

**Contribution of the EDPB to the European Commission's
evaluation of the Data Protection Law Enforcement**

Directive (LED) under Article 62

Adopted on 14 December 2021

Table of contents

- 1 GENERAL EDPB POLICY MESSAGES3
- 2 EDPB WORK ACCORDING TO THE TASKS LISTED UNDER ARTICLE 51 LED6
- 3 SYNTHESIS OF REPLIES TO THE QUESTIONNAIRE BY EDPB MEMBERS7
 - 3.1 Powers of SAs7
 - 3.2 Complaints from data subjects 10
 - 3.3 Consultations and advisory powers of SAs..... 12
 - 3.4 Awareness-raising, training and guidance 13
 - 3.5 Data breach notifications 14
 - 3.6 Powers pursuant to Article 47 (5) LED..... 15
 - 3.7 International transfers 16
 - 3.8 Judicial review of decisions taken by SAs..... 17
 - 3.9 Cooperation between SAs 17
 - 3.10 Human, financial, and technical resources of SAs 18

The European Data Protection Board

Having regard to Articles 51(1)(a)(b) and (h) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

HAS ADOPTED THE FOLLOWING CONTRIBUTION TO THE EUROPEAN COMMISSION'S EVALUATION OF THE DATA PROTECTION LAW ENFORCEMENT DIRECTIVE (LED) UNDER ARTICLE 62:

1 GENERAL EDPB POLICY MESSAGES

1. Together with the GDPR, the LED constitutes a key component of the overarching data protection framework in the European Union. The LED establishes for the first time a set of Europe-wide data protection rules for national domestic data processing operations in the area of law enforcement. Previously, EU legal instruments in this area have been limited to data protection rules for EU agencies, large scale IT systems established under EU law or cross-border exchanges of personal data in the framework of police and judicial cooperation in criminal matters.¹ The EDPB underlines the importance and high added value of this approach to introduce a dedicated legislative act aiming at a higher and more harmonized level of data protection also in the area of law enforcement. In the view of the EDPB, the LED may serve as a starting point to set a standard also beyond the borders of the EU, like the GDPR already does today.
2. In order to regulate data processing in the area of law enforcement, the EU legislator adopted a directive to aim in principle at a minimum harmonisation and complement existing instruments of EU law. The transposition of the LED into national law, which required amending numerous acts of law, has been subject to delays in several Member States. On 5 May 2016, the LED entered into force. According to Article 63 paragraph 1 LED, Member States had to adopt and publish the laws, regulations and administrative provisions necessary to comply with the LED by 6 May 2018. More than three years later, this transposition has not been fully completed in all Member States. This should be taken into account by the Commission when evaluating the responses to the questionnaire. The EDPB strongly urges those Member States still in the phase of the implementation to invest all means possible to ensure that the transposition is fully compliant with the LED without any further delays.
3. The EDPB welcomes that the EU legislator provided for regular evaluations of the application and the functioning of the LED, to be conducted by the Commission every four years. Undertaken comprehensively and thoroughly, evaluations of acts of law can have a considerable positive impact on the quality of legislation. The EDPB is dedicated to contributing to this important task.
4. Taking into account that the past four years have been characterised primarily by the national processes to transpose the LED and that case law is only starting to be developed the EDPB considers that, in practice, it is a relatively early stage for a comprehensive evaluation of the implementation and application of the provisions of the Directive as transposed. Moreover, because of the recent

¹ Council Framework Decision JHA/2008/977.

implementation of the LED, on some parts of the LED, there is only limited experience and empirical data, differing across Member States. Therefore the EDPB recalls that it would be too early to draw conclusions on the effectiveness of this legal instrument and to even consider any revision of the LED at this stage.

5. Consistency and harmonisation have been key objectives of the EU data protection reform. In this context, the adoption of the LED and Chapter VII and IX of Regulation (EU) 2018/1725 have been important steps towards a comprehensive alignment of the data protection framework in the field of law enforcement and criminal justice, both at national and Union level. This is a continuous process, during which the divergences, that create legal fragmentation of the data protection legislation in the Union, have to be identified and properly addressed.
6. The LED aims at the harmonisation of the protection of personal data and by that also at supporting the possibility of the cooperation of police authorities by way of exchange of personal data. Along comes the need for bilateral and multilateral cooperation of national supervisory authorities (SAs). This need is amplified by the trend for constant cross-border interconnection of databases, the interoperability regulations only being one of many projects in this regard. As foreseen in Chapter VII of the LED, the EDPB underlines the need for close cooperation between the Member States' SAs within the EDPB.
7. In many regards, some of the LED provisions are formulated in a general manner as they are the result of a compromise between different policy interests and perspectives which have found expression during the legislative process. As a result, some legal provisions of the LED may lead to different interpretations and present a particular challenge for the work of the EDPB, such as the scope of the LED and the powers of supervisory authorities.
8. The contributions of the EDPB in recent years have focused especially on the GDPR, as the need for guidance was initially greater due to its direct applicability. The evaluation of the LED is welcomed as it may also show the areas in which more guidance is needed. In this regard, the EDPB commits to further contribute to provide guidance on the interpretation of the LED by issuing guidelines, recommendations and best practices, where necessary, and it would like to take this opportunity to point out what contributions it considers as priorities in the near future.
9. The EDPB will elaborate and give guidance on the concept of sufficient investigative and corrective powers as used in Article 47 LED. This guidance could support Member States and SAs to evaluate whether national laws effectively provide for sufficient investigative and corrective powers, which are key to properly enforce the LED, ensure a consistent application of the LED across the EU and comply with Article 8(3) of the EU Charter of Fundamental Rights.
10. Today criminal investigations increasingly involve the collection and analysis of large and complex datasets, which may necessitate new IT tools. In this regard it is understandable that the law enforcement authorities, both at Union and national level, intend to benefit from the best possible legal and technical instruments to accomplish their tasks. While digital tools like AI may contribute to the greater efficiency and effectiveness of combatting serious crime, their use in the law enforcement and criminal justice sector remains highly sensitive and should be subject to strict conditions and safeguards, notably those resulting from the full and correct transposition and effective application of the LED.
11. Therefore, the EDPB sees the great need to provide further guidance in order to ensure the use of emerging new technologies by law enforcement authorities be in compliance with the Charter of Fundamental Rights and the LED. In this respect, the EDPB will publish in 2022 guidelines on the use of

facial recognition technologies by law enforcement authorities. In addition to the comments already provided on the Commission's proposal for a regulation on the use of AI, the EDPB will continue to follow this important piece of legislation and may provide additional guidance.

12. Another key aspect is the legal framework for the cooperation with law enforcement authorities in third countries and with international organisations. The promotion of high data protection standards will thus constitute one of the essential elements of the future EDPB work, while at the same time recognising, also in practice, that there are legitimate needs for the international cooperation of law enforcement authorities. The EDPB has already provided guidance on the adequacy assessment of the level of data protection in third countries and international organisations pursuant to Article 36 LED.² In addition, the EDPB is currently working on guidelines on the interpretation of Article 37 LED on transfers subject to appropriate safeguards.
13. The EDPB recognises that adequacy decisions are an important tool to ensure the continuous protection of personal data transferred from the European Union to third countries and international organisations. Therefore the EDPB encourages the Commission to actively pursue possibilities for adoption of adequacy decisions for third countries/international organisations provided they meet the criteria. The EDPB welcomes the interest of third countries to engage with the EU in the context of an adequacy decision. The EDPB remains committed to providing independent assessments of the tools developed by the European Commission with regard to the requirements of LED, especially enforceable rights, effective redress and safeguards concerning onward transfers. The EDPB considers these assessments to be of the utmost importance. The EDPB will participate in the evaluation of current adequacy decision and the adoption of future ones.
14. The EDPB wishes to underline the fact that the effective implementation of the tasks under the LED requires the availability of the necessary resources - both human and technical. Yet, the majority of EDPB members have not received sufficient human, financial and technical resources to deal with LED-related issues. New legislative and technological developments in the processing of data for law enforcement purposes have increased the workload of EDPB members in volume and complexity. Also, DPAs may often have to balance their resources between supervision of the GDPR and the LED. EU Member States should ensure that the resources of SAs increase in proportion to their workload to allow them to fulfil their mandate to protect the rights of data subjects and closely follow any developments in this regard. Even more crucial than the number of available staff, are the skills of the experts, who should cover a very broad range of issues - from criminal investigations and police cooperation to big data analytics and AI. This necessarily has an impact on the work of the EDPB. It should be noted that the EDPB is to a large extent dependent on the resources of the Member States and in its day to day work, the most limiting factor is the availability of staff to take over the work packages connected with the drafting of guidelines, recommendations and best practices.

² See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021
https://edpb.europa.eu/sites/edpb/files/files/file1/recommendations012021onart.36led.pdf_en.pdf

2 EDPB WORK ACCORDING TO THE TASKS LISTED UNDER ARTICLE 51 LED

15. The EDPB has focused its work since its creation on 25 May 2018 especially on the GDPR. Some of its work in this regard touched upon the collection and processing of data from entities subject to the GDPR by law enforcement authorities, inside the EU and abroad. The EDPB issued statements, contributions and guidance on matters such as the collection of Passenger Name Records (PNR)³, the Terrorist Finance Tracking Programme (TFTP)⁴, the Budapest Convention on Cybercrime⁵, facial recognition⁶, and government access to data for law enforcement and security purposes.⁷
16. More specifically under the LED, the EDPB began providing guidance on data transfers by publishing an adequacy referential⁸ to assist the European Commission in assessing the level of protection of personal data in third countries and international organisations in the framework of its adequacy decisions pursuant to Article 36(3)LED. This guidance may also serve as reference to third countries and international organisations interested in obtaining adequacy. The EDPB relied subsequently on this guidance for its opinion on the draft decision of the European Commission on the adequacy of the United Kingdom under the LED.⁹
17. The EDPB has also produced guidance and statements on EU instruments other than the LED governing the processing of data by competent authorities via specific frameworks¹⁰ and police and judicial cooperation.¹¹ One of the main tasks of the EDPB under the LED is to promote cooperation and the exchange of information and best practices among its members.¹² To this end, the EDPB also established via its rules of procedure (Title VII)¹³ the Coordinated Supervision Committee (CSC) that is progressively assuming the task of coordinating supervision between the EDPS and the EDPB members

³ [EDPB letter](#) to the European Commission, 22 January 2021; [EDPB letter](#) to MEP Sophie in't Veld, 9 October 2019.

⁴ [EDPB letter](#) to MEP Moritz Körner, 3 December 2020.

⁵ [EDPB's contribution](#) to the consultation on a draft second additional protocol, 4 May 2021; [EDPB statement](#) 02/2021, 2 February 2021; [EDPB contribution](#) to the consultation on a draft second additional protocol, 13 November 2019.

⁶ [EDPB-EDPS Joint Opinion](#) on the Artificial Intelligence Act, 18 June 2021; [EDPB letter](#) to MEP in't Veld, 10 August 2021; [EDPB letter](#) to MEP Sophie in't Veld, Moritz Körner, Michal Šimečka, Fabienne Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI, 10 June 2020.

⁷ [EDPB Opinion](#) 32/2021 on the draft adequacy decision on South Korea under the GDPR, 24 September 2021; [EDPB Recommendations](#) 01/2020 on supplementary measures, 18 June 2021; [EDPB opinion](#) 14/2021 on the draft adequacy decision on the United Kingdom under the GDPR, 13 April 2021; [EDPB Recommendations](#) on European Essential Guarantees for surveillance measures, 10 November 2020; [EDPB pleading before the CJEU](#) in the case Schrems II, 17 July 2019; [EU-U.S. Privacy Shield Third Joint Annual Review Report](#), 12 November 2019 and [Second Joint Annual Review Report](#), 22 January 2019; [EDPB letter](#) to MEPs Sophie in't Veld and Moritz Körner on the US-UK agreement under the US Cloud Act, 15 June 2020; [EDPB-EDPS Joint response to the LIBE Committee on the Impact of the US Cloud Act](#), 12 July 2019.

⁸ [Recommendations 01/2021](#) on the adequacy referential under the Law Enforcement Directive, 2 February 2021.

⁹ [EDPB opinion](#) 15/2021 on the draft adequacy decision on the United Kingdom under the LED, 13 April 2021.

¹⁰ [EDPB letter](#) to MEPs on the expansion of the Prüm Framework, 28 July 2020.

¹¹ [EDPB letter](#) to Chairman of the LIBE Committee on the Interoperability Regulations, 13 November 2019.

¹² Article 51(1)(h)LED

¹³ [EDPB Rules of Procedure](#), 8 October 2020.

over EU Large scale information systems and agencies processing law enforcement data or data of interest to law enforcement. The EDPB prepared the CSC's entry into operation in December 2019.

3 SYNTHESIS OF REPLIES TO THE QUESTIONNAIRE BY EDPB MEMBERS

18. The European Commission addressed to the EDPB and to the national data protection supervisory authorities a questionnaire for its evaluation and review of the LED, in accordance with Article 62. This questionnaire examines aspects relevant to the national data protection supervisory authorities (SAs), including their powers under national law transposing the LED and experience in using them, their experience dealing with complaints from data subjects, their exercise of consultation and advisory powers, their awareness-raising activities and trainings, and their experience with international transfers. The questionnaire also analyses the cooperation between SAs both bilaterally and via the EDPB. The resources available to SAs for the supervision of data protection in the area of law enforcement are also a relevant question, since the effective fulfilment of their mandate largely depends on them. Finally, the SAs use this opportunity to provide their insights on the effectiveness and challenges found in the implementation of the LED in their respective EU Member States.
19. In addition to the general policy messages above, the EDPB would like to provide below a synthesis of the contributions and replies by its members to each of the questions asked via the Questionnaire on the Evaluation of the LED sent by the European Commission. The questionnaire was not addressed to the European Data Protection Supervisor (EDPS), since the LED does not apply to the processing of personal data by the Union institutions, bodies, offices and agencies that the EDPS supervises, in accordance with Article 2(3)(b) LED.
20. This synthesis is based on the information provided by the EDPB membership for LED-related matters, which is limited to the national supervisory authorities of the 27 EU Member States. The 4 EFTA countries: Iceland, Liechtenstein, Norway and Switzerland apply the LED as part of the Schengen *acquis*, and are observers to the EDPB on LED related matters.
21. This synthesis considers the consolidated replies provided at national level. Notwithstanding, due to a federal structure and/or internal division of labour, the SAs competent for LED-related matters in some EU Member States, such as Germany and Belgium, have had diverse experiences in applying (different) national legislation to implement the LED.

3.1 Powers of SAs

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

22. Although a majority of the SAs consider that the LED did strengthen their investigative and corrective powers, 8 of them consider that it did not. One of them argues that the new law transposing the LED reduced the investigative and corrective powers it had previously under a general data protection law, which also applied to the law enforcement sector, although the SA makes a broad interpretation of the scope of the powers received.

Q2: Please list your investigative powers

23. All the SAs replied that they have the power under national law to obtain from the controller and the processor access to all personal data and to all information necessary for the performance of their tasks. Most of them also have the power 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. The majority of them also have the power to carry out investigations in the form of data protection audits. Several SAs specify having additional powers, such as the right to obtain free of charge information from entities other than the controller and the processor, the right to seize documents and extracts of data from IT systems, and the right to obtain from controllers and processors other forms of assistance for the performance of their tasks.

| SA | Corrective Powers | | | |
|----|---|---|---|-------|
| | To obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks | 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 | To carry out investigations in the form of data protection audits | Other |
| LU | ✓ | ✗ | ✗ | ✗ |
| CY | ✓ | ✓ | ✓ | ✓ |
| NL | ✓ | ✓ | ✓ | ✓ |
| DE | ✓ | ✓ | ✓ | ✗ |
| EE | ✓ | ✓ | ✓ | ✓ |
| IE | ✓ | ✓ | ✓ | ✓ |
| BG | ✓ | ✓ | ✓ | ✗ |
| PT | ✓ | ✗ | ✗ | ✗ |
| IT | ✓ | ✓ | ✗ | ✓ |
| FI | ✓ | ✓ | ✓ | ✗ |
| PL | ✓ | ✓ | ✓ | ✗ |
| ES | ✓ | ✓ | ✓ | ✓ |
| SI | ✓ | ✓ | ✓ | ✗ |
| HU | ✓ | ✓ | ✗ | ✗ |
| AT | ✓ | ✓ | ✓ | ✗ |
| CZ | ✓ | ✓ | ✓ | ✗ |
| DK | ✓ | ✓ | ✓ | ✗ |
| SK | ✓ | ✗ | ✓ | ✓ |
| FR | ✓ | ✓ | ✓ | ✓ |
| SE | ✓ | ✓ | ✓ | ✓ |
| BE | ✓ | ✓ | ✓ | ✗ |
| HR | ✓ | ✗ | ✗ | ✓ |
| LT | ✓ | ✓ | ✓ | ✗ |
| LV | ✓ | ✓ | ✓ | ✗ |
| RO | ✓ | ✓ | ✓ | ✗ |
| EL | ✓ | ✓ | ✓ | ✗ |
| MT | ✓ | ✓ | ✗ | ✗ |

Q3: Do you consider your investigative powers effective?

24. Almost all SAs, save for one, consider effective the investigative powers they have received by national law transposing the LED. However, some SAs refer to the fact that, due to the exemption laid down in Article 45(2) LED, they are prevented from supervising courts and other independent judicial authorities when acting in their judicial capacity.

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

25. Although the majority of SAs do not report difficulties in applying their investigative powers, several SAs note some difficulties, such as the absence of identification of the controller, incomplete information received from competent authorities, disagreement with competent authorities on the

scope of the SA's mandate and investigative powers, and practical difficulties such as obtaining appropriate security clearance to access classified information.

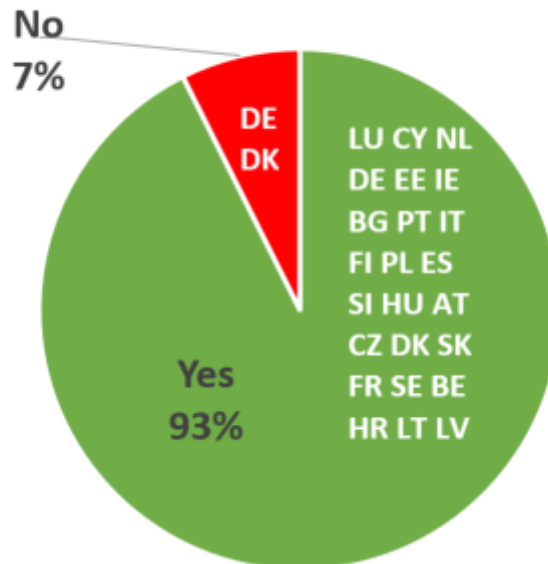
Q5: Have you conducted investigations and/or inspections on your own initiative or only on the basis of complaints?

26. The majority of SAs report having conducted investigations and/or investigations both on their own initiative and on the basis of complaints received from data subjects.

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

27. Almost all SAs, save for 2, have all the powers listed under Article 47(2)(a), (b – including rectification, erasure, restriction) and (c) of the LED. Regarding the SAs that do not have all the powers listed under Article 47(2) LED, one of them lacks the power to issue warnings under Article 47(2)(a) LED, and the other one lacks the power to order the controller to bring processing into compliance (including rectification, erasure and restriction) under Article 47(2)(b) LED, as well as the power to impose a temporary or definitive limitation, including a ban, on processing under Article 47(2)(c).

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



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

28. A majority of SAs report having the same corrective powers towards all enforcement authorities. Some SAs specifically point out that they do not have the same corrective powers towards courts and public prosecutor's offices (in accordance with national law transposing Article 45(2) LED), as well as towards intelligence agencies acting on issues relevant to law enforcement, and some specific types of data held by the police, such as data on informants, undercover agents, and protected witnesses.

Q8: Do you consider your corrective powers effective?

29. The vast majority of SAs, save for 3, consider their corrective powers effective. Some of them note that it may be too early to assess this given the recent date of transposition of the LED into national law in their countries.

Q9: Have you used your corrective powers?

30. A majority of SAs have used their corrective powers under the LED. A few SAs have not exercised them to date mainly due to a lack of complaints received or the fact that they did not find systemic infringements of data protection law found in the course of their inspections of competent authorities. SAs report a limited number of cases of exercise of these powers in relation to the EU large-scale information systems SIS II and VIS. Competent authorities or processors complied with the decisions issued by the SAs in the exercise of these powers, save in two cases.

| Country | Number of cases related to the supervision of - SIS II and VIS | | | Number of other cases NOT related to the supervision of SIS II and VIS | | |
|---------|---|--------------|--------------|--|--------------|--------------|
| | Art.47(2)(a) | Art.47(2)(b) | Art.47(2)(c) | Art.47(2)(a) | Art.47(2)(b) | Art.47(2)(c) |
| BE | 1 | 3 | - | 3 | 18 | 1 |
| BG | - | - | - | - | 9 | - |
| DE | - | - | - | 7 | 7 | - |
| DK | - | 2 | - | - | 25 | - |
| EE | - | - | - | 5 | - | - |
| ES | - | - | - | - | - | - |
| FI | - | - | - | 2 | 2 | - |
| FR | - | - | - | - | 7 | - |
| HU | - | - | - | - | 3 | - |
| IE | - | - | - | - | 3 | 3 |
| IT | - | - | - | 1 | 3 | - |
| LT | - | - | - | - | 1 | - |
| MT | 1 | - | - | 2 | - | - |
| NL | - | 2 | - | - | - | - |
| PL | - | - | - | 3 | 13 | - |
| SE | - | - | - | - | 7 | - |
| SI | - | - | - | - | 1 | - |

3.2 Complaints from data subjects

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

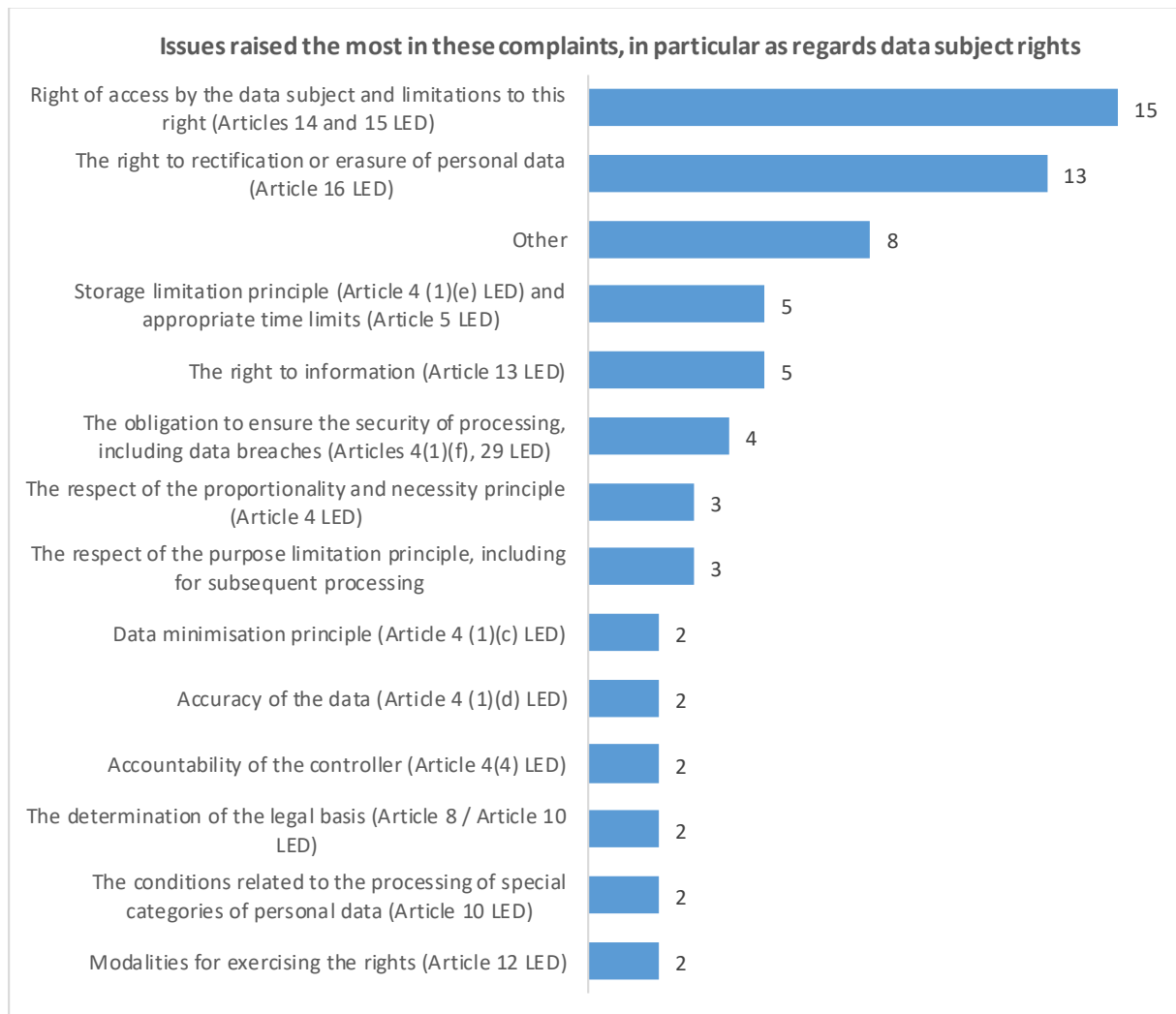
31. More than a third of the SAs report an increase in the number of complaints received following the transposition of the LED in their Member States.

Q11: Indicate the issues raised the most in these complaints, in particular as regards data subject rights?

32. The issues raised in the complaints made to some SAs are diverse. The highest number of complaints concerned the right of access by the data subject and limitations to this right (Articles 14 and 15 LED) and the right to rectification or erasure of personal data (Article 16 LED). Other issues raised to a lesser

extent were, by decreasing order, the storage limitation principle (Article 4(1)(e) LED) and appropriate time limits (Article 5 LED), the right to information (Article 13 LED); the modalities for exercising the rights of data subjects (Article 12 LED); the obligation to ensure the security of processing, including data breaches ((Articles 4(1)(f), 29 LED); the respect of the principles of purpose limitation (Article 4(1)(b) LED), data minimisation (Article 4(1)(c) LED), the accuracy of the data (Article 4(1)(d) LED), the accountability of the controller (Article 4(4) LED), the determination of the legal basis (Article 8), the conditions related to the processing of special categories of personal data (Article 10 LED); and others such as unauthorised accesses of police data bases and use of personal data.

[Note: the figures below reflect the number of SAs having received complaints on each specific issue]



Q12: Are you following up on all complaints?

33. A majority of the SAs are following-up on all complaints. Some SAs report that they do not follow up on all complaints received because of organisational, technical and human resource constraints. In addition, some SAs indicate that they have cases where they cannot make a decision on the substance due to formal and procedural deficiencies of the complaint.

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

34. 4 SAs have received complaints by organisations representing data subjects under Article 55 LED.

3.3 Consultations and advisory powers of SAs

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

35. Half of the SAs utilized the prior consultation procedure in accordance with Article 28 (1)(a) or (b) LED. In this context, most SAs that were consulted by competent authorities provided written advice and/or used their corrective powers pursuant to Article 28 (5) LED.

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

36. Two SAs have established a list of processing operations subject to prior consultation pursuant to Article 28 (3) LED.

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

37. All SAs are consulted by their national parliaments/governments during the preparation of legislative or other regulatory measures with a data protection dimension. The majority of SAs are consulted systematically, whereas several SAs only occasionally.

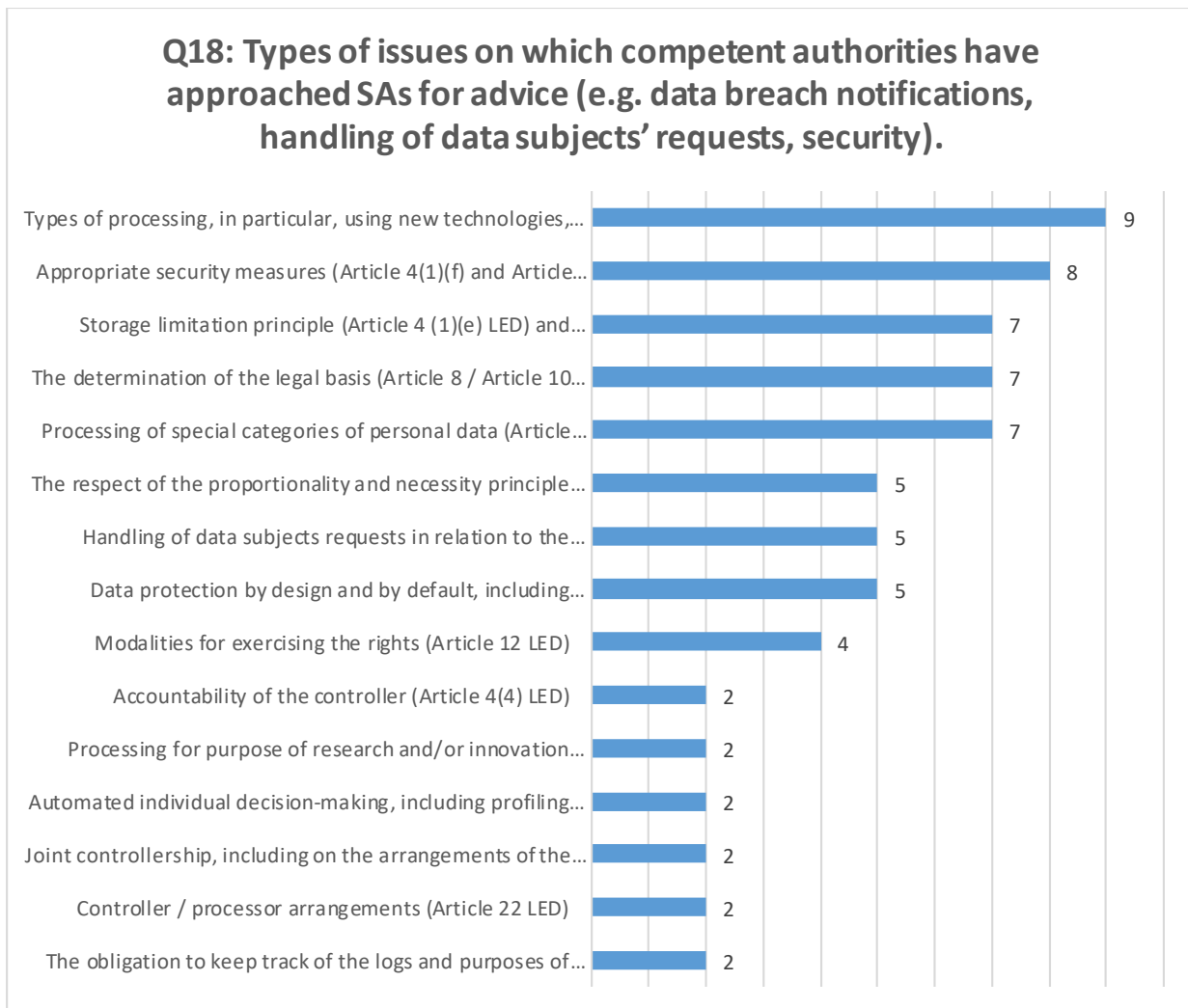
Q17: How many opinions under Article 47(3) LED, other than prior consultations pursuant to Art 28(1) LED, have you issued upon request or on your own initiative?

38. The number of opinions that SAs have issued under Article 47 (3) varies significantly among them, ranging from 0 to 338 opinions. The figures provided also depend on the interpretation given at national level of the term “opinion” under Article 47 (3) LED. Some SAs do not keep specific statistics on the number of opinions issued under Article 47 (3) LED.

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).

39. The most common type of issue on which competent authorities approached SAs for advice was specific types of processing, in particular, using new technologies, mechanisms or procedures (Article 27 / Article 28 (1)(a) LED), closely followed by appropriate security measures (Article 4 (1)(f) and Article 29 LED); the processing of special categories of personal data (Article 10 LED); the determination of the legal basis (Articles 8 and 10 LED); the storage limitation principle (Article 4 (1) (e) and appropriate time limits (Article 5 LED).
40. To a lesser extent, competent authorities also approached SAs for advice on the following issues, by decreasing order: the handling of data subjects requests in relation to the exercise of their rights (Chapter III LED); respecting the proportionality and necessity principle (Article 4 LED); data protection by design and by default, including anonymisation and pseudonymisation (Article 20 LED); modalities for exercising the rights (Article 12 LED); Controller / processor arrangements (Article 22 LED); automated individual decision-making, including profiling (Article 11 LED); processing for purposes of research and/or innovation (Article 9(2) LED); accountability of the controller (Article 4(4) LED); joint controllership, including on the arrangements of the joint controllers’ responsibilities (Article 21 LED); the obligation to keep track of the logs and purposes of processing regarding the logs (Article 25 LED); and others, such as transfers to third countries, notification of data breaches, the role and status of DPOs under the LED, and the supervision of the processing of data by judicial authorities.

[Note: the figures below reflect the number of SAs having been approached on each specific issue]



3.4 Awareness-raising, training and guidance

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

41. A majority of SAs have issued guidance and / or practical tools supporting competent authorities or processors to *comply with their obligations*. The guidelines covered the following topics: assisting the judiciary, offices of the prosecutor, and police authorities in complying with the principle of accountability; exchanging personal data with the police; appointing a data protection officer; processing data in crime areas such as organised crime and terrorism; records of processing activities and logging; video surveillance; information to data subjects; notification of data breaches; obligations of controllers; and the exercise of rights by individuals.

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

42. A majority of SAs have provided training to or carried out awareness-raising activities for competent authorities and / or processors, including their DPOs. These trainings covered topics including data processing by the police, prosecution offices, judicial and correctional authorities; delimitation of areas of application between the GDPR and the LED; use of personal data from social media networks;

processing of data in police files; video surveillance techniques and big data; handling of data subject rights; and processing prisoners' personal data.

3.5 Data breach notifications

Q21: How many data breach notifications have you received?

43. The fact that several SAs do not keep separate statistics on data breach notifications under the LED makes it difficult to provide accurate figures. The number of data breach notifications received varies greatly across countries, ranging from 0 to over 500 depending on factors such as the size of their population.

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

44. As mentioned above, several SAs do not keep statistics on this matter. 6 SAs that have received data breach notifications under the LED and keep statistics, report that they have followed up with investigations in all the cases, and 5 in no case.

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

45. As mentioned above, several SAs do not keep statistics on this matter. Most of the SAs that have received data breach notifications under the LED and keep statistics report that they have not advised or ordered competent authorities to take measures mitigating the risks. One SA has advised or ordered competent authorities to take measures mitigating the risks in all the cases.

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? (%)

46. Several SAs indicate that they do not keep statistics on the application of Article 13(3) LED. Most of the SAs that have received data breach notifications under the LED and keep statistics report that they have no cases in which the communication to the data subject has been delayed, restricted or omitted on the grounds set out in Article 13(3) LED, and only 1 SA reports that communication to the data subject has been delayed, restricted or omitted on this ground in all the cases.

3.6 Powers pursuant to Article 47 (5) LED

Q25: Have you exercised your power to: - bring infringements of your national law(s) transposing the LED to the attention of judicial authorities? - commence or otherwise engage in legal proceedings?

47. 3 SAs report that they have exercised their power to bring infringements of their national law(s) transposing the LED to the attention of judicial authorities. 4 SAs have exercised their power to commence or otherwise engage in legal proceedings.

Q26: Did you face difficulties in exercising this power?

48. Almost all SAs, save for 1, have not faced any difficulties in exercising their power pursuant to Article 47(5) LED. However, 2 SAs report that Article 47 (5) LED has not been transposed into their national law.

Q27: How many requests under Article 17 LED have you received? What were the outcomes of the cases?

49. Some SAs do not keep statistics on the matter. Approximately half of the SAs that do keep statistics report that they have received requests under Article 17 LED. The number of requests received by SAs ranges from 1 to 1553.
50. The outcomes of these requests were diverse. In most cases, the SAs informed the data subject that all necessary verifications or a review had been conducted and/or had declared the request inadmissible. In several cases, the controller was ordered to rectify or erase the personal data, or to restrict the processing of personal data. The SAs also report cases in which all or some of the requested data was provided to the data subject, as well as cases in which the controller was ordered to provide full or partial access to the personal data. One SA reports that they applied corrective powers, namely a ban on processing of video surveillance with facial recognition and of video surveillance and audio recordings.

Q28: Did you encounter any particular problems?

51. Most SAs do not report any particular problems. One SA explains that, as a consequence of the LED transposition into their national law, the modalities for the exercise of rights with regards to the majority of the above-mentioned cases have changed. Since the data controller has become the first contact point for the data subjects, numerous complaints, previously handled by the SA, have been transferred to another authority.¹⁴ However, the legal or regulatory provisions governing the exercise of rights have not been fully updated and the change of regime is not well known to the data subjects. The same SA also reports difficulties arising when files are covered by both the LED and other national provisions, in particular in relation to national security. In such cases, in order to exercise their rights with regard to all the data recorded in the same file, data subjects are required to initiate two parallel procedures (one for data related to national security and one for other data), which makes the exercise of their rights more complex. Another SA reports that, Article 17 LED has not been transposed into their national law. As a result, this SA had to apply general administrative law in order to reach a decision on the data subject's request.

¹⁴ However, it is relevant to underline that more than one third of the SAs report an increase of the number of complaints - see Question 10.

3.7 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?

52. One SA has encountered a case where a controller transferred personal data based on a on a 'self-assessment' pursuant to Article 37(1)(b) LED.

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?

53. One SA has carried out an investigation into data transfers based on derogations under Article 38 (1) LED.

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

54. One SA has received information about a data transfer based on the derogations found in Article 39(1) LED. One of these cases raised issues of non-compliance with the requirements set out in this Article.

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?

55. Over one third of the SAs have carried out activities to promote the awareness of controllers/processors with respect to their obligations under Chapter V of the LED.

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)?

56. Over one third of the SAs have exercised advisory powers towards the government and/or competent authorities on data transfers under Chapter V of the LED. A few of them issued guidelines, recommendations and/or best practices

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?

57. 5 SAs have provided assistance to Member States in assessing and, where necessary, reviewing their international agreements involving international data transfers that were concluded prior to 6 May 2016, which remained unaffected pursuant to Article 60 of the LED.

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?

58. 3 SAs have received/handled complaints specifically addressing the issue of data transfers.

Q36: Have you exercised your investigative and/or enforcement powers with respect to data transfers?

59. 3 SAs have exercised their investigative and/or enforcement powers with respect to data transfers. One of them imposed consequently limitations on data transfers.

Q37: Have there been cases in which you have cooperated with foreign data protection authorities (for instance, exchange of information, complaint referral, mutual assistance)

60. 6 SAs cooperated with foreign data protection authorities. Among these, 4 could rely on existing mechanisms for this cooperation.

3.8 Judicial review of decisions taken by SAs

Q38: Have data subjects / competent authorities / processors contested your decisions (or inaction) before national courts?

61. Data subjects contested decisions (or inaction) of SAs before national courts concerning national legislation transposing the LED in almost half of the SAs. The outcomes of these legal actions were diverse, with some complaints declared inadmissible, some decisions by SAs upheld, and others being overturned or referred back to SAs. Some of these judicial proceedings were pending at the time the SAs answered the questionnaire.
62. In two cases, Courts upheld the SA's decision to impose administrative fines on competent authorities. In another case, a SA filed an appeal against a Court's decision overturning its decision. The SA argued in its appeal that the national criminal procedural law does not always take precedence over the national data protection provisions implementing the LED, and that the latter needed to be taken into account when interpreting the former. In another case, one SA issued an order against the local police asking it to delete a biometric database created by them containing templates of likely thousands of citizens. The competent authority filed an action against the order, which an administrative court overturned. The SA lodged an appeal against that judicial decision that is still pending.

3.9 Cooperation between SAs

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

63. 6 SAs have used the mutual assistance tool foreseen under Article 50 LED. Some SAs do not keep specific statistics on requests for mutual assistance transmitted under Article 50 LED. One SA noted that the Internal Market Information System (IMI) that is currently used for cooperation between SAs under Article 61 of the GDPR is not tailored specifically to the provision of mutual assistance under Article 50 LED. However, the same SA confirms that formal requests for mutual legal assistance under Article 61 LED are rare and that SAs usually resort first to informal requests for cooperation to avoid triggering unnecessarily legal deadlines and effects.

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

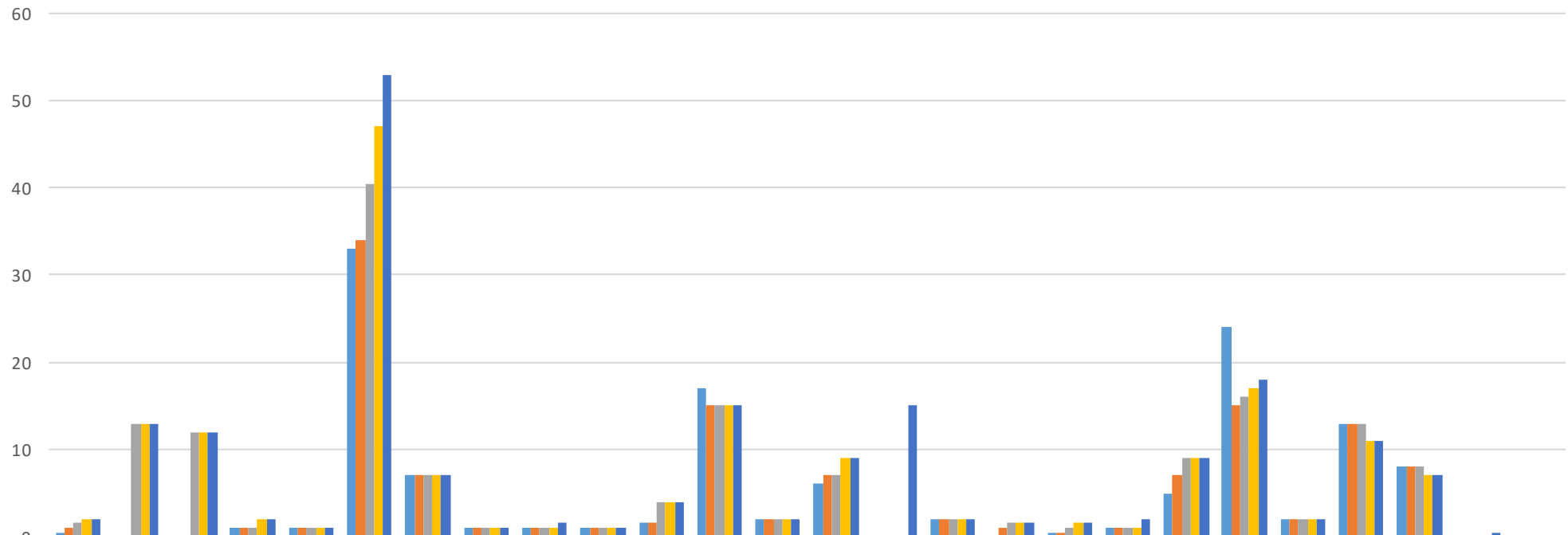
64. One SA reports having encountered obstacles when requesting or providing assistance to another DPA. However, this SA specifies that there is not sufficient experience on this instrument yet to draw clear conclusions. This SA refers to future guidance from the EDPB on this matter that may shed more light on possible obstacles to the provision of mutual assistance.

3.10 Human, financial, and technical resources of SAs

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? Please provide data for 2017, 2018, 2019, 2020, 2021. What percentage of overall staff does this represent?

65. Some SAs have seen their work force dedicated to issues falling within the scope of the LED increase over the last four years. However, in the majority of SAs the full time equivalents of staff dedicated to LED-related issues has remained constant or decreased. In several SAs there are no persons dedicated full time to issues falling within the scope of the LED. Their staff members alternate between LED and GDPR-related issues.
66. The EDPB Secretariat dedicates 1,5 person in full-time equivalent to working on issues falling within the scope of the LED and for providing the Secretariat of the Coordinated Supervision Committee (for the coordinated supervision of IMI, Eurojust, EPPO and in the near future other EU bodies, agencies and large scale information systems).

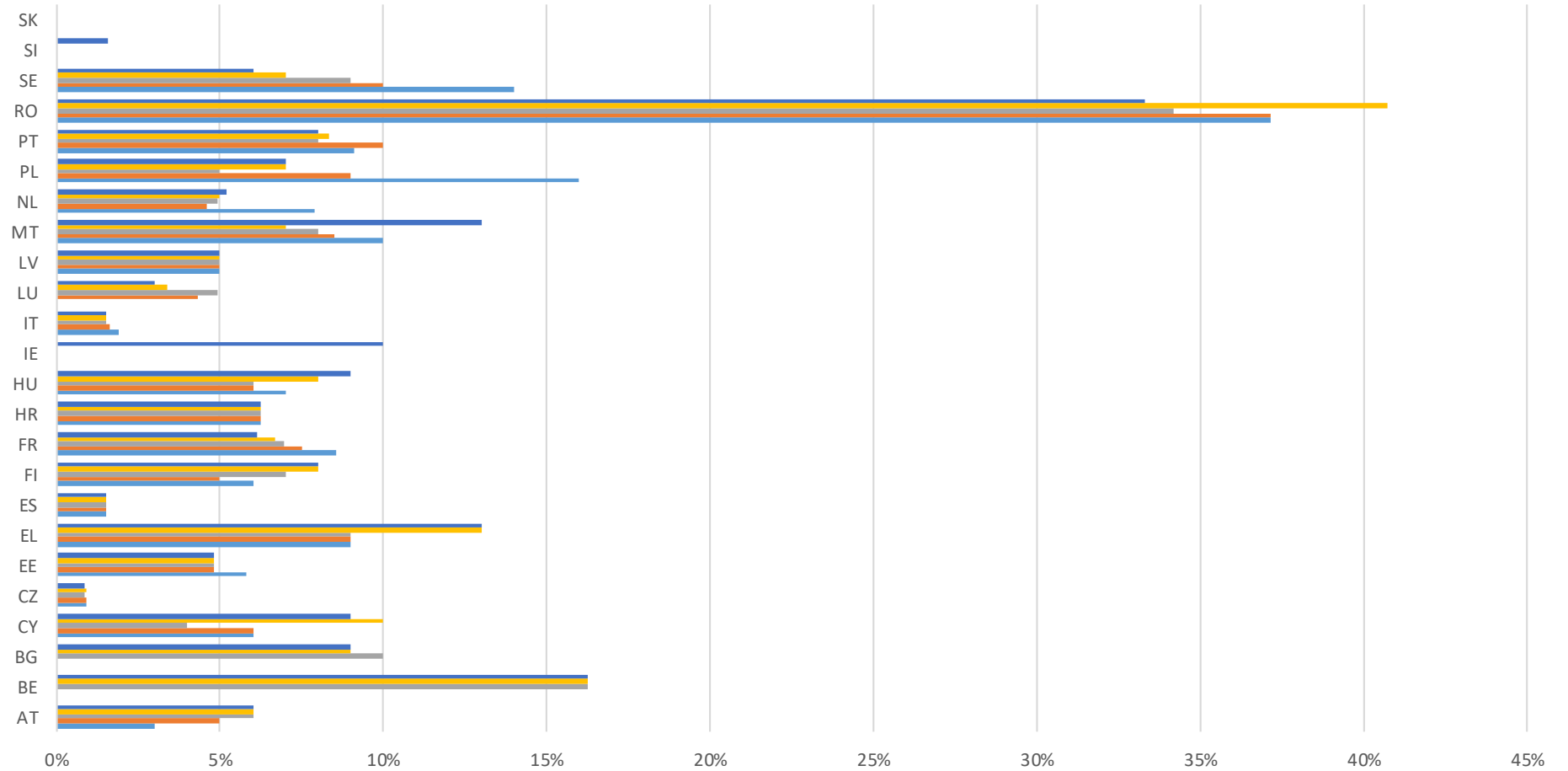
Q41 Number of persons (in full time equivalents) in SAs (respectively EDPB Secretariat) working on issues that fall within the scope of the LED specifically



| | AT | BE | BG | CY | CZ | DE | DK | EE | EL | ES | FI | FR | HR | HU | IE | IT | LU | LV | MT | NL | PL | PT | RO | SE | SI | SK |
|------|-----|----|----|----|----|------|----|----|-----|----|-----|----|----|----|----|----|-----|-----|----|----|----|----|----|----|-----|----|
| 2017 | 0,5 | | 0 | 1 | 1 | 33 | 7 | 1 | 1 | 1 | 1,5 | 17 | 2 | 6 | | 2 | | 0,5 | 1 | 5 | 24 | 2 | 13 | 8 | | 0 |
| 2018 | 1 | | 0 | 1 | 1 | 34 | 7 | 1 | 1 | 1 | 1,5 | 15 | 2 | 7 | | 2 | 1 | 0,5 | 1 | 7 | 15 | 2 | 13 | 8 | | 0 |
| 2019 | 1,5 | 13 | 12 | 1 | 1 | 40,5 | 7 | 1 | 1 | 1 | 4 | 15 | 2 | 7 | | 2 | 1,5 | 1 | 1 | 9 | 16 | 2 | 13 | 8 | | 0 |
| 2020 | 2 | 13 | 12 | 2 | 1 | 47 | 7 | 1 | 1 | 1 | 4 | 15 | 2 | 9 | | 2 | 1,5 | 1,5 | 1 | 9 | 17 | 2 | 11 | 7 | | 0 |
| 2021 | 2 | 13 | 12 | 2 | 1 | 53 | 7 | 1 | 1,5 | 1 | 4 | 15 | 2 | 9 | 15 | 2 | 1,5 | 1,5 | 2 | 9 | 18 | 2 | 11 | 7 | 0,5 | 0 |

¹⁵ The numbers for Germany represent the number of persons (in full time equivalents) working on issues that fall within the scope of the LED in all German SAs, which are responsible for the supervision of their respective Länder or federal authorities. However, the number of those persons differ from one German SA to the other, but especially in case of the Federal SA compared with the Länder SAs that have considerably less staff available.

% of the staff working on LED issues



| | AT | BE | BG | CY | CZ | EE | EL | ES | FI | FR | HR | HU | IE | IT | LU | LV | MT | NL | PL | PT | RO | SE | SI | SK |
|-------------|----|--------|-----|-----|-------|------|-----|------|----|-------|-------|----|-----|------|------|----|------|------|-----|-------|--------|-----|-------|----|
| ■ 2021: (%) | 6% | 16,25% | 9% | 9% | 0,86% | 4,8% | 13% | 2% | 8% | 6,12% | 6,25% | 9% | 10% | 1,5% | 3,0% | 5% | 13% | 5,2% | 7% | 8% | 33,33% | 6% | 1,55% | 0% |
| ■ 2020: (%) | 6% | 16,25% | 9% | 10% | 0,89% | 4,8% | 13% | 2% | 8% | 6,66% | 6,25% | 8% | | 1,5% | 3,4% | 5% | 7% | 5% | 7% | 8,33% | 40,74% | 7% | | 0% |
| ■ 2019: (%) | 6% | 16,25% | 10% | 4% | 0,87% | 4,8% | 9% | 1,5% | 7% | 6,97% | 6,25% | 6% | | 1,5% | 4,9% | 5% | 8% | 4,9% | 5% | 8% | 34,20% | 9% | | 0% |
| ■ 2018: (%) | 5% | | 0% | 6% | 0,92% | 4,8% | 9% | 1,5% | 5% | 7,50% | 6,25% | 6% | | 1,6% | 4,3% | 5% | 8,5% | 4,6% | 9% | 10% | 37,15% | 10% | | 0% |
| ■ 2017 (%) | 3% | | 0% | 6% | 0,92% | 5,8% | 9% | 1,5% | 6% | 8,54% | 6,25% | 7% | | 1,9% | | 5% | 10% | 7,9% | 16% | 9,09% | 37,15% | 14% | | 0% |

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

67. A majority of SAs consider their resources insufficient for their work on the LED from a human and financial point of view. SAs mention as one of the main causes their workload, which has grown in volume and complexity. The entry into force of the LED and its subsequent transposition into EU law, the amendment or adoption of EU instruments governing the processing of data in EU large scale information systems (such as SIS II, VIS, EURODAC, CIS, ECRIS-TCN, ETIAS, EES), and new technological developments in the law enforcement area account for this growth. The growing workload has not been accompanied by a proportionate increase in the resources of SAs. In the absence of additional resources, SAs dedicate staff to work on GDPR and LED-related issues simultaneously, with these two files competing for resources. Some SAs report as consequences of the lack of sufficient resources: rulings from judicial authorities against SAs for inaction, and SAs supervising in a reactive manner, rather than based on risk.
68. The Secretariat of the EDPB is seeing its workload on LED-related matters increase significantly due to the same developments mentioned above, its support and contributions to the EDPB's discussions and guidance, and its new role in providing the Secretariat for the Coordinated Supervision Committee (CSC). The scope of coordinated supervision of the CSC, which was created at the end of 2019, will increase as it is mandated with ensuring the coordinated supervision of all EU large scale information systems (e.g. IMI, SISII, VIS, ETIAS, EES, Eurodac) and agencies (Eurojust, Europol, EPPO) in the coming two years.

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

69. Almost half of the SAs face specific challenges when supervising competent authorities in terms of expertise (criminal law / technical / IT) and resources. The most reported challenge is insufficient IT resources (in terms of technology and expertise), followed by insufficient expertise in technologies used in the area of law enforcement. Some SAs mention insufficient or even nonexistent IT forensic capabilities (including technical means and experienced IT experts), and lack of interoperability between technical systems, which may hinder communications between the SAs and competent authorities. The increasing complexity of the IT systems used by law enforcement, including the EU large scale information systems, compounds this challenge. Some SAs encounter difficulties in hiring and retaining technical and legal experts in law enforcement working methods and technologies. Some SAs advance as potential solutions in-depth training and certification mechanisms.

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

70. SAs report that the transposition of the LED brought more harmonisation, foreseeability, and clarity on the regulations governing the processing of personal data in the area of law enforcement, the responsibilities of competent authorities, and in particular on the rights of data subjects. It also raised the competent authorities' awareness of them (especially of those competent authorities working at the central level) and of the general public. As a result of the transposition of the LED some competent authorities allocated more resources for data protection, by investing for instance in the implementation of the principles of privacy by design and by default in their IT systems. The overall security of data processed is reported as having improved.

71. The transposition of the LED also increased the enforceability of the principles of transparency and accountability on competent authorities. The LED compelled competent authorities to carry out data protection impact assessments in a number of cases; brought more scrutiny over their transfers of data to third countries. The LED also increased their data protection obligations (e.g. in establishing data retention periods, implementing the principle of data minimisation and reporting data breaches), including in relation to the rights of data subjects, which are better protected.
72. Some SAs also welcome the increase of new investigative and corrective powers for supervisory authorities that resulted from the national transposition of the LED, and the additional weight given to their opinions. In some cases, the transposition of the LED also extended the jurisdiction of supervisory authorities over the processing of data by public prosecutor offices. However, other SAs consider that the LED does not provide in its Article 57 for detailed, effective and dissuasive measures, as those found under Article 83 GDPR. National legislation transposing the LED can, in theory, provide penalties that are effective, proportionate and dissuasive penalties when transposing the LED. Several SAs note that this is not the case in their countries. One SA sees no valid reason for making such distinction between the regimes for penalties in the GDPR and in the LED.

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

73. Half of the SAs have identified challenges on the application of the LED in relation to new technologies. These challenges concern mainly big data, artificial intelligence and facial recognition technologies. These new technologies are complex legally and technically. They often involve the use of special categories of data, such as biometric data. Some new technologies pose high risks to the rights of individuals and require specific, clear, precise, and foreseeable legal basis laid down in primary legislation and not only in secondary legislation. SAs also identified the use of drones, bodycams, data from electronic communications and the interconnection between information systems as other developments that raise challenges. The use of new technologies is usually associated with lack of transparency and non-compliance with data security standards.
74. The speed of technological developments increases. Regulations often follow them belatedly, which produces gaps in the legislation. Some SAs also struggle to keep pace with them. The LED does not lay down rules for new technologies, save for the obligation to conduct data protection impact assessments and a specific framework for the processing of sensitive data. Some SAs consider that the LED's principles may be insufficient to regulate strictly these technologies and assess the compliance of competent authorities.

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

75. A majority of the SAs have found important problems in the transposition of the LED in their respective countries. They point to significant delays in the transposition of the LED into national law and the adoption of secondary legislation needed to regulate important aspects such as storage periods and the conditions for the exercise of data subject rights.
76. Several SAs consider that the LED has not been adequately transposed in their countries, and that national law is unclear and incomplete on some issues. One of these issues is the scope of application of the LED, especially as regards data processing operations by judicial, state security, tax, customs and migration authorities, and as regards the processing of data in relation to minor offences and administrative fines, which may fall outside the LED's concept of "criminal offence". Another issue is the interplay of the LED with data protection regimes laid down in other instruments, such as the GDPR

and those not covered by EU law in areas such as state security. This interplay affects the exercise of data subjects' rights. In some EU Member States national law fails to provide sufficient guidance on the processing of special categories of data.

77. Some SAs also find problematic the insufficient powers their national implementing legislation confers on them. For example 2 SAs lack adequate powers to sanction violations of national legislation adopted under the LED through warnings or administrative fines.

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

78. One SA mentioned that in its country national legislation transposing the LED also applies to the processing of data by and on behalf of the Defence Forces and by the police in relation to national security. This provides additional protection of personal data processed in these areas.
79. Another SA suggested evaluating whether the data subjects' exercise of their rights through the supervisory authority, as provided by Article 17 LED, is effective in enhancing data protection in the area of law enforcement.
80. Some other SAs raised the need to clarify the interplay between Article 10 GDPR, which covers the processing of personal data relating to criminal convictions and offences or related security measures, and the LED to ascertain its scope.
81. One SA also proposed creating a legal basis for joint inspections in the LED, similar to the one found under Article 62 GDPR to foster cooperation between SAs and the EDPS in the exercise of their respective supervisory tasks.

For the European Data Protection Board

The Chair

(Andrea Jelinek)