Evaluation of the LED under Article 62 – Questions to Data Protection Authorities / European Data Protection Board

Fields marked with * are mandatory.

Background

The Data Protection Law Enforcement Directive (LED)[1] entered into force on 6 May 2016 and the Member States had to transpose it by 6 May 2018[2]. It applies to the 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 is the first instrument that takes a comprehensive approach to data protection in the field of law enforcement, including by regulating 'domestic' processing. It is therefore a significant development compared with the earlier Framework Decision (which covered only transmission between Member States) that it repealed and replaced.

By harmonising the protection of personal data by law enforcement authorities in EU and Schengen countries, it contributes to increased trust and data exchange between authorities for law enforcement purposes, provided such exchange is based on a law, while at the same time ensuring that the rights of individuals are effectively protected.

As required by the LED[3], the Commission shall present to the European Parliament and to the Council a first report on the evaluation and review of the Directive by 6 May 2022[4]. 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 has already started a dialogue with the Member States through the Council Working party on Data Protection. A dedicated questionnaire has also been sent to civil society organisations by the European Union Agency for Fundamental Rights (FRA).

For the purpose of the evaluation and review the Commission shall in particular examine the application and functioning of the LED provisions on international data transfers[7]. Besides, this questionnaire 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 on your activities (e.g. as regards the decision-making, awareness-raising, training etc.) which fall under the scope of the LED.

We would be grateful to receive the replies to this questionnaire in its online form in English, before **5 November 2021**, so that they can be sent to the European Commission as part of the EDPB contribution to the LED review by 17 December 2021

Please note that your replies may be made public.

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 the date when the LED was transposed in your Member State to 5 November 2021**, unless otherwise specified.

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

---

[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] Article 63(1) LED, [3] Article 62(1) LED,[4] Reports should subsequently be issued every four years. [5] Article 62(5) LED,[6] Article 62(4) LED, [7] Article 62(2) LED

QUESTIONNAIRE

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

* **Select your Country**

Germany

Powers

* **Q1: In your opinion, did the LED strengthen your investigative powers / corrective powers?**

- (●) Yes
- ( ) No

* **Q2: Please list your investigative powers**

- [x] To obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks
- [x] To obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law
- [x] To carry out investigations in the form of data protection audits
- [x] Other(s)

*** Q2.1: Please specify the other investigative powers not listed above**

The investigative powers of the Federal Commissioner for Data Protection and Freedom of Information ("BfDI") are implemented in Section 16 (4) of the Federal Data Protection Act ("BDSG"). According to this provision, the public bodies of the Federation are obligated to provide the Federal Commissioner and his or her assistants with (1) access to all official premises at all times, including to any data processing equipment and means, and to all personal data and all information necessary to perform their tasks; and (2) all information necessary to perform their tasks.

The investigative powers have also been implemented in state law - in some states with restrictions, as described below:

North Rhine-Westphalia: Pursuant to Section 60 (3) DSG NRW, the data protection supervisory authority is (only) entitled to the investigative powers pursuant to Article 58 (1) (e) GDPR – to obtain access to all personal data and to all information necessary for the performance of its tasks – accordingly.

Lower Saxony: Pursuant to Section 57(7) of the NDSG, the investigative powers may be limited to the extent that they may only be exercised personally by the State Commissioner for Data Protection (note: member of the supervisory authority within the meaning of Article 43 LED) if the security of the Federal Republic or of a Land so requires. The decision is made by the relevant supreme state authority. In addition, the supreme state authority may refrain from disclosing the relevant personal data to the State Commissioner for Data Protection in this case - provided that special confidentiality has been assured. So far, however, these regulations have not been applied in Lower Saxony.

Hesse: Pursuant to Section 14 (5) of the HDSIG - as in Lower Saxony - investigative powers may only be exercised personally by the Hessian Data Protection Commissioner in individual cases if a supreme state authority determines that federal or state security so requires. In this context, personal data of a data subject who has been assured of special confidentiality by the controller may not be disclosed, even to the Hessian Data Protection Commissioner.

*** Q3: Do you consider your investigation powers effective**

- (●) Yes
- ( ) No

Q3.2: If needed, please provide more details below:

In general, the investigative powers of the supervisory authorities can be considered effective, apart from the restrictions mentioned above (Q2.1). However, the BfDI would welcome a clarification of the BfDI's investigative powers provided for in Art. 47(1) LED in Section 16 (4) BDSG. Section 16 (4) BDSG is limited to the obligations of the responsible parties to grant the BfDI and his or her assistants access to buildings, facilities and data and to provide all necessary information. This obligation is however not countered by an explicit power of the BfDI to demand such access or information. For the sake of clarity, explicit investigation powers should be stipulated along the lines of Article 58 (1) GDPR. This also applies for some regulation in state laws.
The DPA North Rhine-Westphalia considers the investigative powers as "effective" only to a limited extent. There is no explicit power to order the controllers to provide the DPA with the information and documents necessary for the performance of its tasks.
Therefore, it would be helpful to clarify in Article 47(1) LED that effective investigative powers at least also require obligations of data controllers comparable to Article 58(1)(a) of the GDPR or corresponding rights and enforcement options of the supervisory authority. In fact, it has already been argued to the DPA North Rhine-Westphalia by controllers that there is no right to demand that the necessary documents be sent to the DPA (further details below, Q4).

In addition, within the scope of application of the LED, the DPA North Rhine-Westphalia lacks the power of investigation under Article 58(1)(f) of the GDPR, which allows to obtain access to the premises, data processing facilities and equipment of the controller and processor.

* **Q4: Do you face any practical difficulties in applying your investigative powers?**

- (●) Yes
- ( ) No

* **Q4.1: which kind of difficulties - for instance, have you been prevented from accessing information on the grounds of protection of sensitive information?**

Some DPAs reported difficulties:

- Some controllers have denied their obligation to provide the DPA North Rhine-Westphalia with all the documents needed to fulfill its tasks. This is justified by the fact that the national implementation law (Data Protection Act of North Rhine-Westphalia) refers solely to the power of investigation under Article 58(1)(e) of the GDPR. The responsible bodies argue that they would only have to grant the DPA access to personal data and information. However, they would not be obligated to provide information in the sense of a transfer (in the absence of a reference to Article 58 (1)(a) of the GDPR).
- In some cases, public prosecutors' offices refused to issue an opinion on the grounds that the Commissioner was not competent under state law.
- Some different views on the scope of the investigative powers (e.g. during ongoing criminal investigations) exist between the DPA and the public prosecutors' office. The implications of these contrary opinions are currently being discussed between the stakeholders.
- In four prominent cases involving threats from the right-wing scene, the police, as the data processing agency, provided the DPA with partly incomplete information, citing procedural rights of employees or approval requirements from the public prosecutor's office as the reason.
- In 2019 there was a dispute between a state Police authority and the state DPA regarding its investigative powers, namely access to documents and information from the controller. The conflict in question has been resolved, however, the issue is of a general nature and could be repeated in other circumstances. It therefore deserves attention:

According to the state law the controller is obliged to provide information and access to files and documents which are related to the data processing as far as this is necessary to fulfill the tasks of the supervisory authority. The existing exception clause in the law did not apply in this case. The DPA requested to see orders of the competent court and prosecutor's office for longer-term observations using special technical devices intended specifically for surveillance purposes (Sections 163 f, 100h (1) No 2. German Code of Criminal Procedure). The technical device used was the automatic number plate recognition. The police argued that the orders permitted the permanent automatic data collection and storage of all number plates of cars passing motorways for a period of 20 months. Since a specialized police unit was responsible for the processing of the data (controller) and was in possession of the requested documents the DPA addressed the police. However they refused to hand out the investigative orders on grounds of lacking responsibility for the decision. The police claimed only the prosecution service could decide about the DPAs access to the documents and since the investigation in this case was ongoing the prosecutor rejected the request.

* **Q5:Have you conducted investigations and/or inspections on your own initiative or only on the basis of complaints?**

Multiple replies are possible

- [x] On our own initiative
- [x] On the basis of complaints

* **Q6: Do you have all the powers listed under Article 47(2)(a), (b – including rectification, erasure, restriction) and (c) LED?**

- ( ) Yes
- (•) No

* **Q6.1: Which powers you do not have**

Multiple replies are possible

- [ ] No power to issue warnings (Art. 47(2)(a) LED)
- [x] No power to order the controller or processor to bring processing into compliance (including rectification, erasure and restriction) (Art. 47(2)(b) LED)
- [x] No power to impose a temporary or definitive limitation, including a ban, on processing
- [ ] Other(s)

Q6.1.2: No power to order the controller or processor to bring processing into compliance (including rectification, erasure and restriction) (Art. 47(2)(b) LED)- Please provide more information if possible:

These powers are not implemented in the following States / Federal level:

Federal Law (partially)
Bavaria
Berlin
Lower Saxony
Mecklenburg-West Pomerania
Thuringia

Q6.1.3: No power to impose a temporary or definitive limitation, including a ban, on processing - Please provide more information if possible:

These powers are not implemented in the following States / Federal level:

Federal Law (partially)
Baden-Wuerttemberg (Police sector, see Q7)
Bavaria
Berlin
Brandenburg
Lower Saxony
Hesse
Mecklenburg-West Pomerania
North Rhine-Westphalia
Schleswig-Holstein
Thuringia

* **Q7:Do you have the same corrective powers towards all law enforcement authorities?**

- ( ) Yes
- (•) No

* **Q7.1: what are the differences?**

In the following States as well as on the Federal level the corrective powers are different towards the authorities.

Federal Law
Baden-Wuerttemberg

Brandenburg
Bremen
Saarland

The differences are the following:

- Federal Level: Section 69 of the Federal Criminal Police Office Act (“BKAG”) provides that the BfDI may order “appropriate measures” if this is necessary to remedy a significant breach of data protection law. This presupposes that it has objected to the violations in accordance with Section 16 (2) BDSG. The question of whether the term “appropriate measures” also includes ordering the deletion of data has not yet been the subject of a decision. However, it is foreseeable that this question will become relevant. However, this provision only refers to the Federal Criminal Police.

The Customs Investigation Service Act ("ZFdG") has also been revised and entered into force in April 2021. Although the remedial powers have now been expanded, they still have shortcomings, similar to the BKAG. According to this, the BfDI may, if it has previously objected to violations pursuant to Section 16 (2) BDSG, order appropriate measures if this is necessary to eliminate a significant violation of data protection regulations. However, these powers are restricted in the explanatory memorandum to the law. According to the clarification in the explanatory memorandum to the law, the deletion of personal data is expressly excluded. However, the explanatory memorandum itself does not have any regulatory effect, but only serves as an aid to interpretation. Therefore, a contrary result could also be justified by way of LED-compliant interpretation. A decision on this is still pending in practice - also with regard to Section 69 BKAG.

In its current version, the Federal Police Act ("BPolG") does not yet provide for any further-reaching corrective powers. After the previous draft law failed in the legislative process, a revision of the law is still pending. However, the regulations envisaged in the previous draft law provided for extended corrective powers comparable to those of the ZFdG and the BKAG.

The corrective power to order an appropriate measure under the BKAG, the ZFdG and the previous draft of the BPolG are each subject to the additional restriction of a significant data protection breach. Article 47(2) LED is thus likely to be implemented only inadequately.

- Baden-Wuerttemberg:
There are different powers for the law enforcement authorities in the justice sector (Article 47(2) fully implemented) and for the police (Article 47(2) only partly implemented).
There are also restrictions with regard to public prosecutors' offices and the central office of the state judicial administrations for investigating National Socialist crimes: The powers under Article 47(2)(b) and (c) exist only to the extent that these bodies act in administrative matters. Section 9(4) of the LDSG-JB stipulates in this regard that, in particular, the decisions of the public prosecutor and preparatory or executive measures in the context of investigative, criminal or law enforcement proceedings, even insofar as they relate to the initiation of investigative proceedings, are not administrative matters. This also applies to the corresponding decisions and measures in proceedings for the investigation of criminal offenses taken by the central office of the state justice administrations for the investigation of National Socialist crimes.

- Brandenburg: Towards the police Article 47 (2)(a) and (b) powers were implemented. With respect to the public prosecutor's office /justice sector, the DPA Brandenburg data protection supervisory authority has, on the basis of the second sentence of Section 2 (1) in conjunction with Section 18 (2) of the Brandenburg Data Protection Act (BbgDSG). The supervisory authority has all powers under Article 58 GDPR except for the imposition of fines (on the basis of the second sentence of Section 2 (1) in conjunction with Section 18 (2) of the Brandenburg Data Protection Act (BbgDSG)). This leads to the fact that the powers vis-à-vis the public prosecutor's office and the police are different.

- Bremen: The powers apply only to the police sector. The LED has not yet been implemented in the justice sector.

- Saarland: The Saarland SA has all the powers listed under Art. 47 (2) LED. However, in some areas the corrective powers towards law enforcement authorities still differ. In the field of preventive police work the SPolDVG (act on data processing by the police of the Saarland) applies which includes said powers in the meaning of Art. 47 (2) LED. In the field of correctional facilities the SJVollzDSG (act on data processing by the correctional facilities of the Saarland) applies which refers to the powers under the GDPR instead.

* **Q8: Do you consider your corrective powers effective?**

- ○ Yes
- ◉ No

* **Q8.1: Please explain why do you do not consider your corrective powers effective?**

[Multiple replies are possible]

Q8 cannot be answered by "yes" or "no" as it depends on the corrective powers each DPA individually has.

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 Commissioners as well as most of the Commissioners of the States that have not fully implemented the corrective powers of Article 47(2) LED do not consider their powers as fully effective.

* **Q9: Have you used your corrective powers?**

- ◉ Yes
- ○ No

Q9.1:Which corrective powers have you applied and in how many cases? [Please list the powers used according to article 47(2)(a), (b) and (c) LED. Amongst those cases, how many were related to the supervision of SIS II[1] and VIS[2]?]

[1] Council Decision 2007/533/JHA.

[2] Council Decision 2008/633/JHA.

	SIS II and VIS	Other
47(2)(a)	☐	☑
47(2)(b)	☐	☑
47(2)(c)	☐	☐

* **Q9.1.4: Art.47(2)(a) : Number of other cases NOT related to the supervision of SIS II and VIS:**

7

* **Q9.1.5: Art.47(2)(b) : Number of other cases NOT related to the supervision of SIS II and VIS:**

7

* **Q9.2: Have the competent authorities or processors complied with the decisions that you issued in the exercise of your corrective powers?**

- ○ Yes
- ◉ No

* **Q9.2.1: how did you follow-up?**

In some cases the competent authorities have not complied with the decision issued by the DPA. The DPAs concerned reported the following:

Federal Commissioner: Not all competent authorities complied with a decision or recommendations and findings issued. Either a workshop with the competent authority was arranged in order to find a solution or the competent authority filed a lawsuit. In other cases no action on the side of the competent authority was necessary.

Brandenburg: Partly the competent authority complied yes, for instance regarding many processing operations of the competent authority that were improved to comply with the principles in Articles 4 and 8 LED. However, diverging opinions about the question whether a specific provision in national federal law could be seen as lawful legal ground for the processing prevailed. Follow up: it became superfluous since the federal law was amended in 2021. The previous processing of data could not be based on the new provision anymore.

Hamburg: The HmbBfDI issued an official order against the local police to delete a biometric database created by them containing templates of likely thousands of citizens. The Police has sued against the order. The order was subsequently rescinded by the administrative court. An appeal has been lodged by the HmbBfDI. Meanwhile the database in question was erased as ordered by the HmbBfDI. According to the plaintiff this was not because of the order but because the database was of no use for criminal investigation anymore.

Saarland: The competent authorities complied with the decisions that were issued by the Saarland SA. However, there exists no legal procedure to obtain a binding decision by a court, in case a competent authority or processor does not comply with a decision issued by the Saarland SA.

Complaints

* **Q10: Has there been an increase in complaints following the LED transposition in your Member State?**

- ◉ Yes

- ( ) No

* **Q10.1: Please indicate approximate increase in percentages.**

A slight majority of the DPAs has recorded an increase in complaints.

Since most of the DPAs do not keep specific statistics for the LED, the increase cannot be quantified precisely. One DPA has indicted the increase with 10%, one with 50% and one DPA with 100%.

* **Q11: Please indicate the issues raised the most in these complaints, in particular as regards data subject rights.**

- [x] The respect of the proportionality and necessity principle (Article 4 LED)
- [x] The respect of the purpose limitation principle, including for subsequent processing
- [ ] Data minimisation principle (Article 4 (1)(c) LED)
- [ ] 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)
- [ ] 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)
- [ ] 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)
- [ ] Other

Q11.1: The respect of the proportionality and necessity principle (Article 4 LED) - raised issues:

- Duration of the processing of personal data by the police / retention of personal data in police information systems / data bases
- mass collection of data: automatic number plate recognition
- unnecessary data processing and mistakes related to cases of traffic offences punishable by fines
- the necessity of data processing in the context of traffic offence proceedings
- Retrieving personal data about the religious beliefs of the complainant without any relevance for the affected case
- Duration of time limits to store personal data being too extensive

Q11.2: The respect of the purpose limitation principle, including for subsequent processing- raised issues:

- Duration of the processing of personal data by the police / retention of personal data in police information systems / data bases
- mass collection of data: automatic number plate recognition

Q11.5: Storage limitation principle (Article 4 (1)(e) LED) and appropriate time limits (Article 5 LED) - raised issues**:**

- Duration of the processing of personal data by the police / retention of personal data in police information systems / data bases
- Duration of time limits to store personal data being too extensive

Q11.7: The determination of the legal basis (Article 8 / Article 10 LED) - raised issues:

- unlawful use of databases (not necessary for the performance of the task) by members of the police
- mass collection of data: automatic number plate recognition
- unnecessary data processing and mistakes related to cases of traffic offences punishable by fines
- alignment of personal data by the police
- the necessity of data processing in the context of traffic offence proceedings
- transmission of personal data from the police to other public authorities or private individuals
- queries by the police from various registries
- The processing of special categories of personal data regarding the handling of drug addictions in prison without any sufficient security measures and legal basis

Q11.8: The conditions related to the processing of special categories of personal data (Article 10 LED)- raised issues**:**

- Retrieving personal data about the religious beliefs of the complainant without any relevance for the affected case
- The processing of special categories of personal data regarding the handling of drug addictions in prison without any sufficient security measures and legal basis
- The processing of personal data concerning health out of a psychological report

Q11.11: The right to information (Article 13 LED) - raised issues:

- no or not sufficient information provided by law enforcement authority to the data subject about stored data in databases

Q11.12: Right of access by the data subject and limitations to this right (Articles 14 and 15 LED) - raised issues:

- Delayed responses to requests for access to personal data
- limitations of this right
- Verification of the access of data being obtained to the complainant

Q11.13: The right to rectification or erasure of personal data (Article 16 LED) - raised issues:

- Duration of the processing of personal data by the police / retention of personal data in police information systems / data bases
- Storage of personal data of the complainant despite the criminal investigations being suspended without conviction
- Duration of time limits to store personal data being too extensive
- Non-erasure, partial erasure of data from databases

Q11.18: The obligation to ensure the security of processing, including data breaches (Articles 4(1)(f), 29 LED) - raised issues**:**

- Transfer of sensitive personal data without ensuring the security of processing the personal data in a confidential manner
- Lack of encryption regarding the electronic transfer of personal data
- The processing of special categories of personal data regarding the handling of drug addictions in prison without any sufficient security measures and legal basis

* **Q12: Are you following up on all complaints?**

- (●) Yes
- ( ) No

* **Q13:Have you received complaints by organisations representing data subjects under Article 55 LED?**

- (●) Yes
- ( ) No

Consultations and advisory powers

* **Q14:Have competent authorities utilised the prior consultation procedure in accordance with Article 28 (1)(a) or (b) LED?**

- (●) Yes
- ( ) No

* **Q14.1:In this context, did you provide written advice and/or use your corrective powers pursuant to Article 28(5) LED?**

- (●) Yes
- ( ) No

* **Q14.1.1: in how many cases did you provide written advice and/or use your corrective powers pursuant to Article 28(5) LED?**

4 DPAs indicated that they have provided written advice and/or used corrective powers. These 4 DPAs received approximately 15-20 requests for prior consultation. In approximately 12-17 cases written advice was given by the supervisory authority or corrective powers have been used.

* **Q15:Have you established a list of processing operations subject to prior consultation pursuant to Article 28(3) LED?**

- ○ Yes
- ◉ No

* **Q16:Does your national parliament / government consult you during the preparation of legislative or other regulatory measures with a data protection dimension ?**

- ○ Not at all
- ○ Occasionally
- ◉ Systematically

* **Q17:How many opinions under Article 47(3) LED, other than prior consultations pursuant to Art 28 (1) LED, have you issued upon request or on your own initiative?**

All supervisory authorities indicated that opinions of this type are made on a regular basis. Most of the supervisory authorities do not keep specific statistics and therefore cannot provide details on the amount.

* **Q18:Please indicate the types of issues on which competent authorities have approached you for advice (e.g. data breach notifications, handling of data subjects' requests, security).**

[Multiple replies are possible – please note that as regards consultations in the context of DPIAs relevant replies should be made to Questions 17 and 18]

- ☐ The respect of the proportionality and necessity principle (Article 4 LED)
- ☐ Storage limitation principle (Article 4 (1)(e) LED) and appropriate time limits (Article 5 LED)
- ☐ Accountability of the controller (Article 4(4) LED)
- ☑ The determination of the legal basis (Article 8 / Article 10 LED)
- ☐ Processing of special categories of personal data (Article 10 LED)
- ☑ Types of processing, in particular, using new technologies, mechanisms or procedures (Article 27 / Article 28 (1)(a) LED)
- ☐ Processing for purpose of research and/or innovation (Article 9(2) LED)
- ☐ Automated individual decision-making, including profiling (Article 11 LED)
- ☑ Modalities for exercising the rights (Article 12 LED)
- ☐ Handling of data subjects requests in relation to the exercise of their rights (Chapter III LED)
- ☑ Joint controllership, including on the arrangements of the joint controllers' responsibilities (Article 21 LED)
- ☐ Controller / processor arrangements (Article 22 LED)
- ☐ Data protection by design and by default, including anonymisation and pseudonymisation (Article 20 LED)
- ☐ The obligation to keep track of the logs and purposes of processing regarding the logs (Article 25 LED)
- ☑ Appropriate security measures (Article 4(1)(f) and Article 29 LED)
- ☑ Other

Q18.4: The determination of the legal basis (Article 8 / Article 10 LED)- raised issues**:**

- lawfulness of processing data
- Questions of interpretation of legal regulations
- data transfers to other competent authorities and security clearance/ reliability testing procedures
- Usage/processing of personal data collected in the context of the COVID 19 pandemic for the purpose of criminal investigations
- Implementation of technology to identify traffic offences

Q18.6: Types of processing, in particular, using new technologies, mechanisms or procedures (Article 27 / Article 28 (1)(a) LED)- raised issues**:**

- data protection impact assessment
- Design of IT systems in accordance with data protection law
- Establishment of databases
- video surveillance
- implementation of a new online tool to report an offence to the police (“Onlinewache”)
- the change from an existing case management system to a new one

Q18.9: Modalities for exercising the rights (Article 12 LED) - raised issues**:**

Q18.11: Joint controllership, including on the arrangements of the joint controllers’ responsibilities (Article 21 LED)- raised issues**:**

Q18.15: Appropriate security measures (Article 4(1)(f) and Article 29 LED) -raised issues:

- Advice on pseudonymisation
- Encryption methods
- special security measures regarding the processing of special categories of personal data

* **Q18.16: Other - raised issues:**

Data breaches:
- necessity of data breach notifications

Awareness-raising, training and guidance

* **Q19:Have you issued guidance and / or practical tools supporting competent authorities or processors to comply with their obligations?**

- (●) Yes
- ( ) No

* **Q19.1: Please list them below**

The DPAs have published numerous information concerning general issues of data protection (GDPR and LED) and specific information for issues concerning LED. Various information has been provided and published jointly by the conference of the supervisory authorities in Germany. In addition to this, the DPAs provide specific information and tools, such as:

Guidelines etc.:
- Practical tool /guideline how to carry out data protection impact assessment and risk assessment
- instructions for maintaining a record of processing activities as well as guidance on logging
- Checklist for data protection officers of public bodies
- Guidelines for prosecutors and police
- Video surveillance by public authorities
- Guidelines for the procedure of administrative offence authorities in connection with traffic offences
- Instruction for police to act on dashcam violations
- special advice within their annual activity reports in the meaning of Art. 49 LED

Online-Tools:
- data breach notification form
- online-form for the communication of the contact data of data protection officers to the supervisory authority

* **Q20:Have you provided training to / carried out awareness-raising activities for competent authorities and / or processors (DPOs included)?**

- (●) Yes
- ( ) No

* **Q20.1: how many and on which topics?**

The manner and topics of training differ for each supervisory authority. The answers are therefore copied in directly:

Federal: The BfDI regularly conducts training sessions on data protection issues in the field of law enforcement as part of the education program offered by the Federal Academy of Public Administration.

Baden-Wuerttemberg: Our in-house training centre offers open training events on a wide range of topics, in which public authority employees and data protection officers can participate. However, individual events can also be booked (e.g., employees of a public authority are to be trained on a specific topic).

Bavaria: Yes, several times a year. Topics include: Data processing by the police, by the public prosecutor's office, by correctional institutions.

Berlin: In 2019, we held a training course at the Berlin/Brandenburg Judicial Academy on the topic of "Data protection and information security in the work of the courts and public prosecutor's office". Regular working meetings are held with the official data protection officers of the Berlin courts and public prosecutors' offices.

Hesse: Yes, up to date at approximately ten occasions, e.g. on general data protection issues, data protection impact assessment, data breach notification and video surveillance.

Lower Saxony:
- Monthly exchange of experience of the police DPOs
- Seminars on video surveillance by public authorities

- Training of police data protection coordinators

North Rhine-Westphalia:
Training on the topic: Delimitation of the areas of application of the GDPR and the LED as well as general information about the LED and the North Rhine-Westphalian implementation law enacted for this purpose.

Rhineland-Palatinate:
- The LfDI Rhineland-Palatinate carries out training sessions in cooperation with the police academy of Rhineland-Palatinate twice a year. Topics: Freedom of information, data protection issues regarding social media, video surveillance techniques, big data and artificial intelligence.
- The LfDI Rhineland-Palatinate participates every year at the annual expert conference of the data protection officers and provides guidance/advice to specific topics such as data subject's rights, handling of data breaches.

Saarland: The Saarland SA raises awareness of data protection regulations regarding competent authorities in the scope of the LED by hosting or taking part in training events (for example at the Saarland University of applied sciences for administration which is also responsible for the education of police officers).
On top, the Saarland University offers a course on the practical dimension of data protection ("Datenschutzrecht in der Praxis") where the SA shares experiences from its field of work. This year, the hosted lecture will be on the topic of the LED and its transposition into the legal framework of the Saarland.

Saxony: Training events on data protection in the police and judicial sector.

Schleswig-Holstein:
- New data protection officers of the police regularly visit the office of the supervisory authority for a short term.
- Seminars on data protection in law enforcement and on general topics
- Presentations on the new regulations for DPOs and Controllers
- Regular exchange with data protection officers

Data breach notifications

* **Q21: How many data breach notifications have you received?**

Several DPAs do not keep specific statistics for breach notifications in the field of LED and can therefore not provide quantitative data.
10 DPAs have quantified the breach notifications. In total, these 10 authorities received nearly 400 notifications.

* **Q22: In what proportion have you followed up with investigations?(%)**

The investigations are not statistically recorded, so that no detailed information can be given. Some DPAs have indicated that follow-up communication or investigation is generally conducted in any case of notification.

* **Q23: In what proportion have you advised or ordered competent authorities to take measures mitigating the risks ?(%)**

Most DPAs do not keep statistics specifically on this relation.
One DPA has taken measures in approximately 40% of the notifications, two DPAs in approximately 30 % and one DPA in approximately 5 %.

* **Q24: In what proportion has the communication to the data subject been delayed, restricted or omitted on the grounds set out in Article 13(3) LED? (%)**

One DPA indicated that in approximately 25 % of the cases the communication with the data subject has been delayed, restricted or omitted. One DPA indicated that in one case the communication to the data subjects has been delayed to avoid obstructing official or legal inquiries and investigations.

Power pursuant to Article 47(5) LED

Q25: Have you exercised your power to

	Yes	No
* bring infringements of your national law(s) transposing the LED to the attention of judicial authorities?	◉	○
* commence or otherwise engage in legal proceedings?	○	◉

* **Q26:Did you face difficulties in exercising this power?**

- ○ Yes
- ◉ No

Exercise of data subjects' rights through the SA

* **Q27: How many requests under Article 17 LED have you received?**

Most DPAs have not received any such requests or do not keep specific statistics. In total there have been presumably around 50 requests to German DPAs.

* **Q27.1: What were the outcomes of the cases?**

Multiple choices are possible

- ☐ Request declared inadmissible
- ☐ All or some data requested provided to data subject
- ☐ SA informed data subject that it has conducted all necessary verifications or a review
- ☐ Controller ordered to provide (partial) access to the personal data
- ☐ Controller ordered to rectify personal data
- ☐ Controller ordered to erase personal data
- ☐ Controller ordered to restrict the processing of personal data
- ☐ SA applied other corrective powers (e.g. a ban on processing and/or fines)
- ☑ Others

* **Q27.1.2: Other - Please specify:**

For the most part, no infringements were found. Serious infringement were not found in any case.

* **Q28:Did encounter any particular problems?**

- ○ Yes
- ◉ No

International transfers

* **Q29: Have you encountered cases where a controller transferred personal data based on a 'self-assessment' pursuant to Article 37(1)(b) LED?**

- ◉ Yes
- ○ No

* **Q29.1: What kind of "categories of transfers" did the controller communicate (Article 37(2) LED)?**

BfDI: According to § 79 (3) BDSG, transposing Art. 37 (2) LED into German federal law, the controller shall file a report to the BfDI at least once a year covering transfers conducted on the basis of an assessment pursuant to Art. 37 (1)(b) LED respectively § 79 (1) (No.2) BDSG. As part of this annual notification of transfers, a competent authority e.g. specifies the following categories: Date, time of transfer, recipient state and purpose of transfer.

* **Q29.2: Have there been cases where you requested documentation pursuant to Article 37(3) LED?**

- ○ Yes
- ◉ No

* **Q30: Have you carried out any investigations into data transfers based on derogations, in particular those set out in Article 38(1)(c) and (d) LED?**

- ◉ Yes
- ○ No

* **Q30.1: Did the investigation reveal (possible) issues of non-compliance ?**

- (●) Yes
- ( ) No

* **Q30.1.1: What are the non-compliance issues revealed by the investigations?**

Q30.1 cannot be answered by "yes" or "no", because the investigation is still ongoing

* **Q30.2: Have there been cases where you requested documentation pursuant to Article 38(3) LED?**

- ( ) Yes
- (●) No

* **Q31: Have you received any information pursuant to Article 39(3) LED about data transfers based on Article 39(1) LED?**

- ( ) Yes
- (●) No

* **Q32: 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

* **Q33: Have you exercised your advisory powers towards the government and/or competent authorities with respect to data transfers under Chapter V of the LED, for instance as regards the level of appropriate safeguards under Article 37(1)(a), (b) LED)?**

- (●) Yes
- ( ) No

* **Q33.1: Have you issued any guidelines, recommendations and/or best practices in this regard?**

- ( ) Yes
- (●) No

* **Q34: Have you provided (or been asked to provide) assistance to Member States in assessing and, where necessary, reviewing their international agreements involving international data transfers (for instance, relating to mutual legal assistance, police cooperation) that were concluded prior to 6 May 2016?**

- ( ) Yes

- (●) No

* **Q35: Have you received/handled complaints (by data subjects and/or bodies, organisations or associations in accordance with Article 55) specifically addressing the issue of data transfers?**
  - (●) Yes
  - ( ) No

* **Q36: Have you exercised your investigative and/or enforcement powers with respect to data transfers?**
  - (●) Yes
  - ( ) No

* **Q36.1: In particular, have you ever imposed (temporary or definitive) limitations, including a ban, on data transfers?**
  - ( ) Yes
  - (●) No

* **Q37: Have there been cases in which you have cooperated with foreign data protection authorities (for instance, exchange of information, complaint referral, mutual assistance)?**
  - (●) Yes
  - ( ) No

* **Q37.1: Are there existing mechanisms on which you can rely for such cooperation?**
  - (●) Yes
  - ( ) No

Q37.1.1: Please specify if possible:

Yes, Internal Market Information System (IMI), Article 61, Voluntary Mutual Assistance Notification.

Judicial review

* **Q38: Have data subjects / competent authorities / processors contested your decisions (or inaction) before national courts?**
  - (●) Yes
  - ( ) No

* **38.1: Please indicate the number of cases respectively for data subjects and competent authorities /processors:**

Total: 17
data subjects: 14
competent authorities/processors: 3

38.2: What was the outcome?

Multiselection is possible

- [x] Complaints declared inadmissible
- [x] Decisions upheld
- [x] Decisions overturned

Q38.2.1: If possible, please provide additional information on decisions upheld

The LfDI Rhineland-Palatinate imposed a fine sanctioning the unlawful retrieval of personal data out of police data bases by a police officer for private purposes.
Two data subjects have challenged the HmbBfDI's decision in the area of the LED. In both cases, the plaintiffs argued that the HmbBfDI had not taken sufficient action in response to a complaint. In one case, the complaint was dismissed; in the other, the plaintiff withdrew the complaint.
Berlin: There were two cases in which complainants applied for legal aid in preparation for legal action due to inaction on the part of our authority. Both were rejected. In addition, there was one complaint by a complainant against a final decision by us, which was also rejected.
Saarland: Two of the Saarland SA's decisions got contested in October 2021. The court proceedings are still ongoing (status: 15th October 2021). The cases were both filed by an individual who opposes any and all decisions by Saarland public authorities. One of the cases concerns data storage within police information systems; the other concerns data processing by the public prosecutors' office. Since there are other proceedings by said individual that are still pending, it is foreseeable that the decisions in those cases will also be challenged before the competent court.

Q38.2.2: If possible, please provide additional information on decisions overturned

The HmbBfDI issued an official order against the local police to delete a biometric database created by them containing templates of likely thousands of citizens. The Police has sued against the order. The order was subsequently rescinded by the administrative court. An appeal has been lodged by the HmbBfDI. Meanwhile the database in question was erased as ordered by the HmbBfDI.

Cooperation

* **Q39: Have you used the mutual assistance tool under Article 50 LED?**

- (•) Yes

- [ ] No

Q39.1: Please provide numbers for:
Requests you received - please indicate the type of cooperation requested, differentiating between:

	Nbr
* Request for information	2
* Request to carry out investigations	0
* Request to carry out inspections	0
* Other	0

Q39.2: Please indicate how you replied to those requests.:

	Nbr
* Requests declined	0
* Information provided	2
* Investigation carried out	0
* Inspection carried out	0
* Other	0

Q39.3: Requests you sent - please indicate the type of cooperation requested, differentiating between:

	Nbr
* Request for information	0
* Request to carry out investigations	0
* Request to carry out inspections	0
* Other	0

* **Q40: Have you encountered any obstacles (e.g. of an administrative nature) when requesting or providing assistance to another DPA?**

- [ ] Yes
- [x] No

* **Q40.1: Please describe them as well as possible solutions.**

There have not been any obstacles.

Human, financial and technical resources

Q41: How many persons (in full time equivalents) in your DPA (respectively EDPB Secretariat) work on issues that fall within the scope of the LED specifically?

	Number (FTE)	%
* 2017	33,3	The percentage varies from less than five to approximately 15 for the respective DPAs
* 2018	33,95	see above
* 2019	40,52	see above
* 2020	47,0	see above
* 2021	53,31	see above

* **Q42: How would you assess your DPA's resources for its work on the LED from a human and financial point of view?**

- ○ Sufficient
- ◉ Insufficient

Q42.1: Please explain why the resources are insufficient:

Q42 cannot be answered by "yes" or "no", as the assessment is made by each DPA individually, based on their individual ressources. Some DPA consider their ressources as sufficient, some consider them as insufficient.

Those DPAs that assessed their ressources as insufficient reportet a lack of resources to carry out inspections in regular timely intervals and on from own initiative.

* **Q43: Do you face any specific challenges when supervising competent authorities in terms of expertise (criminal law / technical / IT) and IT resources?**

- (●) Yes
- ( ) No

* **Q43.1: what are the challenges you are facing?**

- [ ] 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
- [x] Others challenges

* **Q43.1.6: Other challenges - please specify.**

Two authorities pointed out difficulties in auditing and evaluating complex IT procedures.

Horizontal questions

* **Q44: In your opinion, what has been the main impact(s) of the transposition of the LED in your Member State?**

The main impacts can be summarised as follows: Although the corrective powers required under Article 47 LED have not yet been sufficiently implemented in federal law as well as some state law (see Section 1 above), the implementation of the LED has resulted in an increase in powers for most supervisory authorities. In certain cases, the supervisory authorities have the power to issue orders. Some DPAs report, that the significant increase in remedial powers and their quality (enforceable for the first time) has gained them significantly more respect from responsible bodies. Their statements have gained more weight and their advice is often (more) followed, as otherwise consequences threaten for the first time. This constitutes an improvement compared to the legal situation prior to the LED.
With the LED and its implementation, the fundamental principles and concepts for the transfer of personal data to third countries were transferred to the area of law enforcement for the first time. As a result, the issue of third country transfers has received significantly more attention.
With the transposition of the LED the security of processing has been enhanced because of the higher standards with regards to security measures, especially the conduction of data protection impact assessments and the notification of data breaches. The supervisory authorities became more involved on the part of the responsible bodies in the context of data protection impact assessment and the obligation to be consulted that goes hand in hand with it in some cases. At the same time, this has led to greater awareness on the part of the responsible bodies with regard to the assessment of risks to the rights and freedoms of the data subjects.
The implementation of the LED also led to a strengthening of the rights of the data subjects.

* **Q45: Have you identified any specific challenges regarding the application of the LED in relation to new technologies? Please explain?**

- (●) Yes
- ( ) No

* **Q45.1: Please explain.**

The use of AI is also being researched and tested in the area of law enforcement. For example, AI is being used to predict where and what type of crimes are likely to occur (predictive policing and crime hotspot analytics). The assessment of such and other conceivable use case scenarios raises various challenges for data protection supervisory authorities. This concerns, for example, the requirements for transparency of AI-supported processes and algorithms. Only if it is comprehensible how an AI system operates and generates its outcomes, the risk of its application can be assessed. Thus, the transparency of AI systems is essential. However, it is unclear whether and by what means transparency can be ensured in a sustainable and permanent manner. The issue of transparency also applies in the context of the data controller's information obligations vis-à-vis data subjects. It is also questionable how other data protection principles, such as the principles of data minimization and purpose limitation, impact the use of AI in law enforcement, respectively how the legal boundaries for the use of AI are to be drawn in this regard.

* **Q46: Have you identified any important problems regarding the transposition of the LED in your Member State?**

- (●) Yes
- ( ) No

* **Q46.1: Please explain.**

Several DPA refer to the corrective powers that have not been fully implemented in the federal law and some state laws:

The powers to order the controller or processor to bring processing into compliance (including rectification, erasure and restriction) (Art. 47(2)(b) LED) are not implemented in the following States / Federal level:

Federal Law (partially)
Bavaria
Berlin
Lower Saxony
Mecklenburg-West Pomerania
Thuringia

The powers to impose a temporary or definitive limitation, including a ban, on processing (Art. 47(2)(c) LED) are not implemented in the following States / Federal level:

Federal Law (partially)
Baden-Wuerttemberg (Police sector, see Q7)
Bavaria
Berlin
Brandenburg
Lower Saxony
Hesse
Mecklenburg-West Pomerania
North Rhine-Westphalia
Schleswig-Holstein
Thuringia

For further details see the comments to Q6 and Q 7.1 above.

* **Q47: Is there anything else you would like to mention relevant for the LED evaluation that is not covered in this questionnaire?**

- (●) Yes
- ( ) No

* **Q47.1: Please specify.**

Concerning the LED:

The LED is applicable to the area of “prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties”. This wording still harbours uncertainty for the exact scope of the LED; not just from the perspective of the data subject but also from the view of a practitioner or lawmaker. Since there are many cross-sectional matters it is sometimes unclear which authorities and which activities actually fall within the scope of the directive and which legal texts have to be changed or created to fully transpose the LED into national law.

Concerning the response to this questionnaire:
Please not, that the responses do not always apply to every german DPA as the DPAs.
In addition, not all responses include feedback from all supervisors:
- The responses to the powers, Q1-Q9, to Cooperation, Q39-40, and to the Horizontal Questions, Q44-Q47, include the feedback from all 17 DPAs.
- The responses to Q10-Q38 include the feedback from 16 DPAs.
- The responses to Q41-43 include the feedback from 15 DPAs.