Contribution ID: 4333ae96-791f-46b0-9c9f-429a6ff1a852
Date: 15/12/2025 13:46:30

Report on the application of the LED under Article 62 LED
Questions to Data Protection Authorities/the European Data Protection Board (2025)

Fields marked with * are mandatory.

Background

The Data Protection Law Enforcement Directive (LED)[1] applies to domestic and cross-border processing of personal data by competent authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offences and executing criminal penalties, including safeguarding against and preventing threats to public security. The LED takes a comprehensive approach to data protection in the field of law enforcement, including by regulating 'domestic' processing.

In 2022, the European Data Protection Board provided a consolidated contribution[2] of the individual replies of the DPAs to the questionnaire circulated in preparation of the 2022 Commission's first report. Following the Commission's presentation to the European Parliament and to the Council of the first report on the evaluation and review of the Directive in 2022[3], it is required to present a report every four years thereafter[4]. The Commission will present the second report in May 2026. Following the review the Commission shall, if necessary, submit appropriate proposals for amendments, in particular taking account of developments in information technology and in the light of the state of progress in the information society[5].

The LED stipulates that the Commission shall take into account the positions and findings of the European Parliament, of the Council and of other relevant bodies or sources[6]. The Commission may also request information from Member States and supervisory authorities. The Commission intends to consult Member States through the Council Working party on Data Protection. The European Union Agency for Fundamental Rights (FRA), is also conducting research based on interviews with competent authorities/prosecutors and Data Protection Authorities on the practical implementation of the LED.

For the purpose of the evaluation and review of the Directive, the Commission shall in particular examine the application and functioning of the LED provisions on international data transfers[7]. This questionnaire also

seeks to cover other aspects with particular relevance for the supervisory authorities, such as the exercise of their tasks and powers and their cooperation with each other, as well as the consistent application of the LED in the EU.

As this questionnaire intends to contribute to evaluating the LED, in your replies please provide information which falls under the scope of the LED. The reporting period covers the period from January 2022 to the 31 of August 2025. Please note that the European Commission intends to send out a version of this questionnaire on a yearly basis. Future versions will be aligned to the extent possible to the annual questionnaire on the GDPR.

The Commission would be grateful to receive the **individual replies to this questionnaire in its online form in English**, and the EDPB contribution to the LED review by 16 January 2026. In order for the EDPB to compile its contribution to the LED review, individual DPA replies should be submitted by 15 October 2025 eob.

Please note that your replies may be made public or may be disclosed in response to access to documents requests in accordance with Regulation (EC) No 1049/2001.

When there are several DPAs in your Member State, please provide a consolidated reply at national level.

When replying, please take into account that the questions below concern the period from January 2022 to 31 August 2025.

Following the input from other stakeholders, it is not excluded that the Commission might have additional questions at a later stage.

Deadline of submissions of the answers to the questions by DPAs: **15 October 2025 eob.**

---

[1] Directive (EU) 2016/680 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.

[2] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

[3] Communication from the Commission to the European Parliament and the Council - First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), 25.7.2022 COM(2022) 364 final. Individual replies from data protection supervisory authorities to the European Commission's first evaluation of the LED in 2022 can be found here.

[4] Article 62(1) LED

[5] Article 62(5) LED.

[6] Article 62(4) LED.

[7] Article 62(2) LED.

Information:

Please save your submission ID (by either downloading the PDF version of the submission or by copying it after the submission) in order to be able to later amend your submission.
If you would like to work on a submission before finalising it, please use the "Save as draft" button on the right-side panel of the published survey tab. You will be able to continue working on the submission with the given draft link. If you need to change a submission, please go to Edit contribution. You will find all the required information on the Help page for participants.

Questionnaire

We kindly ask the countries that have more than one SA to send us one consolidated reply.

* Please select your SA:

Poland

Please describe your role and function in your DPA.
(*Ideally the person answering this questionnaire works on the LED on a regular basis*).

The national contribution was compiled by the Chief Coordinator for EU Large Scale IT Systems in Personal Data Protection Office (UODO), based on material received from the relevant departments of the Office and from the Presidents of the Courts and Prosecutors, who act as supervisory authorities for their subordinate units. In some cases, questionnaires from courts and prosecutors' offices were filled in by the Data Protection Officers. It should be noted that 80 supervisory authorities participated in the evaluation, which means that not all authorities entitled to participate in the evaluation provided their information.

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?

- ○ Yes
- ◉ No

2 Exercise of data subjects' rights through the DPA

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

- ○ Yes
- ◉ No

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?

- ○ Yes
- ◉ No

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?

Polish law implementing the Law Enforcement Directive (LED) grants the President of the Personal Data Protection Office the possibility to establish a list of processing operations subject to prior consultation. To date, the President of the Office has not exercised this power. Other supervisory authorities, competent for courts and public prosecutors, are not empowered to perform this task.

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?

Pursuant to Art. 5(1)(12) of the Act implementing LED, issuing opinions on draft acts and regulations on matters concerning the protection of personal data processed for the purposes of the identification, prevention, detection and combating of criminal offences, including threats to security and public order, as well as executing pretrial detention, penalties, fines and coercive measures resulting in the deprivation of liberty, is the sole responsibility of the President of the Personal Data Protection Office, and not of other supervisory authorities competent for courts and prosecutors. The President of the Personal Data Protection Office was consulted during the reporting period, but only to a limited extent. Although competent ministers often submit draft legislation to the President of the Personal Data Protection Office in accordance with the Rules of Procedure of the Council of Ministers, some authorities disregard this obligation and fail to communicate important drafts concerning the processing of personal data. Such practice not only contravenes the applicable regulations, but also deprives the drafters of the possibility to obtain expert support from the supervisory authority at an early stage of the legislative process. In many cases, draft laws and regulations that were not consulted with the President of the Personal Data Protection Office at an earlier stage are submitted to the Office later – via the Government Legislation Centre or, in the case of laws, directly from Parliament – with a request for an opinion or position. Some of the opinions were also prepared by the President of the Personal Data Protection Office ex officio – as a result of independent monitoring of the legislative process with regard to draft regulations that were not submitted to him for review in any way, but which nevertheless concerned the protection of personal data.

3.4 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.)?

As part of the consultations referred to in Art. 28(2) LED, the President of the Personal Data Protection Office issued opinions on draft legal acts concerning, among other things: 1. Defining the tasks and responsibilities of public authorities in personal data processing, including precisely determining the roles of entities performing specific processing operations. 2. Sharing and transferring data between authorities within the scope of their statutory powers, including data flows in preparatory, criminal, and misdemeanor proceedings. 3. Processing of special categories of data, including data derived from court judgments or relating to prohibited acts. 4. The scope of data processed in ICT systems supporting the activities of courts, public prosecutors' offices, and other public authorities, including in court proceedings, preparatory proceedings, and within information portals. 5. Compliance of the proposed regulations with the principles of personal data processing, in particular the principles of data minimization, integrity, and confidentiality. 6. Poland's participation in large-scale EU systems and the related obligations of national authorities. 7. The processes of serving court documents and submitting documents in criminal and misdemeanor proceedings via information portals, and securing personal data in this process. 8. Assessment of risks to the rights and freedoms of data subjects resulting from proposed legislative solutions and the model of data processing in administration and the justice system. 9. Processing by the police of fingerprints and facial images of persons who are not citizens of the Republic of Poland. One supervisory authority competent for courts indicated that it had been consulted on the changes made to the processing of personal data in the Law of 27 July 2001 on the organisation of common courts.

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?

- (●) Yes
- ( ) No

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?

	2022	2023	2024	2025 (until August)
Number of notifications (numbers only)	(UODO) 197+13=210	195+20=215	234+26=260	116+35=151
Percentage of measures advised or ordered	16%	26%	25%	26%

5 International transfers

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

- ○ Yes
- ◉ No

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

- ○ Yes
- ◉ No

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?

- ○ Yes
- ◉ No

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?

- ○ Yes
- ◉ No

5.4.b What prevented the carrying out of such activities to promote awareness?

Neither the Office nor other supervisory authorities have noted any cases requiring action to promote awareness among controllers/processors (in particular) with regard to their obligations under Chapter V of the les. Some supervisory authorities have pointed to a "lack of appropriate regulations." One supervisory authority indicated that such training is provided by external companies.

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?

No, we haven't. Neither the Office nor other supervisory authorities have recorded any cases requiring such action. One supervisory authority pointed to the lack of direct cooperation with law enforcement authorities and, consequently, the lack of competence in this area. One district prosecutor's office indicated that it was not competent to take action against law enforcement authorities.

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?

No, we haven't.

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?

No, we haven't.

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?

No such cases have been reported. The act implementing the LED regulates only the cooperation of the President of the Personal Data Protection Office with supervisory authorities in other European Union countries. Cooperation with other authorities supervising the processing of personal data as part of proceedings conducted by courts and tribunals, as well as with supervisory authorities within the meaning of Art. 51 of Regulation 2016/679, is governed by the Law on the Organisation of Common Courts. Under its provisions, judicial supervisory authorities share information and provide mutual assistance to ensure the consistent application of the Act implementing the LED. A similar mechanism exists for supervisory authorities in the public prosecutor's office, based on the Act on the Public Prosecutor's Office. Competent authorities are expected to cooperate with each other and with supervisory authorities overseeing personal data processing in judicial proceedings, sharing information and providing mutual assistance to ensure consistent application of the provisions of the Act implementing the LED.

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?

- (●) Yes
- ( ) No

6.1.a Please list them:

UODO's Activities: Newsletters: Notification of the appointment of the DPO or his deputy must be sent on the appropriate form (No 3/2022), Initiative to develop codes of conduct for courts (No 7/2022), Notifications of the DPO or its deputy should be sent in electronic form (No 7/2022), Some of the provisions of the law implementing LED concerning the DPO need to be amended (No 8/2022), There will be changes to the provisions of the Act implementing the LED relating to the DPO (No 10/2022), The concept of DBN in the Act implementing the LED (No 3/2023), Guide to the rights of persons in SIS (No 7-8/2023), Guidelines on the use of facial recognition technologies in law enforcement (No 2/2024), Judgment on the storage of biometric data (CJEU C 118/22) (No 3/2024), European Data Protection Supervisor assesses the privacy impact of the Regulation to fight migrant smuggling and trafficking in human beings (No 3/2024), Being closer to a citizen cannot be an empty slogan – an interview with Konrad Komornicki, Deputy President of UODO on, among others, the implementation of LED in Poland (No 4/2024), Schengen evaluation mechanism (No 4/2024), Clear procedures allow for action within the limits of the law – interview with Agnieszka Grzelak, Deputy President of UODO on the implementation of LED in Poland (No 5/2024), Amendments to the Act on counteracting threats of sexual crime and protection of minors needed (No 9/2024), Emergency number of the municipal guard – implementation of the information obligation (No 9/2024), Access to data for effective enforcement (No 11 /2024), Fundamental Rights Agency's Guide to the Rights of Persons in Eurodac (No 12/2024), Schengen Recommendations for Poland in the area of personal data protection (No 2/2025), Data on the implementation of data subjects' rights in Schengen (No 4/2025), Designation of the DPO under the law implementing LED - (special edition May 2025), EU Large-Scale Information Systems under supervision (No 6/2025), What is a digital footprint and how to manage it (No 6/2025), Public communication as an exceptional form of notification of a personal data breach to individuals (7-8/2025). Press Releases: Comments on the amendments to the Criminal Code and operational control by the Police; on the draft Cybersecurity Strategy; and on the ECtHR judgment concerning surveillance in Poland. Materials on UODO's website: Information on the appointment of DPOs in courts; guidelines on DPO designation, cancellation, or change under the Act implementing the LED; guidance on breach notification under the same Act. Lectures: Four lectures delivered to the Police and Border Guard on the LED, addressing topics such as data protection breaches, coordinated supervision, and EU data protection standards (2024–2025). Answering to questions from the DPOs: Clarifications on the use of monitoring by municipal guards; recording of images by fire brigade cameras; and the obligation to appoint a DPO for data processing related to crime prevention. Helpline: UODO experts provide advice via the helpline, including on issues related to fulfilling the obligations of controllers and processors under the LED. Activities of Other Supervisory Authorities competent for courts and prosecutors' offices: Letters, Guidelines, Recommendations: Reminders on obligations under the Act implementing LED, including breach notification, record-keeping, and DPO involvement; recommendations on remedying irregularities, data processing agreements, and IT access; guidelines on the role of the deputy DPO and related duties; letters requesting adaptation of processing operations to provisions. Internal Acts and Procedures: Updated Data Protection Policies and IT System Management Instructions; ordinances on the use of portable devices and data carriers; new work regulations; procedures for data breach and incident management; local data protection policies reflecting obligations under LED. Trainings: Introductory, periodic, and thematic training for prosecutors, administrative staff, and trainees; SIS access and refresher training; internal and external seminars, workshops, and self-study materials; consultations aimed at harmonising practices. Educational Materials and Tools: Checklist "before leaving the unit" and data protection knowledge test; templates for data processing agreements; processor assessment forms and related documentation. Ongoing Communication: Regular reminders on security rules (encryption, remote work, breach reporting, clean desk, screen protection); updates on legislative changes; meetings and consultations with data controllers. Additional Remarks: In some cases, the division of responsibilities for educational initiatives between data controllers, data protection officers, and supervisory authorities was unclear. In some cases, authorities reported that no action had been taken or indicated "not applicable."

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?

1) Under Art. 1(3) of the Implementing Act, the Act does not regulate supervision over the processing of personal data by courts and prosecutors. It does not apply to case-file documentation or registers maintained under procedural codes or specific laws. In practice, the processing of personal data by courts and prosecutors for the purposes of preventing and combating crime is governed solely by sectoral rules. Some authorities consider that confidentiality provisions in procedural law are sufficient and that no further changes are needed. However UODO and several judicial SAs stress that criminal procedure lacks safeguards required by LED, such as the rights to information, access, rectification, erasure, restriction, complaint to SA and an effective judicial remedy. This gap also undermines the application of Art. 18 LED. Authorities differ in interpretation: some question such a broad exemption, while others argue that criminal files do not constitute 'filing system' and are therefore outside the LED's scope. UODO disagrees, emphasising that LED covers any processing of personal data, regardless of its form. 2) The absence of a legal definition of "judicial capacity" raises interpretative doubts. Technical and administrative activities (e.g. correspondence, file storage, transport) are often treated as falling within "judicial capacity", thereby excluding them from data protection supervision. UODO has repeatedly stressed that such activities do not constitute the exercise of justice and should be subject to independent supervision under the GDPR/LED. Court practice varies: appellate courts tend to favour broad exclusions from the LED, while regional and district courts—directly involved in sentencing or pre-trial detention—apply narrower interpretations. This inconsistency weakens legal certainty. Consequently, in one case concerning a complaint against UODO's decision, the DPA requested the Supreme Administrative Court to refer a preliminary question to the CJEU on the interpretation of this concept. What is more, according to the Polish Constitution, judicial authorities include only courts. The Public Prosecutor's Office is not another independent judicial authority within the meaning of Article 45(2) LED; in particular, it does not act in judicial capacity. Therefore, in the opinion of UODO, the exemptions under Art. 45 LED should not apply to prosecutors. 3) Supervision in courts and prosecutors' offices follows a hierarchical model in which court presidents or senior prosecutors oversee lower levels. While judicial independence provides some autonomy, the strict hierarchy within the prosecution raises doubts about compliance with the LED's independence criteria. It should also be noted that, in light of the Act on the Organisation of Common Courts (and, analogously, other acts regulating the functioning of courts), the National Council of the Judiciary is the highest supervisory authority (e.g., in the case of supervision of the personal processing by court of appeal or the Supreme Court). The independence of the National Council of the Judiciary in its current form has been questioned repeatedly in the case law of the CJEU (C-585/18, C-624/18, C-625/18, C-791/19, C-487/19) and the ECHR (43447/19, 49868/19, 57511/19, 1469 /20, 50849/21) and there are very serious doubts as to whether this body meets the criteria required by Art. 45 LED. The judgments of the European courts indicate that this body does not meet these criteria due to shortcomings in terms of independence. 4) Although the Act on the Organisation of Common Courts refers to powers and tasks under the Act implementing the LED, most judicial authorities argue that, due to the exemptions in Article 3, courts have no direct obligations under it. Under a similar model in the Act on the Public Prosecutor's Office, prosecutors recognise their competence to supervise data processing in accordance with the LED. 5) Many questionnaires were completed by DPOs on behalf of supervisory authorities, raising doubts whether supervision under Art. 45 LED may be carried out by DPOs rather than by independent supervisory bodies, given the current hierarchical model. 6) Although Art. 45 LED requires that each supervisory authority perform its tasks and exercise its powers, several competences rest solely with the UODO. These include: raising public awareness, advising national institutions during legislation process, assisting data subjects, conducting prior consultations, and participating in the EDPB. Authorities competent for courts and prosecutors lack advisory powers to issue recommendations or consult national institutions or task of preparing annual activity reports. This fragmented system means that judicial and prosecutorial bodies do not perform all tasks provided for in Articles 46–49 LED, resulting in an uneven standard of supervision and limited protection of individuals' data-processing rights within the justice sector.

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?

The Act implementing the LED lays down the way of exercising supervision over the protection of personal data processed by the competent authorities for the purposes of the identification, prevention, detection and combating of criminal offences, including threats to security and public order, as well as executing pretrial detention, penalties, fines and coercive measures resulting in the deprivation of liberty. However personal data processed by public prosecutor's office and courts are excluded from this scope. In the opinion of the President of the Personal Data Protection Office, the Public Prosecutor's Office is neither an independent body nor a judicial authority within the meaning of Article 45(2) LED. Therefore, it should not benefit from the exemptions provided for in that provision. It should be emphasised that the exclusion established by the Act is not limited to activities performed within 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?

- ○ Yes
- ◉ No

8.1.a Please explain. (For example, do you have sufficient access to competent authorities' personal data that is under investigation?)

For the purposes of: - monitoring and enforcing the application of the provisions of the implementing act, - handling and investigating complaints lodged by data subjects whose personal data are processed unlawfully, - inspecting the compliance of the processing of personal data with the provisions of the implementing Act, - conduct proceedings on the application of the implementing Act, including on the basis of information received from another public authority; an employee of the Personal Data Protection Office authorised by the President of the Office have the right to inspect the data filing system subject to the inspection and other documents directly related to the subject of the inspection in the presence of an authorised representative of the competent authority where the inspection is conducted. In addition, the President of the UODO may directly request the Data Protection Officer to carry out a check on application of Act implementing the LED, indicating the scope and timing of that check. The DPO, through the controller, shall submit to the President of the Office a report on the check performed. The President of the Office considers the above powers to be, in principle, effective. So far, there has been no situation in which lack of access to data has prevented the conduct of proceedings. However, in the case of complaints by data subjects, the Act implementing the LED provides for the application of the provisions of the Code of Administrative Procedure. This creates important practical constraints: The Code of Administrative Procedure governs the relationship between the public authority and the subject of the proceedings, whereas in the complaint proceedings conducted by the President of the UODO there are two opposing parties. As a result, the supervisory authority is often not in a position to take adequate and timely action to ensure that individuals can effectively exercise their rights under the LED or to remedy the breach without undue delay. The supervisory authorities of the courts that the following factors have a positive impact on the effectiveness of the proceedings conducted: - The ability to request information and documentation from data controllers and processors; - Inspection powers, including the ability to conduct activities at the entity's premises and remotely; - The ability to issue recommendations, orders, and administrative decisions, including those requiring the adaptation of processing operations to applicable regulations; - The ability to cooperate with other authorities, including law enforcement agencies and courts, to the extent necessary to perform their tasks. At the same time, judicial SAs recognize areas for further improvement, such as streamlining information exchange between authorities, increasing human resources, and developing analytical tools to support the identification of risks in data processing. The supervisory authorities of the public prosecutor’s offices have assessed their investigative powers as effective, as they have the power to: - order the controller or processor or their representatives to provide any information necessary for the performance of the tasks of that authority; - to obtain from the controller and the processor access to any personal data and information necessary for the performance of its tasks by the supervisory authority; - accessing the premises of the controller and the processor, including data processing equipment and means; - ask the data protection officer directly to check the application of the provisions of the implementing act by the controller who appointed him, indicating the scope and time limit for this check.

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

- (●) Yes
- ( ) No

8.2.a Please clarify:

The experience of UODO shows that conducting complaint proceedings under the provisions of the Code of Administrative Procedure is not conducive to amicable settlement of cases. On the contrary, the adversarial nature of such proceedings—where parties with opposing interests engage in a formal dispute—makes it difficult to establish the facts and to swiftly ensure compliance with the LED provisions. In practice, the parties tend to focus on defending their own interests and seeking a favourable outcome, rather than on restoring lawful data processing. In the opinion of PL SA, the primary objective of the procedure should not be the “resolution of a dispute” in the sense of determining which party is right, but rather the prompt rectification of the infringement and the restoration of compliance with LED requirements. Therefore, PL SA calls for the introduction of mechanisms that would allow the data protection authority to operate in a non-administrative, more conciliatory and pragmatic manner. This would enable the authority not only to assist data subjects in exercising their rights, but also to advise them—and, where appropriate, controllers—on concrete steps to prevent or remedy breaches as quickly as possible.

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

	2022	2023	2024	2025 (Until August)
On your own initiative (numbers only)	(UODO) 2 + 96 = 98	16 + 97 = 113	24 + 128 = 152	20 + 77 = 97
On the basis of complaints (numbers only)	(UODO) 33 + 7= 40	35 + 12 = 47	14 + 9 = 23	10 + 5 = 15

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

- (●) Yes
- ( ) No

8.4.a Please specify which ones:

> The experience of the authority shows that conducting complaint proceedings under the Code of Administrative Procedure is not conducive to swift and amicable clarification of cases. The formal nature of the procedure and the adversarial position of the parties result in the focus being placed on defending individual interests rather than ensuring the lawfulness of data processing. This often hinders the collection of complete and reliable information necessary to establish the facts of the case. Additional difficulties arise when data controllers fail to notify the authority of a personal data breach within 72 hours of its identification, invoking ongoing operational activities or the need to maintain the confidentiality of the incident. Although the notification obligation should be fulfilled as soon as the obstacles cease to exist, together with an explanation of the reasons for the delay, in practice the Office often receives such notifications with significant delay - or, in some cases, not at all. This results in substantial limitations on access to data and information necessary to conduct investigations and fully assess the scope and impact of infringements.

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?

- ( ) Yes
- (●) No

8.6 Do you consider your corrective powers effective?

- ( ) Yes
- (●) No

8.6.a Please clarify:

> The President of the UODO holds all the corrective powers listed in the LED. The supervisory authorities of the Public Prosecutor's Office and courts have the power to: 1. issue warnings to controller or processor regarding the possibility that processing operations are likely to infringe provisions of the act implementing LED. 2. issue reprimands to controller or processor where processing operations have infringed provisions of act implementing LED. 3. request controller or processor to bring data processing operations into compliance with the provisions of the implementing act. However, despite the direct reference in the Act on the organisation of common courts to corrective powers concerning infringements of the provisions of the Act implementing the LED, most supervisory authorities competent for courts consider that their powers do not include supervision of data processing under this regime. Therefore, the practical application of these provisions should be assessed negatively - or as largely non-existent. In addition, the supervisory authorities of courts and prosecutor's offices do not have the to impose a temporary or definitive limitation, including a ban, on processing (art. 47(2)(c) LED).

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

- (●) Yes
- ( ) No

8.7.a Please clarify:

In this evaluation cycle, the supervisory authorities competent for courts and prosecutors, which did not participate in the previous evaluation, were also invited. This allowed to obtain a broader perspective and compare the scope of their corrective powers with the competences of the President of the UODO.

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[1] and VIS[2]?

[1] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).

[2] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).

47(2)(a)	**2022**	**2023**	**2024**	**2025 (until August)**
SIS	0	0	0	0
VIS	0	0	0	0
Other	5	3	3	2

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[1] and VIS[2]?

[1] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).

[2] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).

47(2)(b)	**2022**	**2023**	**2024**	**2025 (until August)**
SIS (please also specify whether you ordered the controller to provide access/delete data)	0	0	0	0
VIS (please also specify whether you ordered the controller to provide access/delete data)	0	0	0	0
Other (please also specify whether you ordered the controller to provide access /delete data)	(UODO) 6+4=10	3+8=11	2+27=29	0+27=27

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[1] and VIS[2]?

[1] Council Decision 2007/533/JHA, Regulation (EU) 2018/1860, Regulation (EU) 2018/1861, Regulation (EU) 2018/1862 (as of March 2023).

[2] Council Decision 2008/633/JHA, Regulation (EC) 767/2008 (as of March 2023).

47(2)(c)	**2022**	**2023**	**2024**	**2025 (until August)**
SIS	0	0	0	0
VIS	0	0	0	0
Other	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?

- ○ Yes
- ◉ No

8.11.a How did you follow up?

The President of the UODO initiated enforcement proceedings in three cases. In one case, the authority initiated administrative proceedings in connection with an infringement of the law, which will be concluded with an administrative decision. In the course of inspections carried out by the President of the UODO, it was not necessary for the authority to apply corrective measures, as no irregularities were identified. In cases where any doubts arose (at the stage of correspondence), the inspected entities took prompt actions to address them and to improve their data protection practices. In complaint proceedings, the decisions of the President of the UODO ordering compliance with the provisions (e.g. through the deletion of personal data by the police, or by requiring a telecommunications operator or an insurance company to disclose personal data to the municipal guard) were mostly appealed to the Voivodship Administrative Court in Warsaw. These decisions are not final. In some cases, cassation appeals were lodged with the Supreme Administrative Court against the judgments of the Voivodship Administrative Court.

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

The President of the Personal Data Protection Office, as well as some of the supervisory authorities competent for public prosecutors' offices, have exercised their corrective powers. The remaining supervisory authorities competent for prosecutors' offices did not indicate the reasons for not exercising these powers. With regard to the supervisory authorities competent for courts, it was emphasised that, in practice, they consider themselves unable to exercise corrective powers in relation to the entities under their supervision, as they are excluded from the scope of application of the LED under Article 3 of the act implementing the LED. However, 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?

- ○ Yes
- ◉ No

8.14 Total amount of fines imposed (from January 2022 until August 2025, numbers only, in €)

8.15 Amount of the highest fine imposed (from January 2022 until August 2025, numbers only, in €)

8.16 Average amount of the fines imposed (from January 2022 until August 2025, numbers only, 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?

- ○ Yes
- ◉ No

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

- ○ Yes
- ◉ No

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.

There were no such cases.

10 Cooperation

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

	2022	2023	2024	2025 (until August)
Launched	0	0	0	0
Received	1	2	1	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.)

The President of the UODO was requested to carry out an inspection to verify the validity and justification of an alert entered in the Schengen Information System (SIS), pursuant to Article 46(1) of Regulation (EC) No 1987 /2006 and Article 71 of Regulation (EU) 2018/1862 of the European Parliament and of the Council. The request also concerned information on whether the President of the UODO had received a complaint relating to a request for the deletion of personal data from the SIS.

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

- (●) Yes
- ( ) No

10.2.a Please describe them as well as possible solutions

The authority that requested information on whether the President of the UODO had received a complaint concerning a request for the deletion of personal data from the SIS did not refer to Art. 50 LED. The query was submitted through the IMI system under the notification 'Article 61 – Voluntary Mutual Assistance'. Therefore, doubts arise as to whether these requests should be classified as requests under Art. 50 LED.

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

During the period covered by the evaluation, the guidelines of the EDPB on the application of the provisions of LED were not directly used. As indicated by some supervisory authorities competent for courts, in practice, the activities of the data protection authority and personal data controllers were primarily based on national legislation, the positions of the President of the Personal Data Protection Office, and the well-established interpretative practice developed through previous proceedings and consultations. Nevertheless, the EDPB Guidelines remain an important point of reference for harmonising approaches to personal data protection within the European Union, particularly in areas such as Data Protection Impact Assessments (DPIAs), breach notification, and the qualification of the roles of processors.

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

In order to ensure the consistent and effective application of LED across the Member States, future guidelines of the EDPB should address the following thematic areas: – the delineation of the respective scopes of the LED and the GDPR, in particular with regard to processing operations carried out by courts outside the judicial capacity, and by administrative authorities performing mixed tasks; – data protection impact assessments (DPIAs) in the justice and law enforcement sectors, taking into account the specific characteristics of high-risk operations such as the processing of biometric or sensitive data, and profiling; – cooperation mechanisms between supervisory authorities and data protection officers, in the context of prior consultations and ongoing advisory functions, in accordance with Article 28 LED; – transfers of personal data to third countries and international organisations, including practical mechanisms for assessing the adequacy of the level of protection and for implementing appropriate safeguards; – the notifying of personal data breaches in the operational sector, including guidance on risk assessment, incident documentation, and communication of a personal data breach to the data subject; – the role and responsibilities of processors in the public sector, in particular in relation to data processing agreements and the monitoring the compliance with the LED; – the criteria to be considered when carrying out a data protection impact assessment under Article 27 LED. Incorporating the above topics into future EDPB guidelines would enhance transparency in the application of the LED and facilitate the harmonisation of supervisory and administrative practices across the Member States.

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?

	2022	2023	2024	2025 (until August)
Total of complaints	(UODO) 90 + 5 = 95	85 + 9 = 94	105 + 7 = 112	74 + 7 = 81
Total of complaints lodged by bodies, organisations or associations in accordance with Article 55 LED	1	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?

- (●) Yes
- ( ) No

11.2.a Please indicate approximate increase in percentages

37

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

- [x] The respect of the proportionality and necessity principle
- [x] The respect of the purpose limitation principle, including for subsequent processing (Article 4 (1) (b) LED)
- [x] Data minimisation principle (Article 4 (1) (c) LED)
- [x] Accuracy of the data (Article 4 (1) (d) LED)
- [ ] Storage limitation principle (Article 4 (1) (e) LED) and appropriate time limits (Article 5 LED)
- [x] Accountability of the controller (Article 4 (4) LED)
- [x] The determination of the legal basis (Article 8/Article 10 LED)
- [x] The conditions related to the processing of special categories of personal data (Article 10 LED)
- [ ] Automated individual decision-making, including the right to obtain human intervention in automated individual decision - making (Article 11 LED)
- [ ] Modalities for exercising the rights (Article 12 LED)
- [x] The right to information (Article 13 LED)
- [x] Right of access by the data subject and limitations to this right (Articles 14 and 15 LED)
- [x] The right to rectification or erasure of personal data (Article 16 LED)
- [ ] Exercise of the data subject's rights in the context of joint controllership (Article 21 LED)
- [ ] Data protection by design and by default (Article 20 LED)
- [ ] The obligation to keep track of the logs and purposes of processing regarding the logs (Article 25 LED)
- [ ] The obligation to conduct a data protection impact assessment (Article 27 LED)
- [x] The obligation to ensure the security of processing, including data breaches (Articles 4 (1) (f), 29 LED)
- [x] Other:

11.3.a Please clarify:

More than 60% of complaints examined by the President of the Office for Personal Data Protection concerned irregularities in the processing of personal data by the Commander-in-Chief of the Police in the National Police Information System. Some cases also concerned the National Criminal Information Centre (KCIK) and the Central Deprived of Freedom Database (CBOPW) maintained by the Director-General of the Prison Service. The UODO also received complaints from municipal guards concerning the refusal by telecommunications operators or insurance companies to provide data, which made it impossible to identify the perpetrators of offences. Other examples of infringements include: - sharing personal data by directors of prisons with other detainees, - making data available by the police to unauthorized persons (e.g. during intervention, questioning, or in connection with a complaint), - transferring data by the police to district sanitary inspectors, - processing data in KSIP beyond the statutory retention periods, - lack of a legal basis for processing or disclosing data in KSIP, KCIK and CBOPW, - failure to comply with information obligations towards data subjects, - refusal to erase data in the above-mentioned systems. The other supervisory authorities of the public prosecutor's offices reported complaints mainly concerning: - the disclosure of personal data in the introductory part of decisions issued in preparatory proceedings, - lack of anonymisation of data in criminal case files, - the inclusion in case files of materials containing genetic data used for identification purposes, - the exercise of the right of access to data and the right to erasure. It is worth noting that with regard to personal data processed in criminal proceedings, the supervisory authorities pointed out that the data subjects rights may be exercised only within the scope provided for in specific procedural laws governing such proceedings, and not on the basis of the Act implementing the LED.

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 (eg C-205/21, C-80/23) changed your approach?

During this period, a complaint was received concerning the disclosure by medical staff in a penitentiary facility of information contained in an opinion on the complainant's health status to an officer of the Prison Service. However, as the complaint was lodged after the expiry of the 30-day deadline laid down in Art. 50 of the Act implementing the LED, the President of the UODO issued a decision refusing to initiate proceedings. In addition, administrative proceedings are currently pending in a case concerning the processing by the Police of data on the complainant's health status, including the disclosure of such data to a person suspected of committing an offence against the complainant.

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

	2022	2023	2024	2025 (until August)
Total number of decisions	8	4	11	2
Total number of inactions	3	1	0	1

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**:

Decisions	2022	2023	2024	2025 (until August)
Pending judicial proceeding	2	5	2	0
Inadmissible action	4	0	1	0
DPA’s decision upheld/partially upheld etc	4	2	5	0

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**:

Inactions	2022	2023	2024	2025 (until August)
Pending judicial proceeding	0	0	0	0
Inadmissible action	0	1	0	1
DPA’s decision upheld/partially upheld etc	3	0	0	0

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)?

During this period, the decisions issued by the President of the UODO were primarily challenged by data subjects. The challenges related both to procedural aspects (e.g., violations of administrative procedure rules, failure to ensure the active participation of the party in proceedings, lack of access to case files, and insufficient reasoning in decisions) and to substantive aspects (e.g., incorrect interpretation or application of the provisions of the Act implementing the LED, failure to adopt corrective measures such as orders to delete personal data, and inadequate assessment of the necessity of continued processing, including data subject to expunged convictions). Additional objections concerned the disregard of relevant administrative court case-law and the excessive duration of proceedings. Complaints often highlighted issues pertaining 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.

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)?

	2022	2023	2024	2025 (until August)
Full-time equivalents working on the LED.	(UODO) 6+ 47=53	6+ 47=53	6+ 47=53	6+ 47=53
Percentage of overall staff	16%	14%	14%	14%

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

- ○ Sufficient
- ◉ Insufficient

13.2.a Please explain why:

The President of the Office for Personal Data Protection considers the Office's human resources to be insufficient. They represent 5% of the resources of the supervisory authorities competent for courts and prosecutors' offices (which completed the questionnaire), despite the fact that the scope of tasks (including the number of complaints lodged) and the number of entities subject to supervision by the President of the UODO are significantly higher. With the current staffing levels, the capacity to conduct a larger number of inspections on operators applying the LED provisions is severely limited. Similar conclusions were also drawn by Schengen Evaluators during their evaluation mission to Poland in 2024. Most (but not all) of the supervisory authorities competent for prosecutors' offices assessed their human resources as sufficient. Nevertheless, the analysis of their responses indicates that tasks related to the application of the LED are often performed by data protection officers (DPOs). It was highlighted that these individuals are also tasked with other responsibilities and do not receive additional financial resources for performing these extra functions. Limited financial resources were also noted as a key factor contributing to staff shortages, including insufficient funding for implementing additional safeguards and remunerating employees responsible for data protection. Among supervisory authorities competent for courts that recognise their oversight under the LED procedure, some assessed their human resources as sufficient. However, the majority indicated that available resources are inadequate for the proper fulfilment of tasks related to the supervision of personal data processing under the Act implementing the LED. In some cases, responses were also prepared by DPOs.

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

- ◉ Yes
- ○ No

13.3.a What challenges are you facing? (Multiple choice is possible)

- ☑ Insufficient expertise in criminal law
- ☑ Insufficient expertise in working methods and practices of law enforcement authorities
- ☑ Insufficient expertise in international cooperation in criminal matters
- ☑ Insufficient expertise in technologies used in the area of law enforcement
- ☑ Insufficient IT resources
- ☐ Other challenges

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

In accordance with the judgments of the courts (Provincial Administrative Court in Warsaw, 19 December 2018, ref. II SA/Wa 700/18 and 10 October 2017, ref. II SA/Wa 314/17), the UODO does not have the authority to intervene in procedures conducted by police authorities or to assess decisions regarding the usefulness of personal data collected within the framework of police statutory activities. In practice, this means: Inability to verify police working methods – the Office cannot assess whether the police correctly select the means of processing personal data in criminal proceedings. This limits the ability to gain knowledge about investigation techniques used by law enforcement authorities, methods for selecting and processing personal data in investigations, and methods for assessing the suitability of data for law enforcement purposes. Limitation on the assessment of the usefulness of data – UODO cannot analyse which data is necessary or proportionate in a specific procedure. This prevents gaining practical knowledge about the criteria used by law enforcement authorities when selecting information. Impact on the development of UODO staff expertise – Office personnel have limited access to real-life examples of the application of the law in operational practice, which hinders the development of competencies in: criminal law and its practical application, the working methods and practices of law enforcement authorities, international cooperation in criminal matters. As a result, this case law creates a situation in which UODO can only analyse and supervise the formal and legal aspects of data processing, but not their practical application in the operational activities of the police. Although case law limits UODO's ability to intervene in police operations, this gap can be partially mitigated through: 1. Specialised training and workshops: Training delivered by experts in criminal law, cybersecurity, and law enforcement technologies. 2. Case studies and simulations: Analysis of hypothetical scenarios for processing personal data in criminal proceedings without breaching actual operational procedures. 3. Cooperation with law enforcement authorities for knowledge sharing: Conducted within the limits of the law and without interfering with ongoing proceedings (e.g., exchange of experience regarding data protection standards in the police). 4. Development of technological competences: Investment in IT tools and digital training to enable better assessment of data processing risks.

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:

Without access to real investigative procedures, it is difficult to assess the risks of a data breach in practice, even with knowledge of the rules. Conclusion: see 13.2.a.1.

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:

Restrictions on access to police procedures make it difficult to understand how authorities cooperate with foreign partners and what risks this may entail for personal data. Conclusion: see 13.2.a.1.

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:

In the context of the development of new technologies and the digitisation of law enforcement activities, UODO employees report the need for practical training and exchange of experience, e.g. on: • analysis of digital data and security of information systems, • the use of tools to detect data breaches in the digital environment, • practical aspects of international cooperation (e.g. exchange of data within Europol). Conclusion: see 13.2.a.1.

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

Although jurisprudence limits police interference, this gap can be partially compensated by: Invest in IT tools and digital training to better assess the risk of data processing. Conclusion: see 13.2.a.1.

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

- ○ Yes
- ◉ No

13.4.b Please provide more details:

One of the obstacles to using the EDPB expert pool is that, under current Polish law, proceedings must be conducted in the Polish 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?

- ◉ Yes
- ○ No

14.1.a Please provide more details:

Law implementing LED does not provide President of UODO with any effective, proportionate, or dissuasive penalties for infringements of the provisions adopted under LED (Art. 57 LED). In proceedings concerning violations of this Act, UODO may not impose administrative fines. Consequently, the DPA lacks preventive and deterrent instruments. If a detected infringement is subsequently remedied, the DPA—unlike under GDPR—cannot issue a reprimand or impose administrative fines. This restricts the range of available instruments and deprives the procedure of its deterrent effect. It is not possible to issue reprimand where other corrective measures cannot be applied—e.g. when restoring compliance is impossible or has already occurred before the administrative decision is issued by UODO. Reprimand is not provided for in act implementing LED. Its absence limits the effectiveness of the DPA's powers, as a reprimand serves both a preventive and educational function—it allows the authority to respond to a remedied infringement while providing clear guidance to the controller or processor. Notably, UODO is the only SA without the power to issue reprimand, unlike SAs competent for courts and prosecutors. Although LED does not specify the exact sanctions, the DPA is not equipped with any enforcement tools, rendering the current implementation of Art. 57 LED ineffective. Point 7 of the questionnaire highlights difficulties arising from the implementation of Art. 45 LED. Under this model of data protection, data subjects are effectively deprived of guarantees for the enforcement of their rights. Furthermore, Polish system lacks a mechanism for indirect access that would allow data subjects to obtain an additional safeguard if LEA refuse to provide information, rectify or erase data. Consequently, citizens cannot request that UODO verify the lawfulness of data processing in this area. This effectively deprives individuals of the possibility to exercise one of the key protective instruments envisaged by LED, thereby weakening the right to an effective remedy. The argument that this safeguard could be ensured via the right to lodge a complaint is not convincing, considering the complementarity of the two instruments. In the draft act submitted in 2018, the drafters claimed that the mechanism under Art. 17 LED is implemented through complaints to the UODO (Art. 52 LED). From the outset, the President of UODO pointed out that this is a separate instrument, which should be implemented through other procedures and serves different objectives. As confirmed in CJEU case-law (C-333/22), this view is correct. It should also be noted that Art. 4 LED was incorrectly implemented—the rules on personal data processing provided in LED are not fully reflected in Chapter on principles relating to processing of personal. Only the principle of legality was included, while the remaining principles were moved to the chapter dedicated to the controller and processor, treating them not as the foundation of the data protection system but merely as controller obligations. The implementing act also uses outdated terminology for special categories of personal data, referring to them as "sensitive data" instead of "special categories of personal data." The President of UODO has repeatedly called for amendment of provisions concerning the role of DPOs in law enforcement authorities. Current law allows assignment of controller tasks to the DPO, such as conducting DPIAs and submitting requests for prior consultation. The DPO's role is to support the controller by providing recommendations and monitoring implementation, not to replace the controller. Current provisions may create conflicts of interest for the DPO. Legislation should also clarify the scope of controller data that must be provided to UODO regarding DPO appointments, dismissals, or changes, as there is no obligation to notify the President of UODO of changes to controller data. Certain judicial SAs and President of UODO emphasize urgent need to amend implementing act to fully and unambiguously align it with LED, particularly regarding ordinary courts. Judicial SAs report interpretative challenges: delimitation of the scope of LED and GDPR for processing by courts outside judicial capacity and by LEA; classification of processing as high-risk requiring prior consultation; application of rules on transfers to third countries in operational cooperation; and exclusion of supervision by an independent authority over judicial bodies regarding data not within judicial capacity.

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

- (●) Yes
- ( ) No

14.2.a Please provide more details:

The catalogue of data not subject to personal data protection under Act implementing LED has been expanded. This concerns data contained in case files, record-keeping activities, or IT-based systems, processed under the Act on the Support and Social Rehabilitation of Minors. The provisions apply to: - proceedings in cases of demoralization against persons over 10 years of age who are not yet adults; - proceedings concerning criminal acts committed by persons after the age of 13 but before turning 17; - enforcement of educational, therapeutic, or corrective measures against persons subject to such measures, but not beyond the age of 21, unless otherwise provided by law. Additionally, with respect to separate provisions regulating personal data protection in common courts, the role of the Minister of Justice as the data controller in court ICT systems has been clarified, along with the role of presidents and directors of competent courts, as well as the Minister of Justice as joint controllers of personal data processed in court ICT systems in the course of administering justice or performing tasks related to legal protection (Journal of Laws 2023, No. 1860). Regarding the Act on the Public Prosecutor's Office, from 28 September 2023, it has been specified that personal data processed by common organisational units of the Public Prosecutor's Office in the field of law enforcement are subject to supervisory duties, powers, and tasks under Article 44(1) and (8) of the Act implementing the LED (notifying data breaches, conducting inspections), which are to be carried out by the National Prosecutor.

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

- (●) Yes
- ( ) No

14.3.a Please clarify:

The President of UODO suggests that the following issues be considered in the assessment: - the status and role of the Data Protection Officer (DPO), - maintaining the independent status of the supervisory authority, - whether all supervisory authorities designated in a Member State are competent to carry out the tasks assigned to them and exercise the powers conferred on them by LED within the territory of their Member State, - 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, - whether the Member State has effectively adopted rules establishing penalties for infringements of LED provisions. The following issues were reported by the judicial supervisory authorities: – The need to further harmonise the definition of high-risk operations and the criteria for their identification in the justice and law enforcement area. In practice, there are differences of interpretation that hinder the uniform application of Art. 28(1) LED, – No dedicated tools supporting risk analysis in the context of the LED, analogous to those available in GDPR. The development of 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 the IT systems used by the competent authorities, in particular as regards ensuring compliance with the principles of data minimisation, purpose limitation and retention, – The need to strengthen the competences of the DPO in the operational sector, through dedicated training taking into account the specificity 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.

President of UODO emphasizes that ensuring 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, does not obstruct the activities of LEA or courts. Independent supervision of compliance with the LED is a fundamental element of the rule of law, a cornerstone of the protection of human dignity, and a tool to enhance transparency, accountability, and professionalism in the processing of personal data. Proper application of LED rules supports lawful and efficient performance of operational tasks by authorities, rather than limiting their effectiveness. LED provisions contribute to public security and the cybersecurity of judicial and LEA. By setting standards for integrity, confidentiality, and responsible data processing within IT systems, LED strengthens the protection of personal data in the digital environment, minimises the risk of breaches, and reduces potential cyber threats that could impede the effective performance of duties by state authorities. Data protection is an integral part of strategic state security. Compliance with LED rules also increases public trust in judicial and LEA, while supporting the effectiveness of their operational activities and ensuring compliance with EU data protection standards. Personal data protection is not merely a legal obligation but also a tool to enhance efficiency, transparency, and professionalism in the functioning of public authorities. The President of UODO suggests that these points be considered as political messages in the EDPB report to clearly highlight the role of personal data protection as an element of the rule of law, public security, and cybersecurity within the justice and law enforcement sectors. From a judicial perspective, it is crucial that future reports by the Commission and the EDPB clearly distinguish between the competences of law enforcement authorities applying the LED and the activities of courts operating under a separate legal regime. Judicial supervisory authorities stress that the questions in the questionnaire largely do not relate to the functioning of ordinary courts. They underline that LED and the implementing act primarily concern LEA and other bodies competent for crime prevention and detection, not courts. Furthermore, judicial supervisory authorities recommend including the following policy priorities and communications in the EDPB report to ensure consistent and effective application of Directive 2016/680 across Member States: 1. Strengthen the role of Data Protection Officers (DPOs) in the operational sector: In many Member States, DPOs carry out advisory and supervisory functions within law enforcement and judicial authorities. However, limited access to operational information and insufficient dedicated training impede their effective performance. The EDPB should promote policies supporting the development of DPO competences in the operational sector, taking into account the specificities of data processing in investigative, preventive, and repressive activities. 2. Clarify the boundaries between LED and GDPR regarding courts and administrative authorities: Difficulties arise in classifying processing operations conducted by courts outside the administration of justice. Ambiguities create divergent interpretations and complicate supervision. The EDPB should initiate the development of EU level guidelines to ensure uniform understanding and application of the LED in relation to the GDPR. 3. Promote interoperability of IT systems compliant with LED: Cross-border cooperation among law enforcement authorities requires IT systems that ensure compliance with data protection rules. The EDPB should support legislative and technical initiatives to harmonize interoperability standards while maintaining a high level of data protection. 4. Enhance risk assessment and DPIA mechanisms in the operational sector: Currently, there is a lack of analytical tools tailored to the operational context of law enforcement authorities. The EDPB should encourage the development of risk matrices, DPIA templates, and consultation procedures dedicated to the operational sector to improve risk assessment and supervision. 5. Harmonize rules on data transfers to third countries: International cooperation often involves transferring personal data across borders. Clear and uniform rules are necessary to ensure an equivalent level of data protection in relations with third countries. The EDPB should support legislative and interpretative measures to achieve consistency and safeguard data subjects' rights.

Contact

Contact Form