law for processing special categories of personal data. In two cases, the SAs reported that this was due to the manner of the transposition of Article 10 LED into their national legislation. Two SAs also reported that controllers failed to demonstrate that the processing was strictly necessary, as required by Article 10 LED. In two cases, the SAs reported that infringements were linked to breaches of data protection principles, particularly purpose limitation and data minimisation. Regarding the impact of recent CJEU case-law, some SAs (3 SAs) noted that this has not led to a change in their approach, largely because the relevant national legal frameworks have not yet been amended or because the issues addressed in the judgements did not directly correspond to the cases assessed by the SAs. However, one authority reported that it had applied the CJEU case-law in a case where strict necessity had not been demonstrated by the controller.

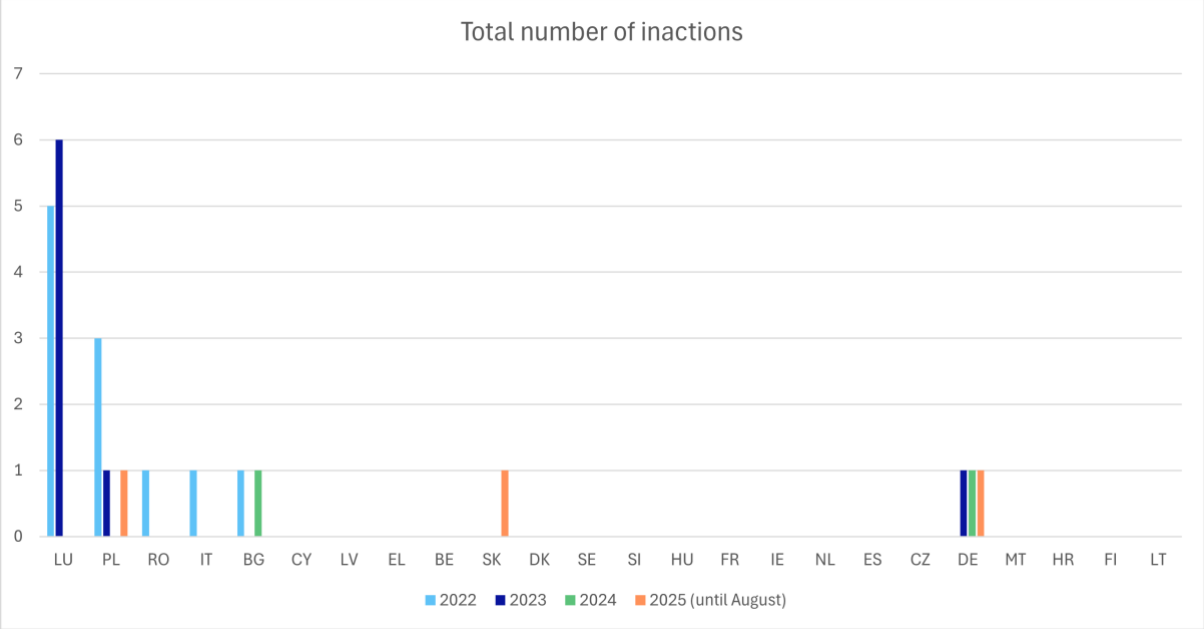
12 Judicial review – contested decisions

12.1 Please indicate the number of decisions/inactions per year (from January 2022 to 31 August 2025) that were challenged in court.

84 The graph below shows the number of decisions per year that were challenged in court, during the reporting period.

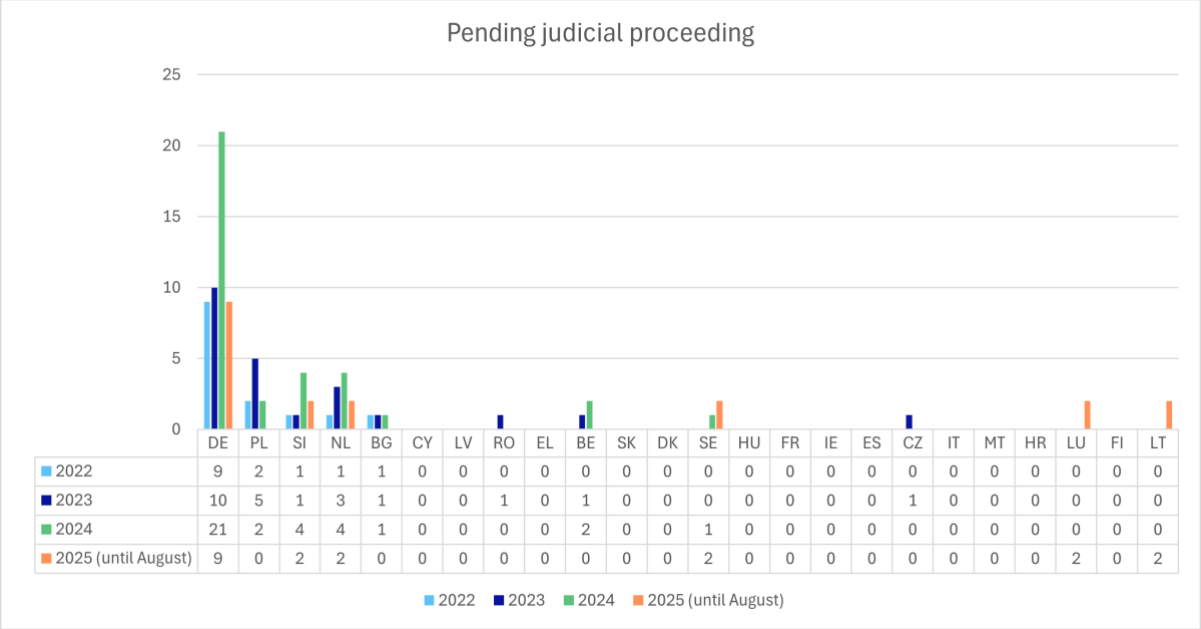


85 The graph below shows the number of inactions per year that were challenged in court, during the reporting period.



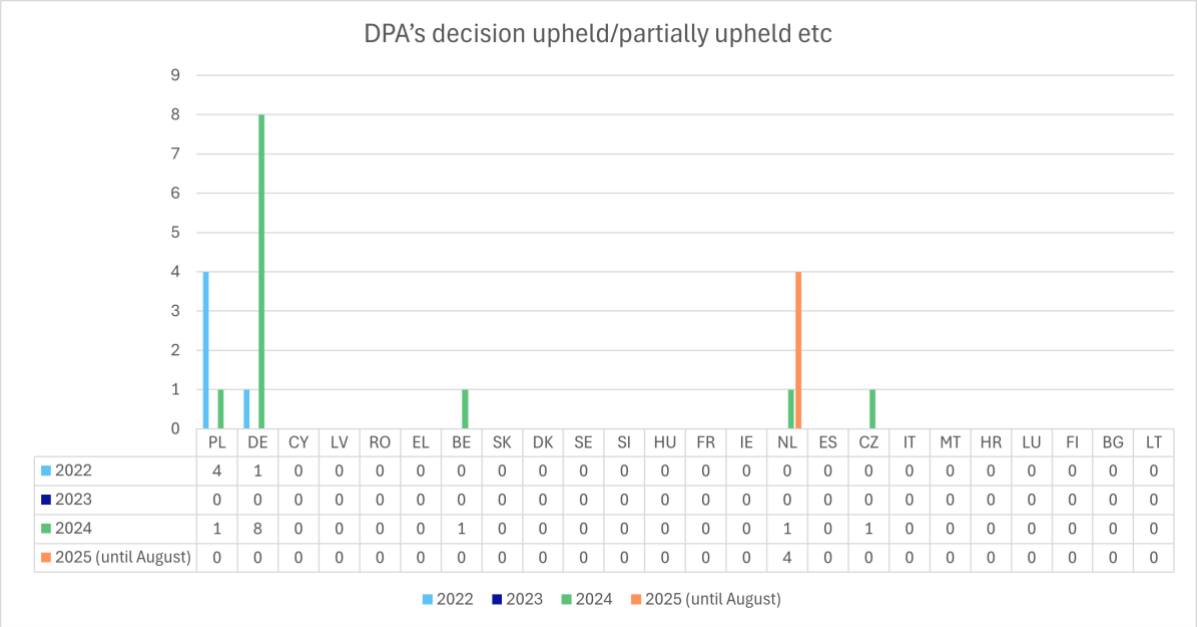
12.1.a Please indicate, per year and per outcome, how many actions in court are pending, were considered to be inadmissible, or led to the DPA's decision being (partially) upheld - Decisions:

86 The graph below delicts the number of pending judicial actions, per year, during the reporting period in terms of decisions.



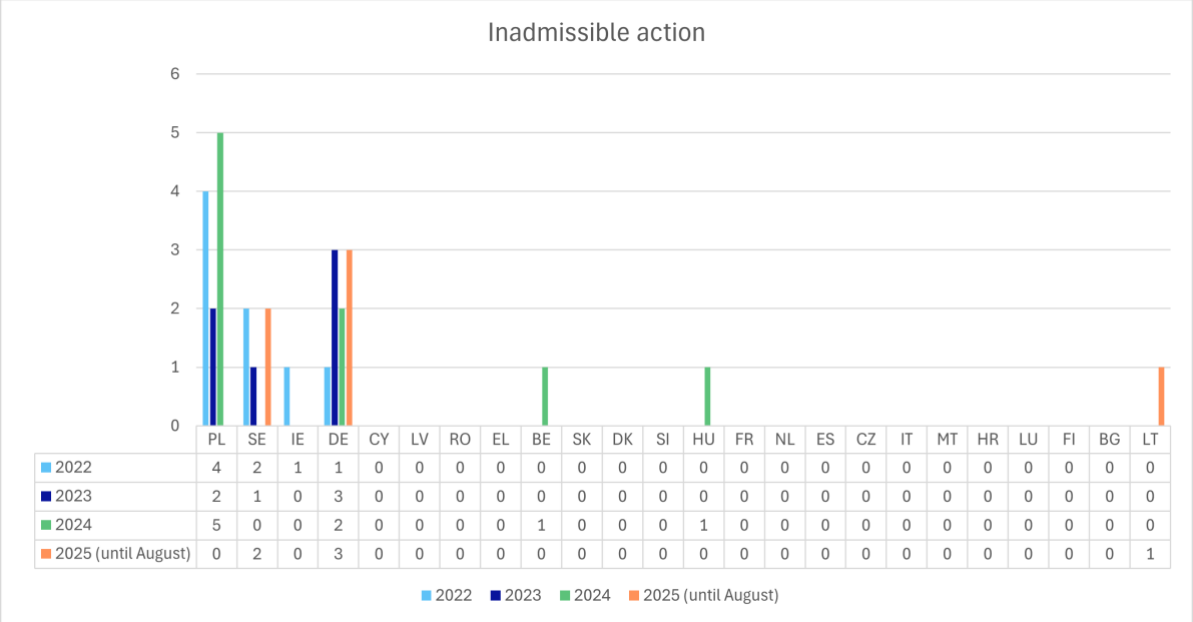
	DE	PL	SI	NL	BG	CY	LV	RO	EL	BE	SK	DK	SE	HU	FR	IE	ES	CZ	IT	MT	HR	LU	FI	LT
2022	9	2	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	10	5	1	3	1	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
2024	21	2	4	4	1	0	0	0	0	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	9	0	2	2	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	2	0	2

87 The graph below shows the number of upheld / partially upheld decisions, per year during the reporting period.



	PL	DE	CY	LV	RO	EL	BE	SK	DK	SE	SI	HU	FR	IE	NL	ES	CZ	IT	MT	HR	LU	FI	BG	LT
2022	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2024	1	8	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0
2025 (until August)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0

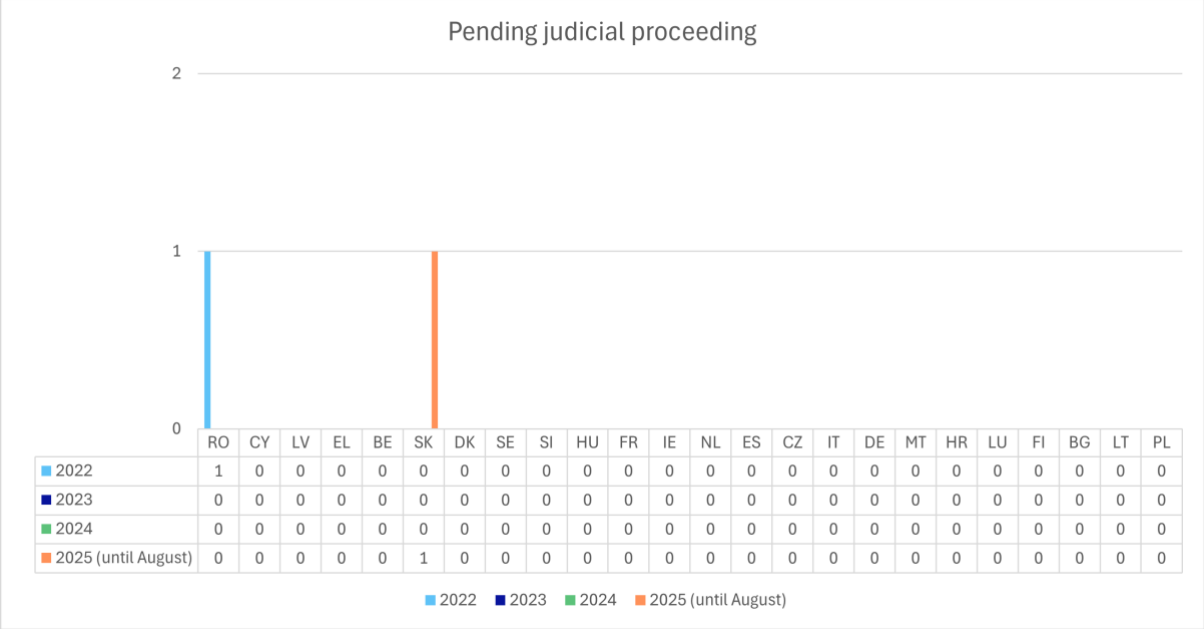
88 The graph below shows the number of inadmissible actions, per year during the reporting period.



	PL	SE	IE	DE	CY	LV	RO	EL	BE	SK	DK	SI	HU	FR	NL	ES	CZ	IT	MT	HR	LU	FI	BG	LT
2022	4	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	2	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2024	5	0	0	2	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	0	2	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

12.1.b Please indicate, per year and per outcome, how many actions in court are pending, were considered to be inadmissible, or led to the DPA's decision being (partially) upheld - Inactions:

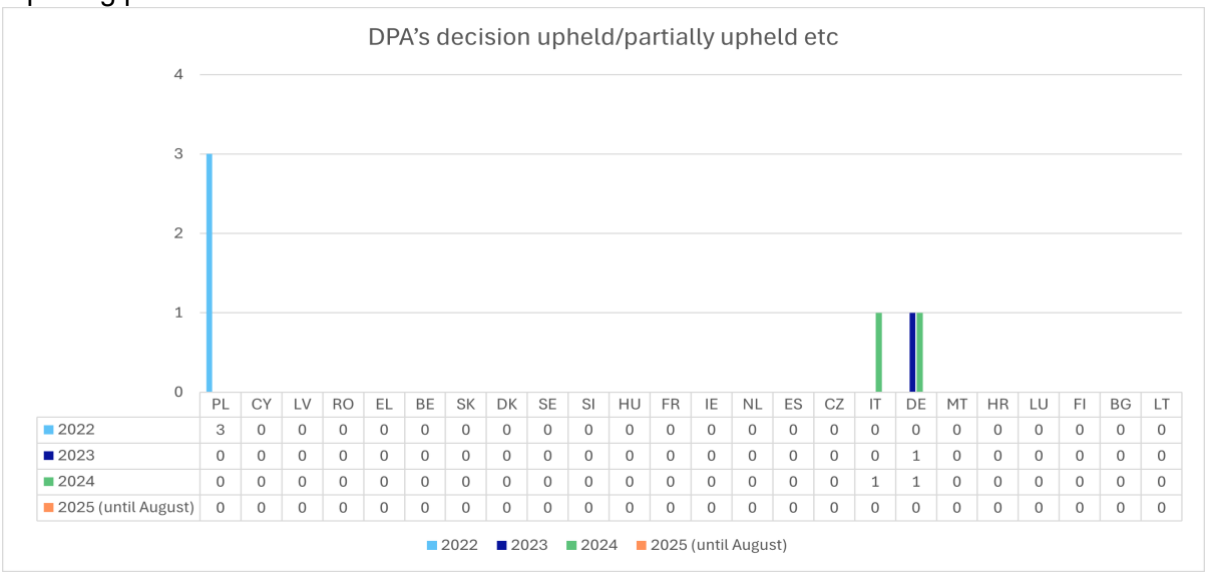
89 The graph below depicts the number of pending judicial actions per year during the reporting period, in terms of inactions.



	RO	CY	LV	EL	BE	SK	DK	SE	SI	HU	FR	IE	NL	ES	CZ	IT	DE	MT	HR	LU	FI	BG	LT	PL
2022	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2023	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2024	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2025 (until August)	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

90 The graph below depicts the number of inadmissible actions per year for the reporting period.

91 The graph below depicts the number of upheld/partially upheld actions per year for the reporting period.



12.1.c What were the main aspects challenged (e.g., a decision of a DPA may be challenged on more administrative issues' aspects, such as the fine amount or just concern a more LED-related issue, e.g., the right to erasure - either substantial matters or administrative matters for the DPAs' decision) and by who (competent authority /processor/ data subject)?

92 9 SAs provided the following information. One SA stated that administrative matters were challenged in one case by a data subject on parts of a decision. Another SA reported that in one ongoing case, a data subject lodged a complaint with a court in 2024 against a decision of the SA regarding a rejected SIS access request by the responsible body and that in another case, there was a dispute over whether a suitable legal basis exists and whether log data falls under the data subject's right of access, where the police filed a lawsuit in response to the SA's formal complaint and the court ruled there was no right to access this information. That SA also reported that decisions were challenged by the data subjects on the basis that the results of the SA's investigations were incorrect, while another decision concerned the right to erasure regarding data stored by the police, including a separate decision on an alleged data transfer from the public prosecutor's office to a lawyer; all of which were upheld in court. Another SA reported that the main issues challenged concern the refusal of access or partial access to personal data by the competent authorities. An SA also reported a discussion on the issue of legal personality for the supervisory body on police information management

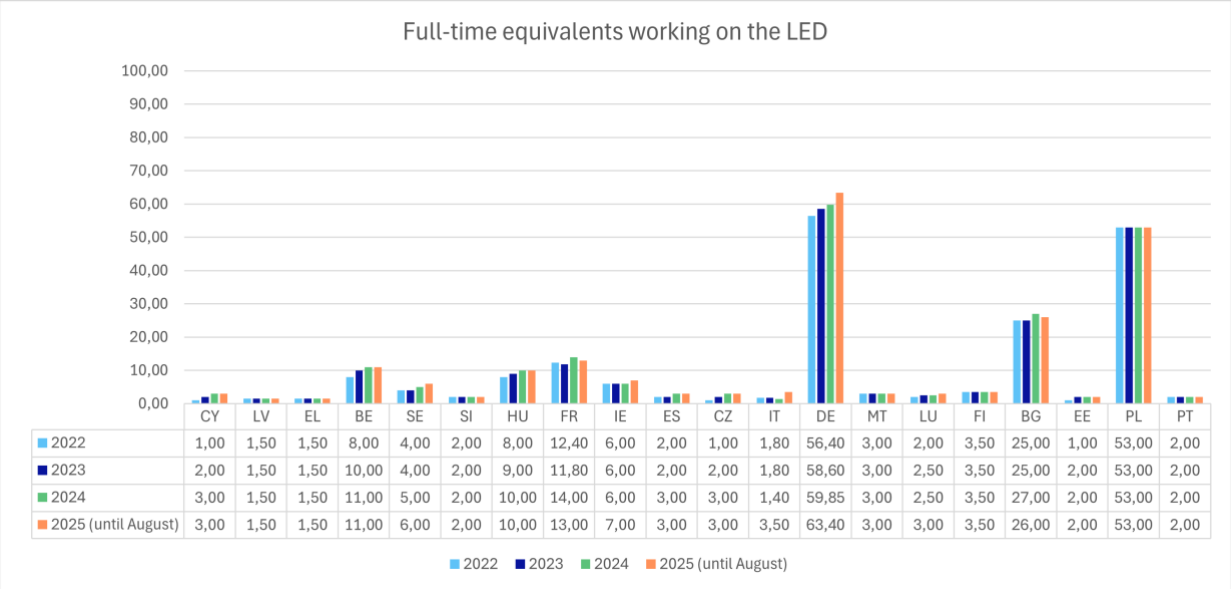
which is responsible for supervising police data processing under the LED and GDPR regarding the legality and completeness of investigations and decisions, as well as the national standardised system of indirect access. Another SA stated that disputes have mostly concerned access to data subjects' data, as restrictions on access are rather broad or are being interpreted broadly; among these, some cases involved denying data subjects access to prison registry data entries concerning them. An SA stated that there has been a single legal challenge brought in respect of an SA decision on LED-related matters and that the proceedings considered procedural matters (including whether the proceedings were brought within time) and did not relate to substantive LED matters, with the challenge initiated by the data subject. In another case, the SA reported that in 2023, it found the data controller had violated the principles of purpose limitation and accountability and had failed to take the necessary data security measures due to the publication of security camera recordings on a Facebook page. The SA imposed a fine for the violations, and the data controller sought annulment of the decision. The court dismissed the data controller's claim in 2024. A data controller challenged the decision of the SA, while the data subject intervened as an interested party on the side of the SA. In its decision, the SA found that the data controller had violated the principles of purpose limitation and data minimisation. The court ordered the SA to repeat the process, clarify the lawfulness of the purpose of data processing and examine the circumstances referred to by the data controller in terms of data minimisation.

93 One SA reported a challenge concerning the right of access to personal data and the right of erasure, while another reported that it concerned the inactivity of the SA. In one case, the SA reported it was about access to and erasure of personal data stored in the SIS database. Another SA stated that its decisions were primarily challenged by data subjects and related to both procedural and substantive aspects, as well as to the disregard of relevant administrative court case-law and the excessive duration of proceedings. The complaints often highlighted issues relating to the right to erasure, the right to fair proceedings and the scope of permissible processing of particularly sensitive data, such as information on convictions, solitary confinement, or health-related data. In a few cases, corrective measures were also contested by data processors, such as the National Police Headquarters, which argued for the continued processing of data subject to a deletion order. In another case, the SA issued a decision to impose a fine, which was challenged by the data processor on several grounds, most importantly evidence, interpretation of the law and the amount of the fine. Decisions regarding complaints are challenged by data subjects, usually regarding the finding that no infringement has taken place or that further investigation would be required but the case usually does not meet the criteria for further investigation. An SA stated that such cases referred to inaction on administrative matters for the decision of the data protection authority, refusal of investigation for lack of information on national law and obtaining consent from data subjects, which is ongoing. In terms of decisions, a decision of the SA is challenged for administrative reasons (ongoing case).

13 Human, financial and technical resources

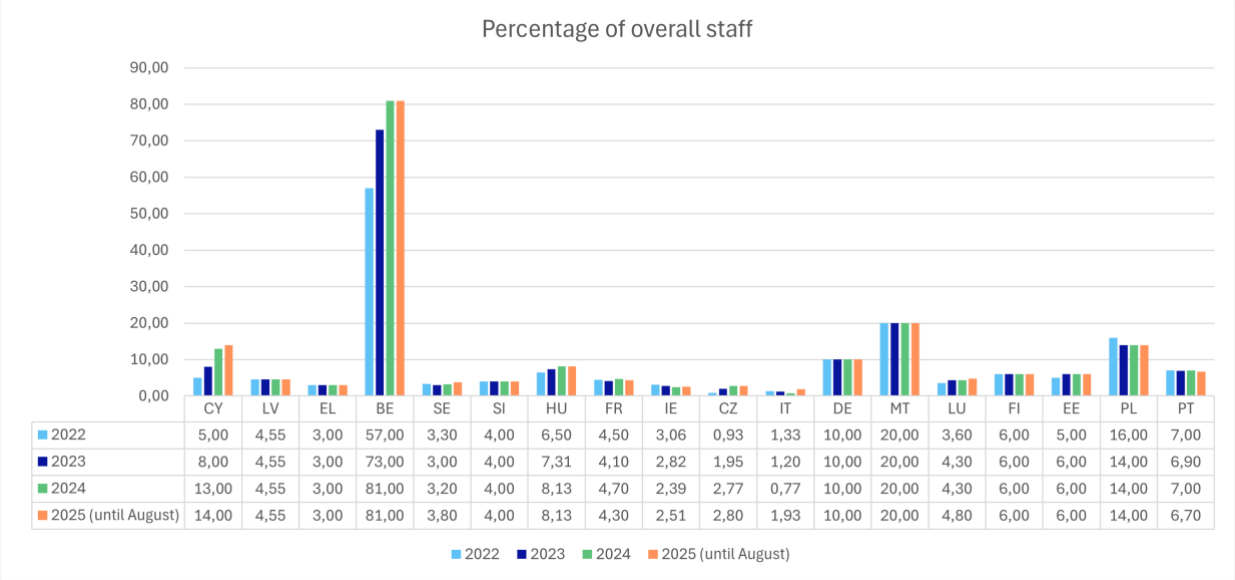
13.1 Please indicate the number of full-time equivalents working on the LED. Please provide data per year (from January 2022 to 31 August 2025). What percentage of overall staff does this represent (per year)?

94 The first graph below depicts the number of full-time equivalents (‘FTEs’) working on the LED, per year, for the reporting period[35].



	CY	LV	EL	BE	SE	SI	HU	FR	IE	ES	CZ	IT	DE	MT	LU	FI	BG	EE	PL	PT
2022	1,00	1,50	1,50	8,00	4,00	2,00	8,00	12,40	6,00	2,00	1,00	1,80	56,40	3,00	2,00	3,50	25,00	1,00	53,00	2,00
2023	2,00	1,50	1,50	10,00	4,00	2,00	9,00	11,80	6,00	2,00	2,00	1,80	58,60	3,00	2,50	3,50	25,00	2,00	53,00	2,00
2024	3,00	1,50	1,50	11,00	5,00	2,00	10,00	14,00	6,00	3,00	3,00	1,40	59,85	3,00	2,50	3,50	27,00	2,00	53,00	2,00
2025 (until August)	3,00	1,50	1,50	11,00	6,00	2,00	10,00	13,00	7,00	3,00	3,00	3,50	63,40	3,00	3,00	3,50	26,00	2,00	53,00	2,00

95 The graph below shows the percentage of overall staff working on the LED, per year, for the reporting period.[36]



	CY	LV	EL	BE	SE	SI	HU	FR	IE	CZ	IT	DE	MT	LU	FI	EE	PL	PT
2022	5,00	4,55	3,00	57,00	3,30	4,00	6,50	4,50	3,06	0,93	1,33	10,00	20,00	3,60	6,00	5,00	16,00	7,00
2023	8,00	4,55	3,00	73,00	3,00	4,00	7,31	4,10	2,82	1,95	1,20	10,00	20,00	4,30	6,00	6,00	14,00	6,90
2024	13,00	4,55	3,00	81,00	3,20	4,00	8,13	4,70	2,39	2,77	0,77	10,00	20,00	4,30	6,00	6,00	14,00	7,00
2025 (until August)	14,00	4,55	3,00	81,00	3,80	4,00	8,13	4,30	2,51	2,80	1,93	10,00	20,00	4,80	6,00	6,00	14,00	6,70

[35] The RO SA does not have full-time employees working only/exclusively on the LED.

[36] Please note that regarding Belgium, the police dedicated DPA in B is the Supervisory Body for Police Information (‘COC’). COC is a law enforcement dedicated DPA with a framework of 12 FTEs (Board of directors included); 10 of those are operational; 8 to 9 FTE fully deployable to exercise oversight and DPA duties on 178 local police forces; 1 federal police force with 52 entities; 1 passenger information unit; 1 general police inspectorate; besides being a LED -dedicated DPA, the COC has also other non DPA-related tasks.

13.2 How would you assess your DPA's resources for its work on the LED from a human and financial point of view?

96 Most SAs (17 SAs) reported that having no staff or no full-time staff is insufficient to ensure consistent and effective implementation and supervision of the LED, particularly given the high number of complaints and mandatory inspections, as well as the evolving needs related to the new EU databases and related audits (i.e. EES, ETIAS, ECRIS-TCN). They also pointed out the lack of appropriate IT tools and financial resources. Also, one SA indicated that more awareness-raising actions are needed. In one country, where courts and prosecutors also act as supervisory authorities for their subordinate units, supervisory tasks are carried out by Data Protection Officers. As a result, functions that should remain distinct, those of DPOs and those of DPAs are performed by the same person, limiting the effective use of human resources. In addition, an SA reported that although its resources have gradually increased, the allocation remains insufficient considering the complexity of supervision in law enforcement, the growing number of regulatory instruments and the constant development of new technologies.

13.3 Do you face any specific challenges when supervising competent authorities in terms of expertise (criminal law / new technologies) and IT resources?

97 The vast majority of SAs (20 SAs) reported having faced specific challenges when supervising competent authorities regarding expertise (criminal law and new technologies) and IT resources. In particular, most SAs stated that these challenges relate to inadequate IT resources (16 SAs) and insufficient expertise in technologies used in law enforcement (9 SAs). Several SAs (6 SAs) also noted insufficient expertise in the working methods and practices of law enforcement authorities, as well as in international cooperation in criminal matters (5 SAs). Several SAs mentioned challenges related to insufficient expertise in criminal law (5 SAs) and some (6 SAs) identified other challenges, as described below.

13.3.a.1 Insufficient expertise in criminal law - please provide more details and advise on what would assist to overcome these challenges:

98 4 SAs reported difficulties in effectively exercising their oversight functions in law enforcement due to insufficient expertise in criminal law and related procedural practices. Legal and structural limitations often restrict their ability to assess the operational relevance and proportionality of personal data processing activities carried out by law enforcement authorities. This lack of access to practical examples hinders the development of a comprehensive understanding of investigative methods, decision-making criteria and the interplay between data protection obligations and criminal procedure rules. The resulting knowledge gap is further exacerbated by the complexity of applying data protection principles within the framework of national criminal legislation, as well as by limited human and financial resources. To address these challenges, SAs emphasise the need for targeted training delivered by experts in criminal law and criminal procedure, cybersecurity and law enforcement technologies, the use of hypothetical case studies and simulations to build applied understanding, structured and non-operational cooperation with law enforcement bodies for experience exchange, the strengthening of technological and analytical competences and the allocation of adequate resources to support capacity-building efforts. These measures would enable supervisory authorities to exercise more informed, balanced and effective supervision of data processing activities in the criminal justice context.

13.3.a.2 Insufficient expertise in working methods and practices of law enforcement authorities - please provide more details and advise on what would assist to overcome these challenges:

99 Several SAs (5 SAs) reported that limited expertise in the operational methods and practices of law enforcement bodies continues to impede effective supervision under the LED. Difficulties in recruiting and retaining personnel with the necessary combination of legal, technical and practical knowledge, as well as restricted access to real investigative procedures and financial constraints, were identified as key factors. To address these challenges, SAs emphasised the need for strengthened cooperation and information exchange with law enforcement bodies, targeted and continuous training, recruitment or secondment of experts with relevant operational experience and adequate resources to build and sustain institutional expertise. These measures would enhance supervisory capacity and ensure more effective and consistent oversight in the law enforcement sector.

13.3.a.3 Insufficient expertise in international cooperation in criminal matters - please provide more details and advise on what would assist to overcome these challenges:

100 4 SAs reported that limited expertise in international cooperation in criminal matters hinders their ability to fully assess and supervise cross-border data transfers under the LED. Key challenges include restricted access to police procedures, difficulties in understanding how authorities cooperate with foreign partners and constraints related to human and financial resources. To address these limitations, authorities highlighted the need for targeted training, participation in exchange programmes and engagement in joint workshops with other supervisory authorities and relevant international organisations. These measures would strengthen institutional capacity and support effective oversight of cross-border law enforcement data processing.

13.3.a.4 Insufficient expertise in technologies used in the area of law enforcement - please provide more details and advise on what would assist to overcome these challenges:

101 8 SAs reported insufficient expertise in technologies used in the area of law enforcement. In particular, one SA stated that it is impossible to keep up with all the new technologies that multiple police forces are experimenting with or already using, as well as the lack of human resources and the inability to provide effective oversight, even by prosecutors or investigative judges. Another SA stated that accessing information and training specifically on the use of new technologies for law enforcement purposes can be challenging and that it would be beneficial to have specialised modules on emerging technologies and cross-disciplinary workshops bringing together legal, technical, and policy expertise. Several SAs noted insufficient in-depth training and certification mechanisms, as well as limited in-house expertise in certain advanced technologies used in law enforcement, such as data analytics, biometric identification systems and automated data exchange solutions. Rapid technological advances and the high demand for staff with advanced technical expertise further compound these challenges. Additionally, the lack of human and financial resources, as well as budgetary restrictions, are further obstacles in this regard.

13.3.a.5 Insufficient IT resources - please provide more details and advise on what would assist to overcome these challenges:

102 14 SAs reported insufficient IT resources. In particular, one SA stated that the challenge of insufficient IT resources can be addressed either by allocating more personnel or by increasing the efficiency of existing resources (i.e., if SAs were granted their own access to police IT systems or to test versions). Another SA stated that there could be more IT forensic capabilities, both in terms of technology and expertise. Most SAs indicate that the issue arises from an insufficient number of IT staff; some pointed to a lack of technical equipment, while others highlighted a lack of financial resources. To this end, one SA stated that increased investment in modern IT tools, cybersecurity infrastructure and analytical software is needed. A few SAs indicated difficulties in finding appropriate technical and legal expertise, and one SA suggested investment in digital training as a way forward.

13.3.a.6 Other - please provide more details and advise on what would assist to overcome these challenges:

103 6 SAs reported the following other challenges, namely one SA reported issues relating to big data and the need for data scientists, data engineers and similar roles. A few SAs pointed out the insufficient number of staff able to focus exclusively on LED issues. In one case, the SA stated that, given the broadening range of new technologies, there is a need to expand the experts' knowledge. Another SA identified the lack of knowledge of the national implementing law as the main challenge, while in one case, issues of scope were highlighted as challenges (i.e., the delineation between GDPR and LED, especially regarding reliance on LED in the context of enforcing a penalty or when processing falls outside the scope of EU law under Article 2(3)(a) LED or Article 2(2)(b) GDPR).

13.4 Have you used the EDPB Support Pool of Experts for LED related tasks?

104 No SA has used the EDPB Support Pool of Experts for LED-related tasks. Most SAs (26 SAs) stated there has not yet been a need to use it for LED-related tasks. One SA stated this was due to a lack of necessary knowledge of national legislation, while another indicated that an obstacle to using the EDPB expert pool is that, under its current national law, proceedings must be conducted in its national language.

14 Horizontal questions

14.1 Have you identified any significant problems regarding the transposition of the LED in your Member State that were not mentioned in the last review?

105 The vast majority of SAs (19 SAs) did not identify significant problems regarding the transposition of the LED in their Member State that were not mentioned in the previous review. However, the following SAs reported as follows.

106 The DE SA reported that the German Code of Criminal Procedure implements the LED for criminal investigations, but many legal norms predating the LED conflict with or do not align

with the LED and the GDPR. In particular, unclear boundaries remain regarding competent authorities, applicable laws, and the scope of the LED and the GDPR (i.e. in the issue of "judicial activity"). In addition, at regional level, LED-related data protection principles are insufficiently implemented in the Security and Public Order Act of Mecklenburg-Western Pomerania.

107 The BE SA faces significant issues with its indirect access system for citizens seeking access to personal data processed by law enforcement authorities under Article 17 LED, as the BE SA can only respond that "necessary verifications have been carried out" without providing any details. Under Article 42 of the Belgian law of 30 July on data protection, the BE SA cannot disclose or justify data processing decisions, although citizens may lodge an appeal. Following the CJEU judgement (C-333/22[37]) and the Advocate General's opinion, it was clarified that Belgium should allow direct access to individuals to data held by law enforcement authorities. However, in 2025, the Brussels Court of Appeal ruled that only the Belgian legislator (not the courts) may amend the law to implement Article 17 LED directly.

108 The SK SA noted that the current national data protection law, which covers both the GDPR and LED, is unclear and new separate laws are under preparation. The PL SA reported substantial shortcomings in the national implementation of the LED. It lacks enforcement tools, such as fines or reprimands (Article 57 LED). Article 4 LED is incorrectly implemented, Article 17 is not implemented at all, and the implementation of Article 45 LED raises serious questions. Also, outdated terminology in the implementing act and unclear DPO rules further weaken oversight and deprive citizens of effective safeguards and remedies.

109 The NL SA reported that the national implementation of the LED is complicated due to the broadly defined and overlapping purposes in the Dutch Criminal Data Act which divides personal data into numerous overlapping categories and more than 15 subcategories. The CZ SA noted that Article 10 LED is inadequately transposed into national law and that processing biometric data under Czech law should be subject to stricter conditions in line with the LED.

110 In Spain, the Basque SA noted that further regulations and clarification are needed regarding police video surveillance and biometric data processing under the LED. The IT SA reported that in December 2021, the amendment to Section 5(1) of the Legislative Decree entered into force, broadening the legal basis for data processing to include general administrative acts identifying the data and purposes of processing. However, the IT SA stated that it remains to be verified whether this additional source (i.e., a general administrative act) introduced by the amendment, effectively supports the LED's objectives. Furthermore, the IT SA stated that the secondary legislation required under Section 5(2) of the national law, intended to define key aspects such as data retention periods, access rights and conditions for exercising data subjects' rights, has not yet been adopted. A legislative amendment is now under discussion to repeal the provision requiring the adoption of such secondary regulation and to reorganise the regulatory framework for processing in criminal justice and police contexts. Lastly, the IT SA reported that it is not aware of a specific independent supervisory body overseeing LED compliance by judicial authorities when acting in their judicial capacity, despite requirements implied by Recital 80 LED and by analogy with Recital 20 GDPR and CJEU case-law (CJEU Joined cases C-313/23, C-316/23, C-332/23[38]).

[37] Judgment of 16 November2023, Ligue des droits humains (Vérification du traitement des données par l'autorité de contrôle), C-333/22, ECLI:EU:C:2023:874

[38] CJEU Joined cases C-313/23, C-316/23, C-332/23 Judgement of 30 April 2025, Inspektorat kam Visshia sadeben savet Case C-313/23 (Joined Cases C-313/23, C-316/23, C-332/23), ECLI:EU:C:2025:303

14.2 Have there been any amendments to your national law implementing the LED from January 2022 to 31 August 2025?

111 While 14 SAs did not report any amendments to their national laws implementing the LED concerning the reporting period, many SAs (11 SAs) reported the following amendments. In particular, between January 2022 and 31 August 2025, the following EU Member States introduced amendments to their national laws implementing the LED, although most changes were targeted rather than comprehensive.

112 In Lithuania, the Law on the Legal Protection of Personal Data Processed for Law Enforcement Purposes ('LLPPD') was amended in 2024, affecting numerous provisions. In Germany, at the federal level, the Anti-Money-Laundering Act was revised to include corrective powers and to provide the legal basis for the operation of the Financial Intelligence Unit, while regional amendments in Rhineland-Palatinate and Saarland in 2025 addressed data protection in penitentiaries and institutions for mentally ill offenders. Belgium adopted two laws in 2024 (i.e., on the digitalisation of justice and on establishing the missions of the ETIAS National Unit).

113 Greece modified several provisions of Law 4624/2019 implementing the LED with Law 5002/2024 and Latvia amended its LED-implementing law in 2024 and 2025 to incorporate references to additional EU directives. In Spain, a 2022 amendment to Organic Law 7/2021 transferred sanctioning powers for certain infractions from SAs to officials within the executive branch, while in Finland, individuals gained the right to complain to an administrative court if the SA failed to process a complaint or to provide an estimate of the time required to process it within three months.

114 The Netherlands lifted a pre-2016 exception for logging obligations in IT systems in 2024. Meanwhile, the CY SA reported that the amending Law 44(I)/2019 ensures that the LED is implemented in the territory of the UK Sovereign Bases Area (SBA) in Cyprus after Brexit, while Sweden considered expanding staff access authorisations. In Poland, the scope of data excluded from protection under the LED was expanded, while clarifications regarding data controllers in court ICT systems and oversight by the National Prosecutor were introduced.

115 Overall, while many amendments refined procedural or institutional aspects, few Member States undertook full legislative overhauls of their LED framework during the reporting period.

14.3 Is there anything else you would like to mention relevant for the LED evaluation that is not covered in this questionnaire?

116 While most SAs (21 SAs) did not refer to other elements that are relevant for the LED evaluation but were not covered in the questionnaire, the following five SAs states as follows. One SA reported the need to amend its national law, from an indirect access to a direct access system. Another SA highlighted the need for EDPB guidelines on the further use of personal data processed under the LED for research purposes. One SA indicated issues regarding the provision of statistics for this report, as its data collection mechanism also includes investigations into processing covered by different legal regimes, while its IT tools for complaints management do not allow identification of LED-related complaints. Another SA reported that it is complicated to apply both the LED and the GDPR in the judicial field, as the traditional distinction between controllers and processors is not straightforward in this context, due to the specificities of the judicial organisation. Another SA reported the need to enhance

the status and role of the Data Protection Officer (DPO); maintain the independent status of the supervisory authority; clarify whether all supervisory authorities designated are competent to carry out the tasks assigned to them and exercise their powers; whether the Member State ensures the right to an effective judicial remedy against decisions of the supervisory authority, the controller or the processor and the right to compensation; and whether the Member State has effectively adopted rules establishing penalties for infringements of LED provisions. In addition, the judicial supervisory authorities of that SA reported the need to further harmonise the definition of high-risk operations and the criteria for their identification in the justice and law enforcement area, as differences in interpretation hinder the uniform application of Article 28(1) LED in practice; that there are no dedicated tools supporting risk analysis in the context of the LED, unlike those available in the GDPR and that developing such tools (e.g. risk matrices, DPIA templates) could significantly improve the work of data controllers in the operational sector; challenges related to the interoperability of IT systems used by competent authorities, particularly in ensuring compliance with the principles of data minimisation, purpose limitation and retention and the need to strengthen the competences of the DPO in the operational sector through dedicated training that takes into account the specificities of data processing as part of investigative, preventive and repressive activities.

14.4 Please add the topics and/or policy messages you would like to include in the EDPB report. Elaborate the reasons why, in your view, such topics should be included.

117 Several SAs pointed out that further clarification on the LED provisions is needed (5 SAs). In particular on the scope of application of the LED, as in some cases it remains unclear whether the Directive applies (i.e. following Art. 1(1) LED the directive applies to “the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety”). The wording that uses “including” suggests that the “safeguarding” and “prevention” should, in their view, actually be read exclusively in the context of “criminal proceedings”. If a competent authority can process data not only to investigate criminal acts (e.g. a burglary) but also to prevent risks (e.g. saving a suicidal person or regulating a car crash) it is uncertain whether both processing operations should be subject to regulations based on the LED. Nonetheless, in Saarland (and Germany in general) the laws lack a distinction in this regard / regarding the scope of the LED and anchor the LED-classification to the acting authority and not to the processing operation; or the concept of ‘purposes’ which may be generally formulated in transposing laws and thus lead to overlaps, also due to the complex subdivision of data categories). Furthermore, a few SAs indicated that clarification would be helpful regarding the boundaries between the LED and the GDPR in the context of processing operations by courts and administrative authorities conducted outside the administration of justice. In terms of issues pertaining to the interplay between the LED and the GDPR, it was pointed out that clarification would be welcomed on the issue of joint responsibility (Article 21 LED in connection with Article 26 GDPR) in the context of partnerships between law enforcement agencies and other bodies (sometimes also private parties), for joint purposes that fall within the scope of the GDPR and are closely related to the purposes of the LED. Also, taking into account the growing number of EU Large-Scale IT systems in Europe (both at EU and national levels), as well as the question of interoperability of those information systems and their often twofold processing purposes (i.e., relating both to border and immigration control and to law enforcement purposes), clarification and guidance would be helpful on the interplay between the LED, the GDPR and such sector-

specific legislation, as well as with other new regulations (such as the AI Act) or other initiatives, such as the work of the high level expert group on access to data by law enforcement authorities.

118 In addition, some SAs indicated that clarification should be sought on issues related to the inconsistency in national implementation of the LED, such as the interpretation of the SA's competence as provided in Article 45(2) LED (i.e. regarding the concept of "judicial authority in the exercise of its judicial functions"). Furthermore, an SA pointed out that further clarity is needed regarding administrative fines and the SAs' corrective powers, as there appears to be a substantial discrepancy in the maximum level of penalties between the GDPR provisions and those of the LED, as transposed by national laws. Similarly, another SA highlighted the need to clarify the scope of the effective investigative and corrective powers set out in Article 47(1) and (2) of the LED. Furthermore, an SA indicated a possible discrepancy regarding the exercise of rights by the data subject and verification by the SA, as provided in Article 17(3) LED in conjunction with the provisions on lodging a complaint with an SA, as provided in Article 52 LED, as Article 17(3) LED allows national legislators to regulate that SAs may only inform the data subject that all necessary verifications or a review have taken place and disclosure of the personal data concerned may also be excluded, although this does not apply to provisions relating to complaints under Article 52 LED. This could lead to situations where public authorities raise the same interests as in Article 15(1) LED (e.g. the prejudicing of prevention, detection, investigation or prosecution of criminal offences) but the SA would not be able to consider these interests when issuing its final decision. It was also noted that greater discretion is needed in handling complaints. In addition, the relationship between complaints and indirect access requests should be clarified (i.e., the issue on whether indirect access requests are a sub-category of complaints, because the underlying processing must be verified in both cases according to Art. 46(1)(g) LED).

119 In addition to providing guidance, some SAs indicated that the role of DPOs in the operational sector should be strengthened, as DPOs carry out advisory and supervisory functions within law enforcement and judicial authorities but their effective performance of their duties may be impeded by limited access to operational information and insufficient dedicated training. Therefore, cooperation between DPOs of competent authorities and supervisory authorities should be further encouraged. A few SAs highlighted that cross-border cooperation among law enforcement authorities requires technological tools and IT systems that ensure compliance with data protection rules. One SA states that risk assessment and DPIA mechanisms in the operational sector should be enhanced, as currently, there is a lack of analytical tools tailored to the operational context of law enforcement authorities. Furthermore, the existence and promotion of analytical tools tailored to the operational context of law enforcement authorities would facilitate risk assessment and DPIA mechanisms in the operational sector. In terms of resources, the majority of SAs indicated that current human resources are insufficient and that additional resources are needed. One SA specified that additional resources are needed in particular in relation to complaints handling, where the SAs would also benefit from greater discretion. Also, it was mentioned that targeted and systematic training, as well as awareness-raising activities are required.