Contribution ID: 8e73efb6-7b2b-4b6e-8202-d53460e32d74
Date: 14/01/2026 19:57:03

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:

Germany

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

The questionnaire was completed by the persons working on the LED in the DPAs, e.g. the Heads of the respective divisions or legal advisors working in the divisions.

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

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).

	2022	2023	2024	2025 (until August)
Number of requests (numbers only)	184 (13 DPAs)	262 (14 DPAs)	266 (14 DPAs)	218 (14 DPAs)

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

- (●) Increase
- ( ) Decrease

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

3.1.a In how many cases – please indicate this per year?

	2022	2023	2024	2025 (until August)
Number of cases (numbers only)	20	23	30	35

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?

No.

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?

In general, German data protection supervisory authorities are regularly involved in legislative procedures concerning the processing of personal data and, in some cases, also in administrative regulations. In particular, regulations in federal and state police laws should be mentioned here. In some cases, involvement did not occur until very late in the legislative process. In some cases, the data protection supervisory authorities were only given a very short period of time for their review.

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.)?

Article 28(1) LED:
- Deployment of facial recognition cameras
- Introduction of intelligent video surveillance by the police
- Use of body-worn cameras by the police
- Automatic number plate recognition
- A system for the automated, AI-based detection of distraction in public traffic
- Automatic speech recognition solution
- Electronic files/document management systems
- Electronic case management systems
- Implementation of a tool which enables a simultaneous search in various police databases and across case files
- Automatic data analysis
- Special software used by the police in the area of terrorism prevention
- Establishment of a joint centre for telecommunications surveillance
- Open Source Intelligence Tools
- New method for locating mobile phones from which emergency calls are being placed

- Electronic monitoring of residence by the police with ankle tags
- Joint IT- and communication systems for the police and regulatory authorities
- Introduction of smartphones for the police
- Online system for reporting incidents to the police
- Set up of new steering and operation control system for the police
- Remote medical examinations of persons in custody
- A research project on audiovisual interrogation situations by the police authorities
- A ressearch project in cooperation with the police regarding the AI-based detection of dangerous situations
- Data processing agreements entered into by the police with data processors

Article 28(2) LED:
Legislative measures in police and security law, e.g.:
- Video surveillance
- Video surveillance in custody
- Use of body-worn cameras by the police, including in homes
- Use of mobile unmanned vehicles
- Facial recognition by matching with public websites
- Real-time remote identification with facial recognition
- Electronic monitoring of personal locations
- Undercover and intrusive measures
- New law enabling the police to automatically collect the location of an emergency call
- New law allowing the police to search for information across various data sources and case files
- Algorithm-based data analysis and profiling
- New law allowing the police to use personal data to test new IT-products or train AI
- New law allowing the use of so-called ‘scan-cars’ in the investigation of parking violations (capturing visuals of license plates and the vehicle suspected of violating parking regulations, as well as the time and location)
- Automated and AI-based detection of traffic offences
- Electronic monitoring of residence by the police with ankle tags for dangerous persons
- Behavioral restrictions for dangerous persons
- Data tranmission to non-public bodies (preventive measure in domestic violence cases)
- Background checks
- Requirements for legitimate change in purpose when processing data
- Meetings for information exchange with various institutions from the public and non-public sector in cases of violence against women
- Protection of the core area of private conduct of life
- Safeguards regarding data processing with a high impact on data subjects, such as notifications in cases of processing and collection of data without the knowledge of the data subject;

Act amending the Laws on the Execution of Prison Sentences

Amendment to the law regulating data processing in institutions handling the accommodation of mentally ill criminals

Law on Assistance and Protection Measures for Mental Illnesses

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 LE
advised or ordered competent authorities to take any necessary measures to either mitigate the risk posed or br

	2022	
Number of notifications (numbers only)	187 (13 DPAs)	251 (14 DPAs)
Percentage of measures advised or ordered	0-20% per DPA	0-25% per DPA

5 International transfers

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

- (●) Yes
- ( ) No

5.1.a What was the nature of the legally binding instrument grounding the transfer (e.g. bilateral MLA agreement, multilateral agreement)? Did the instrument contain all the appropriate safeguards necessary to provide an equivalent level of protection? Did you encounter any cases where the instrument did not meet the standard and what enforcement measures were taken, if any?

Bilateral Agreements. The scope of our investigation did not include the compliance of the agreements with the LED.

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

5.2.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?

Data from criminal investigations. The scope of the investigation of one DPA did not include the compliance of the agreements with the LED.

In another case the data transfer has been carried out lawfully and in accordance with the applicable law.

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

5.3.a Did the investigation reveal (possible) issues of non-compliance (if so, which)? Have there been cases where you requested documentation pursuant to Article 38(3) LED? In relation to any transfers under Article 38 (1)(d) LED, did the controller conduct a fundamental rights “balancing” test and, if so, were you satisfied that it was conducted properly and documented correctly?

No violations were detected, but there were deficiencies in the documentation.

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.a Please provide a few examples:

The obligations under Chapter V of the LED are regularly referred to in the context of reviews, consultations or training courses.

For example, reference was made in consultations to the obligations under Sections 39d et seq. SOG M-V, Sections 78 et seq. Federal Data Protection Act (BDSG).

The Rhineland-Palatinate Data Protection Authority carried out an ex-officio investigation and informed the police authority of Rhineland-Palatinate about the necessary requirements regarding data transfers according to Chapter V of the LED.

Control of specific data transmissions (mandatory under national law).

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?

The obligations under Chapter V of the LED have been referred to in the context of reviews, consultations or training courses. Guidelines were issued by the EDPB. There are no additional national guidelines.

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?

Yes. For example, there was one complaint regarding the transfer of data to Interpol.

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?

Yes, investigative powers have been exercised by some DPAs. These DPAs do not have the listed powers (limitations, ban) at their disposal.

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?

Yes. For example, to examine a joint centre of law enforcement authorities of several member states.

There are no general mechanisms in place.The mechanisms are determined on a case-to-case basis.

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:

Advice is provided regularly in the context of inspections and, where applicable, complaints, as well as in response to reports.

Some DPAs offer training courses, e.g. on the rights and obligations concerning the processing of personal data. These courses address staff members of competent authorities and in particular the DPOs from the competent authorities. Topics: introduction into the legal framework of data processing, compliance with data protection obligations, handling data breaches, data subjects' rights, artificial intelligence in context of law enforcement.

Some DPAs refer to their websites, which for example contain relevant activity reports, guidance, newsletter, brochures, faq. Some DPAs refer to their acitivity reports.

Some DPAs have a regularly, e.g. monthly, network meeting with the data protection officers of the police.

The following Guidelines and tools have been reported by the DPAs:

- A template for an impact assessment
- Handouts on the topic of impact assessment
- Guidance for police authorities regarding the handling of requests for access
- Development of model forms for compliance with and control of the legal requirements regarding the special powers for data collection and special measures according to the Police Law
- Guidance on how to implement video surveillance by the police lawfully
- Advice to the prosecution service on lawful data transmission via fax over IP
- Advice to a prison regarding the list of processing operations

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?

The DPA of North Rine-Westfalia faced difficulties, however, not concerning courts, but public prosecutors. The ministry of justice and some public prosecution offices deny its competence to proceed proactive controls

without a prior complaint. One of several reasons given for this is that the public prosecutors would act in their judicial capacity which is not the case.

The DPA of Bremen also faced difficulties with the supervision of public prosecutors. The public prosecutor's office does not fully authorize the DPAs responsibility for data protection supervision. One reason for this is that the LED has not yet been fully implemented in the federal state of Bremen, in our opinion. The DPA also believes that the courts rely extensively on Article 45(2) of the LED (for further information: 7th Annual Report, 6.4; 8th Annual Report, 6.5).

The DPA of Lower Saxony reports: Pursuant to Section 57(3) of the Lower Saxony Data Protection Act, there is no competence to supervise the public prosecutor's offices in case of collection of personal data during fact-finding investigations until the conclusion of the proceedings. Some other DPAs have also reported difficulties when examining ongoing criminal investigations. They sometimes face a negative stance and supervisory powers are initially denied. They are still trying to find a solution and these contrary opinions keep being discussed between the stakeholders.

The federal DPA (BfDI) faced difficulties, when it examined measures taken by the Federal Police, but the data had meanwhile also become part of investigations by the public prosecutors' offices of the federal states. If the data was processed for the public prosecutors' offices, then the BfDI had no jurisdiction. This was an unsatisfactory situation for those affected, as well as a vacuum of responsibility among the supervisory authorities, if the federal states did not consider themselves responsible because of the reference to the Federal Police.

Regarding the supervision of courts, the definition of acting in "judicial capacity" is sometimes disputed. To the respective DPAs opinion fundamental technical and organisational aspects relating to data processing outside of specific court proceedings do not fall under the exception in Art. 45(2) LED (e.g. technical security measures in the electronic file system; video surveillance; general questions regarding processes that utilize AI such as speech recognition software).

The DPA of Thuringia reports, that it cannot pursue cases that affect judicial independence, e.g., if a court order has been issued and the data processing is based on this order and carried out within the scope of the order (Section 2 (9) sentence 2 of the Thuringian Data Protection Act).

Regarding processing operations by courts which are clearly not part of their "judicial capacity" (staff, finances) no difficulties have arisen.

The federal DPA (BfDI) sees a need for clarification as to the scope of the exception in Article 45(2)(1) LED: "In our understanding, the EU law concept of "judicial authorities acting in their judicial capacity" as an exception should be interpreted rather narrowly and primarily concerns processing in the context of adjudicative activity, i. e., only judges and only insofar as they administer justice (including related processing such as press work relating to specific proceedings). Other judicial activities (and even such carried out by judges) in the broader sense, such as keeping the commercial register (the duties of a judge are listed in Section 17 Rechtspflegergesetz), would therefore not be covered by the exception. The judgment of the CJEU of 24 March 2022, in Case C-245/20 does not preclude this. In paragraph 32, the Court emphasizes that safeguarding the independence of the judiciary in the performance of its judicial tasks, cannot be confined solely to guaranteeing the independence of the judges in the adoption of a given judicial decision. However, in paragraph 34, the CJEU clarifies and limits this idea again when it states that the reference in Article 55(3) GDPR to processing operations carried out by courts 'acting in their judicial capacity' must be understood as not being limited to the processing of personal data carried out by courts in specific cases, but as referring to all processing operations carried out by courts in the course of their judicial activity. This is, of course, unfortunately worded, because it effectively explains/defines judicial capacity as judicial activity. Nevertheless, it makes it clear that the only

issue at stake is protecting the independence of the members or decisions of the courts in the context of their adjudicative activities. This finding is also supported by recent case law of the CJEU, for example on Polish judicial reform (judgment of June 5, 2023, Case C-204/21, in particular para. 91). Conversely, non-adjudicative activities do not fall under the exception of judicial activity."

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?

In Germany, there are no independent judicial authorities outside the courts.

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?)

Most DPAs consider their investigative powers effective.

However, there have been some difficulties:
- Some competent authorities have questioned the necessity of certain information, and some have refused to submit the requested information in certain cases. Some authorities have insisted on only allowing on-site inspection of the necessary information. The provision of information is not enforceable without going to court and is therefore not fully effective. According to Section 20(7) of the Federal Data Protection Act the supervisory authority may not order immediate enforcement against a competent authority or its legal entity pursuant to Section 80(2) sentence 1 no. 4 of the Verwaltungsgerichtsordnung.

- The DPA of North Rhine-Westfalia reports:
We have the power of investigation under Article 58(1)(e) of the GDPR. However, this power is only "effective" to a limited extent. There is no explicit authority to instruct responsible public authorities to provide us with the information and documents we need to perform our tasks, rather than merely granting us access.
Background: Article 47(1) of the LED stipulates that supervisory authorities must at least "the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks" be granted. The North Rhine-Westphalian legislature has therefore merely incorporated the identical power of investigation under Article 58(1)(e) of the GDPR into the North Rhine-Westphalian implementation law. In the absence of an explicit reference in Article 47(1) LED, an investigative power comparable to Article 58(1)(a) GDPR was not included. It can be argued that the investigative powers to

which we are entitled under Article 58(1)(e) GDPR are significantly more extensive than those under Article 58 (1)(a) and therefore also include an obligation on the part of the responsible authorities to send us all information necessary for us to perform our tasks. It can also be argued that without such an obligation on the part of the controllers, we have no “effective investigative powers” and that the JI Directive has therefore not been correctly implemented.
However, it would be helpful to clarify in Article 47(1) of the LED that effective investigative powers require at least obligations on the part of the controllers comparable to those in Article 58(1)(a) of the GDPR, or corresponding rights and enforcement options for the supervisory authority.
In fact, the responsible authorities have already argued that we have no right to demand that the necessary documents are sent to us.
In addition, the LDI NRW lacks the investigative powers under Article 58(1)(f) of the GDPR within the scope of the LED, which allow us, in accordance with the procedural law of the Union or the procedural law of the Member State, to obtain access to the premises, data processing facilities, and equipment of the controller and the processor.

-Discussions were held on the question whether personal data and information from ongoing investigations are covered by the investigative powers.

- The investigative powers are restricted insofar as there is no supervision with regard to a data processing that has been reviewed by a court.

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

- ○ Yes
- ◉ No

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)	135 (14 DPAs)	139 (15 DPAs)	132 (15 DPAs)	179 (15 DPAs)
On the basis of complaints (numbers only)	341 (10 DPAs)	324 (11 DPAs)	386 (11 DPAs)	267 (11 DPAs)

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

- (●) Yes
- ( ) No

8.4.a Please specify which ones:

- Some responsible parties continue to deny their obligation to provide the DPA of North Rhine-Westphalia with all the documents it needs to perform its tasks (see above)

- Some competent authorities have questioned the necessity of certain information, and some have refused to submit the requested information in certain cases. Some authorities have insisted on only allowing on-site inspection of the necessary information. The provision of information is not enforceable without going to court and is therefore not fully effective. According to Section 20(7) of the Federal Data Protection Act the supervisory authority may not order immediate enforcement against a competent authority or its legal entity pursuant to Section 80(2) sentence 1 no. 4 of the Verwaltungsgerichtsordnung.

- Some competent authorities grant access to their data / systems, but insist on their employees being the only ones handling the systems and therefore being present during the entirety of our investigative actions or rather while reviewing files in the live system (“Geführte Klickhand” - “guided click hand”). A separate test account for the SA does not exist. This leads to greater planning efforts for the on-site meetings and inspections can’t be carried out as quick, as thoroughly and as comprehensively as they could be.

- In individual cases, it was no longer possible to use the log data to investigate and clarify a past data protection violations due to deletion routines.
- The evaluation of log data was challenging due to incomplete or incomprehensible log files.
- Administrative offences, e.g. due to unauthorised data queries by police officers, become time-barred due to the long duration of previous preliminary investigations by the public prosecutor's office.

- Due to personal capacities it sometimes requires long time (weeks) to receive a response from the competent authorities.

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

8.5.a Please clarify:

Federal DPA (BfDI):
The corrective powers of the BfDI vis-à-vis the Federal Criminal Police and the Financial Intelligence Unit have been revised. If the BfDI has objected to violations pursuant to Section 16(2) of the Federal Data Protection Act, BfDI may order appropriate measures if this is 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 prior to ordering appropriate measures are not in compliance with Article 47(2) LED. Article 47(2) LED has not yet been transposed with regard to the Federal Police.

Hamburg DPA (HmbBfDI):
- In case of hazard prevention by the Police the HmbBfDI shall raise an objection and request a statement

within a deadline set by the Commissioner if the HmbBfDI identifies violations of data protection regulations, or other deficiencies in the processing or use of personal data by the police, their data processors, or entities to whom the police have wholly or partially delegated their tasks. The Commissioner may also warn the police that intended processing operations are likely to violate provisions of this Act or other applicable data protection regulations. If the Commissioner has raised an objection pursuant to sentence 1 and the violation persists after the statement has been submitted, the Commissioner may seek a judicial determination of the existence of the data protection violation. The Commissioner can not order appropriate measures.

• In case of Criminal Investigation of the Police/Prosecution Service the Commissioner can raise an objection or warn the police too. If the Commissioner has raised an objection pursuant to sentence 1 and the violation persists after the supervisory authority's response, the Commissioner may also order appropriate measures against the supervisory authority if necessary to remedy a significant violation of data protection regulations. The Commissioner is not authorized to order immediate enforcement pursuant to Section 80(2), sentence 1, no. 4 of the Administrative Court Procedure Act.

Mecklenburg-Western Pomerania DPA (LfDI MV):
Until 2023, the LfDI MV was expressly prohibited from ordering erasure in the area of hazard prevention pursuant to Section 48b (2) of the Security and Public Order Act of Mecklenburg-Western Pomerania. This prohibition was removed with an amendment to the Security and Public Order Act of Mecklenburg-Western Pomerania in 2023. With the adoption of the amendment, orders for deletion by the LfDI MV are now possible. In the legislative amendment process, the LfDI MV expressly pointed out this need for amendment. According to the explanatory memorandum to the amendment, the deletion of the exclusion is justified by infringement proceedings brought by the European Commission against the Federal Republic of Germany. (https://www.dokumentation.landtag-mv.de/parldok/dokument/56807/8_2218_gesetz_zur_anpassung_des_sicherheits_und_ordnungsgesetzes_an_bundesverfassungsgerichtliche_vorgaben)

8.6 Do you consider your corrective powers effective?

- ○ Yes
- ◉ No

8.6.a Please clarify:

The DPAs at federal and state level have different corrective powers. Not all of the powers listed in Article 47(2) LED have been implemented in federal and state legislation, in particular the powers according to Article 47(2)(b) and Article 47(2)(c) are often missing . DPAs often have additional powers, such as the right to object to identified infringements ("Beanstandung") and the right to issue reprimands.

Three DPAs have the power to impose a fine according to the national law implementing the LED on individuals. Other DPAs can impose fines in accordance with the GDPR.

The total amount of corrective measures is listed in the answer to Q 8.8, including fines according to the national law implementing the LED.

From 2022 to 31 August 2025, the three DPAs have imposed fines totalling 87.600 Euro. The Amount of the highest fine imposed was 8.660 Euro.

The supervisory authorities of the states that have fully implemented the corrective powers listed in Article 47(2) LED consider their powers as effective. The Federal DPA as well as most of the DPAs of the states that have not fully implemented the corrective powers of Article 47(2) LED do not consider their powers as fully effective.

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

- ○ Yes
- ◉ No

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	4	0	3
VIS	0	0	0	0
Other	48 (15 DPAs)	21 (15 DPAs)	24 (15 DPAs)	17 (15 DPAs)

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)	14 (15 DPAs)	11 (15 DPAs)	19 (15 DPAs)	7 (15 DPAs)

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	1 (15 DPAs)	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?

In most cases, the competent authorities followed the opinion of the DPA or complied with the decisions of the DPA.

In general terms, the relevant competent authorities are formally requested to present effective measures to remedy the data protection violation, as well as procedures to prevent violations and infringements of a similar nature in the future.

In the case of larger procedures, e.g., video surveillance, a follow-up inspection is often carried out on site.

In some cases the legal matter of the case is not resolved and therefore ongoing, even though the data concerned in the specific case have been deleted by the competent authority.

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

In some cases, the technical aspects of the data processing systems used by the competent authorities do not allow them to fully comply with the requirements of data protection law. Therefore, no measures were taken if the systems are absolutely necessary for the fulfilment of official tasks. Alternatives were agreed in some cases.

Corrective powers have not been used when the competent authorities have changed their behaviour voluntarily after being informed by the DPA.

In principle, it is sufficient to point out deficiencies and / or notify the competent authority of the DPA's legal assessment (similar to a reprimand following Article 58 (2) (b) GDPR). Since the public authority is bound by the rule of law, it has to initiate appropriate measures to reach legal compliance independently.
Only if measures are not taken voluntarily, DPAs will use their corrective powers.

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.

Article 47(5) LED has not been transposed into national federal law. The same applies to the law in most federal states.

Only the state of Hamburg has a regulation for the DPA to bring infringements to judicial authorities:
In case of hazard prevention by the Police the HmbBfDI (DPA) shall raise an objection and request a statement within a deadline set by the Commissioner if the HmbBfDI identifies violations of data protection regulations, or other deficiencies in the processing or use of personal data by the police, their data processors, or entities to whom the police have wholly or partially delegated their tasks. If the Commissioner has raised an objection pursuant to sentence 1 and the violation persists after the statement has been submitted, the Commissioner may seek a judicial determination of the existence of the data protection violation.

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	3	0	2	1

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.)

. Request for information about the legal situation for information to be provided to data subjects and for the supervisory rights of data protection authorities with regard to documents subject to secrecy.
- Request for information concerning regulations for the processing of biometric data and the use of body worn cameras in prisons.
- Request for information about the definition of ‚automated processing systems' and about guidance, opinions, or examples, on compliance with Article 25 of the LED.
- Request for information concerning the powers of the DPA in criminal cases.
- The matters related to the lawfulness of the refusal to grant access to the data of the complainant on the basis of the applicable national law, and to the lawfulness of the processing of the data of the complainant, including its transfer, under Germany's national law.
- Request for information concerning the existence of a legal basis for the use of facial recognition technology.

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

- ○ Yes
- ◉ No

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

- Guidelines 01/2022 on data subject rights - Right of access
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- Guideline 01/2023 on Article 37 Law Enforcement Directive

We also expect the currently discussed "Guidelines on data subject rights under the LED - Right of Access" to be helpful for both the DPAs and the controllers.

Although the following guidelines does not explicitly refer to the LED, it has nevertheless proven helpful for working with the LED:
- Guidelines 07/2020 on the concepts of controller and processor

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

- Scope of judicial functions
- Clarification of the respective scopes of the GDPR and the LED
- Processing of special categories of personal data
- Automated individual decision-making in the context of algorithm- and AI-based data analysis.
- The obligation to delete data; data retention; reasonable time limits or aspects for deciding on necessity.
- Any other data subject right listed in the LED besides the right of access.

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	466 (12 DPAs)	577 (14 DPAs)	656 (14 DPAs)	608 (14 DPAs)
Total of complaints lodged by bodies, organisations or associations in accordance with Article 55 LED	n/a	n/a	n/a	n/a

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

30

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)
- [x] 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)
- [x] 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)
- [x] 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:

Unlawful use of databases (not necessary for the performance of the task) by members of the police.

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?

With regard to the processing of special categories of personal data, infringements mainly concerned the fact that the processing was not lawful under national law.

In certain cases, the competent authorities did not adequately consider that processing special categories of personal data is subject to stricter requirements, particularly with regard to providing appropriate safeguards.

For example, the issue of the strictly necessity of processing arose in the context of disclosing the health data of prisoners with infectious diseases (Section 12 LJVollzDSG).

In one case there was no legal basis for processing a DNA profile.

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	9 (14 DPAs)	7 (14 DPAs)	13 (14 DPAs)	4 (14 DPAs)
Total number of inactions	0 (14 DPAs)	1 (14 DPAs)	1 (14 DPAs)	1 (14 DPAs)

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	9 (14 DPAs)	10 (14 DPAs)	21 (14 DPAs)	9 (14 DPAs)
Inadmissible action	1 (14 DPAs)	0 (14 DPAs)	8 (14 DPAs)	0 (14 DPAs)
DPA’s decision upheld/partially upheld etc	1 (14 DPAs)	3 (14 DPAs)	2 (14 DPAs)	3 (14 DPAs)

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 (14 DPAs)	0 (14 DPAs)	0 (14 DPAs)	0 (14 DPAs)
Inadmissible action	0 (14 DPAs)	0 (14 DPAs)	0 (14 DPAs)	0 (14 DPAs)
DPA’s decision upheld/partially upheld etc	0 (14 DPAs)	1 (14 DPAs)	1 (14 DPAs)	0 (14 DPAs)

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)?

- In one case, a data subject lodged a complaint with a court in 2024 against a decision of the BfDI regarding a rejected SIS access request by the responsible body. The case is ongoing and the complaint has not yet been substantiated; only a request for access to the case file has been requested.

- In one case, dispute over whether a suitable legal basis exists.

- The question of whether log data falls under the data subject's right of access was challenged.

- The police filed a lawsuit in response to our formal complaint. The complaint concerned the police's refusal to release log data (Article 25 LED), following his request for information from the police. However, the court ruled that there was no right to access this information.

- The scope of the investigations and the decision by the DPA.

- Decisions were challenged by a data subject because the data subject was of the opinion that the results of the DPA's investigations were incorrect and - therefore - the conclusions based on it were wrong, too.
One decision concerned the right to erasure regarding data stored by the police; the other decision concerned an alleged data transfer from the public prosecutor's office to a lawyer. The decisions were wholly upheld in court.

- Fines imposed on natural persons (employees of the controllers). The main argument was that no unauthorized data processing had taken place.

- The right to erasure.

- Disclosure of personal data by transmission.

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.	56,40 (16 DPAs)	58,60 (16 DPAs)	59,85 (16 DPAs)	63,40 (16 DPAs)
Percentage of overall staff	1,5-10% per DPA	1,6-10% per DPA	1,6-10% per DPA	1,6-10% per DPA

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:

Most of the state DPAs have low human ressources (some less than one full-time equivalent). Due to the high amount of complaints and of mandatory inspections regulated by national law, they have no opportunity to set their own priorities for inspections or other tasks.

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:

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:

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:

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:

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

The challenge of insufficient IT resources can either be overcome by allocating more personell or by increasing the efficiency of already available resources. The same applies to the other possible challenges in 13.3.a.1 to 13.3.a.4.

For example regarding cases in which police IT systems play a prominent role, it is still common practice that the police is hesitant to let the DPA handle the systems during inspections. Instead, the police is operating the systems while the DPA is limited to ask questions and to guide the operating police officer to the relevant pieces of information in the system. In these cases an increase in efficiency could be easily achieved by granting the DPA its own access to the IT systems or to test versions thereof to build up own expertise. This could save a lot of resources / time and further the understanding of the IT infrastructure in question as a whole.

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

- ○ Yes
- ◉ No

13.4.b Please provide more details:

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:

- Regulations concerning data processing in the context of criminal investigations are found in the German Code of Criminal Procedure (“Strafprozessordnung”; StPO). They function as a transposition of the LED especially for the criminal courts, the public prosecutor’s office and the police (when acting as a law enforcement agency). Many of the legal norms predate the LED, however, and therefore have to be interpreted as they often remain silent on specific LED-related issues or conflict with other data protection regulations (e.g. the GDPR).
In some cases, for example, it is not clearly regulated who the competent authority is (police or public prosecutor’s office), which laws apply (StPO or state police law) or which legal provisions exactly permits the data processing in criminal investigations.

- The demarcation between the respective scopes of the GDPR and the LED remains ambiguous. Furthermore, defining the boundaries of “judicial activity” proves challenging in some cases.

- Mecklenburg-Western Pomerania:
In the area of hazard prevention, the principles relating to processing of personal data within the meaning of Article 4 LED are not sufficiently implemented in the Security and Public Order Act of Mecklenburg-Western Pomerania.

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:

Federal Law:
The Anti-Money-Laundering Act (Geldwäschegesetz) now includes corrective powers, providing the legal basis for the operation of the Financial Intelligence Unit.

Rhineland-Palatinate:

In Rhineland-Palatinate, the state data protection act regarding penitentiaries 2025 was amended regarding the right to information.

Saarland:
A new law regarding the data processing in institutions handling the accommodation of mentally ill criminals was adopted in the Saarland in 2025. The old law and its requirements for data processing dated back to 1989.

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

14.4 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.

- The high amount of complaints consumes human resources that are lacking elsewhere. The amount of work involved in handling complaints is often disproportionate to the objective significance of the matter. In order to enable DPAs to use their resources more effectively in fulfilling their entire range of tasks, they should be given greater discretion in handling complaints.

- Regarding the provisions in Article 17 (3) LED, the Saarland DPA would like to point out a discrepancy with the regulation in Article 52 LED.
While Article 17 (3) LED leaves room for the national legislator to regulate that the DPA 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 here (just like in Article 15), this does not apply to the provisions in the context of complaints following Article 52 LED.
This could lead to a situation where the public authorities voice the same interests as in Article 15 (1) LED (e.g. the prejudicing of prevention, detection, investigation or prosecution of criminal offences) but the DPA would not be able to take these interests into account when issuing its final decision.
It is unclear whether the legal assessment under Article 17(3) can be applied to such cases, nonetheless.
Concerning the scope of the LED, in some cases it is still unclear whether the directive should actually be applicable at all. Following Article 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 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.

Contact

Contact Form