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

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compared with the earlier Framework Decision (which covered only transmission between Member States) that it repealed and replaced.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.


---

**QUESTIONNAIRE**

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

*Select your Country*

- **Poland**

**Powers**

* Q1: In your opinion, did the LED strengthen your investigative powers / corrective powers?
  - [ ] Yes
  - [ ] No

* Q2: Please list your investigative 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(s)
Q3: Do you consider your investigation powers effective
- Yes
- No

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

So far, there has been no situation where the President of the Personal Data Protection Office was prevented from accessing information necessary to conduct investigation due to the submission of a complaint by the data subject.

Q4: Do you face any practical difficulties in applying your investigative powers?
- Yes
- No

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

Q7: Do you have the same corrective powers towards all law enforcement authorities?
- Yes
- No

Q7.1: What are the differences?
Pursuant to Art 1(3) of the Act of 14.12.2018 on the Protection of Personal Data Processed in Relation to the Prevention of and Fighting Crime, the processing of personal data by the Prosecutor's Office and Courts has been excluded from the supervision of data protection specified in this Act.

In accordance with Art 3 of the Act of 14.12.2018 the provisions of this Act shall not apply to the protection of data:

1) located in case or activity files or record devices, including those created and processed using information technology, maintained pursuant to:
   - the Act of 26 October 1982 on proceedings in Juvenile Matters;
   - the Act of 6 June 1997 – Executive Penal Code;
   - the Act of 6 June 1997 - Code of Criminal Procedure;
   - the Act of 10 September 1999 - The Penal and Fiscal Code;
   - the Act of 24 August 2001 - Pretty Offences Procedure Code;
   - Act of 22 November 2013 on procedures for dealing with persons with mental disorders who pose a threat to the lives, health or sexual freedom of other person;
   - the Act of 28 January 2016 - Act on the Public Prosecutor's Office;

2) processed in connection with ensuring national security, including as part of the implementation of statutory tasks:
   - the Internal Security Agency,
   - the Intelligence Agency,
   - Military Counterintelligence Service,
   - Military Intelligence Service,
   - Central Anticorruption Bureau.

Chapter 9 of the Act of 14.12.2018 defines i.a. the entities other than the President of the Personal Data Protection Office competent to supervise the personal data processing - Articles 56 - the State Tribunal, 67 - military courts, 75 - administrative courts, 87 - the Prosecutor’s Office, 90 - the Constitutional Tribunal, 93 – the Supreme Court of Poland.

All of the above mentioned exclusions are subjective exclusions, not objective exclusions.

Q8: Do you consider your corrective powers effective?

- Yes
- No

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]?]


<table>
<thead>
<tr>
<th>SIS II and VIS</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>47(2)(a)</td>
<td></td>
</tr>
<tr>
<td>47(2)(b)</td>
<td></td>
</tr>
</tbody>
</table>

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

3

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

13

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

☐ Yes
☐ No

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.

400%

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

☐ The respect of the proportionality and necessity principle (Article 4 LED)
☐ 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)
☐ 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)
☐ 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)
☐ The right to information (Article 13 LED)
☐ Right of access by the data subject and limitations to this right (Articles 14 and 15 LED)
☐ The right to rectification or erasure of personal data (Article 16 LED)
Q11.7: The determination of the legal basis (Article 8 / Article 10 LED) - raised issues:

The applicants mainly questioned the legitimacy of processing their personal data in the National Police Information System.

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

The applicants alleged that the police had failed to provide them with information. The failures were alleged to consist of failure to fulfil the information obligation towards the complainant set out in Article 22(4) of the Act of 14 December 2018, in connection with the processing of his/her personal data in the National Police Information System; refusal to provide information concerning the processing of the applicant's personal data in police records.

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

Refusal to provide access to applicant's personal data processed in the Police National Information System at the applicant's request; refusal to provide access to information concerning the processing of the applicant's personal data in the Police National Information System. Making the complainant's personal data available to unauthorised persons.

Q11.13: The right to rectification or erasure of personal data (Article 16 LED) - raised issues:
The failure to remove the applicant's personal data from the Central Database of Persons Deprived of Liberty or the files of the National Criminal Information Centre.

Q12: Are you following up on all complaints?
- Yes
- No

Q12.1: Please explain why you are not following up on complaints?

The President of the Personal Data Protection Office takes appropriate actions provided for by the law in relation to all received complaints about irregularities in the personal data processing. Complaints submitted to the President of the Personal Data Protection Office must meet the formal requirements set out in the provisions of national law (Code of Administrative Procedure, Act of 14 December 2018). If a complaint contains formal deficiencies, the President of the Personal Data Protection Office shall summon the complainant to remove the formal deficiencies of the complaint within the indicated time limit. In the case of failure to remove formal deficiencies of a submitted complaint, despite the summons of the President of the Personal Data Protection Office, the complaint shall be left without examination. Moreover, in a situation when the complainant's address was not indicated in the complaint, and it is impossible to determine the address on the basis of available data, the complaint shall also be left unexamined (pursuant to Article 63 § 1 of the Code of Administrative Procedure).

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

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?

21

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:

- Can an authority processing personal data under Directive 2016/680 share data on the basis set out in Article 6(1)(f) of the GDPR?
- Is a public authority obliged to transfer the data of a prison inmate who has informed the competent police authorities of the inmate’s intention to commit an offence upon release, despite the inmate’s objection that he does not consent to the disclosure of his personal data?
- Can the image of a passenger in a speed camera photo be made available in the context of an offence investigation conducted by a competent authority?
- Does the provision of information by the Police about the presence of a person (of age and not incapacitated) in the Detention Room to so-called "relatives" violate data protection legislation?
Q18.7: Processing for purpose of research and/or innovation (Article 9(2) LED) - raised issues:

Are controllers processing data under both Directive 2016/680 and GDPR, operating within the same organisational structure of the Authority, required to create separate data protection policies and registers of processing activities?

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

Are controllers processing data under both Directive 2016/680 and GDPR, operating within the same organisational structure of the Authority, required to create separate data protection policies and registers of processing activities?

Q18.16: Other - raised issues:

Can a contract for the provision of DPO services be entered into with an external company in light of Directive 2016/680?

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

• 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?

  4 conferences and training briefings on the implementation of the Directive 2016/680 in Poland in terms of law and practice.
  Since April 2019 the Personal Data Protection Office publishes (in polish) Newsletter dedicated to Data Protection Officers available at: https://uodo.gov.pl/p/archiwum-newslettera-dla-iod. Among the advices on how to apply the provisions of the LED, the Offices covered the following topics:
  - Dealing with prisoners’ correspondence - is it subject to correspondence secrecy protection or can only authorised persons have access to it.
  - Is it permissible to display prisoners’ details, such as their name and details of any suicide attempt or psychiatric treatment, in the staff room in the prison?
  - Is the operator of the prison canteen allows to enter into the computer such data as the prisoners’ name, father’s name, the amount of money at their disposal and data on products purchased when prisoners make purchases?

Data breach notifications

• Q21: How many data breach notifications have you received?
  - Approx. 350

• Q22: In what proportion have you followed up with investigations? (%)
  - No data

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

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? (%)

No data

Power pursuant to Article 47(5) LED

Q25: Have you exercised your power to

<table>
<thead>
<tr>
<th>* bring infringements of your national law(s) transposing the LED to the attention of judicial authorities?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* commence or otherwise engage in legal proceedings?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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?

0

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:

• 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

• 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

• 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?
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

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:**

The Act implementing Directive 2016/680 into the Polish legal order - the Act of 14 December 2018 on the Protection of Personal Data Processed in Relation to the Prevention of and Fighting Crime regulates the cooperation mechanism with supervisory authorities in other European Union countries in the Chapter 6. According to Art. 48(1) of the Act the President of the Personal Data Protection Office shall provide assistance to supervisory authorities in other countries of the European Union upon their request. Such a request may concern, in particular, information request, carrying out consultations, inspections or investigations.

According to Art. 49(1) of the Act the President of the Personal Data Protection Office may request assistance from a supervisory authority in other countries of the European Union, in particular information request, carry out consultations, inspections or investigations.

The Art. 49(3) of the Act specifies that the President of the Personal Data Protection Office may use information received from a supervisory authority in other European Union countries only for the purpose specified in the request for assistance.

The Art 49(4) of the Act adds that the President of the Personal Data Protection Office may request information from a supervisory authority in other countries of the European Union on the results or, if necessary, on the progress or actions taken to respond to the request.
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:

- 24 complaints submitted by data subjects,
- 5 complaints submitted by competent authorities/processors,
- 2 complains for inaction

38.2: What was the outcome?

Multiselection is possible

- Complaints declared inadmissible
- Decisions upheld
- Decisions overturned

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

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

<table>
<thead>
<tr>
<th>Type of Cooperation</th>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request for information</td>
<td>1</td>
</tr>
<tr>
<td>Request to carry out investigations</td>
<td>0</td>
</tr>
<tr>
<td>Request to carry out inspections</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type of Response</th>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests declined</td>
<td>0</td>
</tr>
<tr>
<td>Information provided</td>
<td>1</td>
</tr>
<tr>
<td>Investigation carried out</td>
<td>0</td>
</tr>
<tr>
<td>Inspection carried out</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type of Cooperation</th>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request for information</td>
<td>2</td>
</tr>
<tr>
<td>Request to carry out investigations</td>
<td>0</td>
</tr>
<tr>
<td>Request to carry out inspections</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

• Q40: Have you encountered any obstacles (e.g. of an administrative nature) when requesting or providing assistance to another DPA?
Q40.1: Please describe them as well as possible solutions.

There were no such cases in the Personal Data Protection Office.

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?

<table>
<thead>
<tr>
<th>Year</th>
<th>Number (FTE)</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>24</td>
<td>16%</td>
</tr>
<tr>
<td>2018</td>
<td>15</td>
<td>9%</td>
</tr>
<tr>
<td>2019</td>
<td>16</td>
<td>5%</td>
</tr>
<tr>
<td>2020</td>
<td>17</td>
<td>7%</td>
</tr>
<tr>
<td>2021</td>
<td>18</td>
<td>7%</td>
</tr>
</tbody>
</table>

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:
The amount of budgetary resources of the Polish Data Protection Authority is lower than the amount requested by the Authority. As a result, financial resources, but also financially related, personnel resources of the Office are limited. The Administrative Courts have repeatedly found inaction on the part of the Polish DPA pointing to the broader problem of the limited staff resources and the high turnover of staff, which has significantly impeded the fully effective performance of the tasks assigned.

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
- [x] Insufficient expertise in working methods and practices of law enforcement authorities
- [ ] Insufficient expertise in international cooperation in criminal matters
- [x] Insufficient expertise in technologies used in the area of law enforcement
- [x] Insufficient IT resources
- [ ] Others challenges

Q43.1.2: Insufficient expertise in working methods and practices of law enforcement authorities- please provide more details below:

Employees of the Polish SA report the need to acquire expertise on the working methods and practices of law enforcement agencies - as regards the processing of personal data by the subjects of complaints, from a practical point of view.

Q43.1.4: Insufficient expertise in technologies used in the area of law enforcement- please provide more details below:
Progressive technological development, including new large-scale systems, makes existing IT knowledge and experience obsolete. More training would be desirable for existing control staff and additional IT staff to support this.

Q43.1.5: Insufficient IT resources-please provide more details below:

A certain impediment to work is the fact that the legal information system used in the Complaints Department lacks a commentary on the Act of 14 December 2018 on the Protection of Personal Data Processed in Relation to the Prevention and Fighting Crime.

Horizontal questions

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

The Law Enforcement Directive created new investigative and corrective powers for supervisory authorities, which are uniform for all Member States. The Directive details the principles for processing data in connection with preventing and combating crime.

• 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 dynamic development of new technologies brings new challenges for the protection of personal data and privacy. Due to the progressing technological development, the possibilities of law enforcement bodies to prevent and combat crime, which may affect civil rights and freedoms, have significantly increased. Their impact on civil rights and freedoms and the necessity and proportionality of using such measures in a democratic state under the rule of law are widely commented upon. In particular, this applies to techniques that involve the use of special categories of data, such as biometric data.

Supervisory Authorities were particularly concerned about the lack of provisions treating artificial intelligence as the main subject of regulation, and not only as a side issue on the way to ensuring the protection of other rights. Therefore, the Personal Data Protection Office pays special attention to the issues related to appropriate legal solutions regulating the principles of protection of personal data obtained with the use of Artificial Intelligence.

Proper and primarily risk-based management of information security and integrity is crucial to the functioning of facial recognition technology. It is imperative that technical and organisational safeguards are in place before implementing facial recognition technology. It is extremely important to properly manage the confidentiality, integrity, availability and usability of data.

There is a concern that due to the fact that Artificial Intelligence often misidentifies women and people of non-white skin colour, it may potentially lead to misidentification or violation of privacy, which could also be perceived as discrimination and biased prosecution based on gender or ethnic origin. According to the Directive 2016/680, the risk that may result from data processing to the rights or freedoms of natural persons of varying likelihood and severity could occur in particular where the processing may give rise to discrimination.

The use of biometric signatures should also be noted in this context. Due to pandemic and accelerated digitisation in the Polish Police, the biometric signatures are increasingly used by the Polish Police. The biometric data processing undoubtedly interferes with privacy, posing risks to special categories of personal data and therefore the decision to process biometric data should take into account factors such as, inter alia, the necessity, the proportionality of the effects to the purposes to be achieved and the social acceptability of collecting biometric data. Any potential leakage of this special category of personal data will result in a high risk of violation of the rights and freedoms of individuals and its negative consequences may be felt for a long time. Undoubtedly, such a solution without a proper data protection impact assessment and risk analysis can pose a significant security risk. Taking into account the planned solution should be assessed in more detail from the technical and information security perspective, indicating whether it is secure enough to effectively protect citizens’ rights and whether it is necessary when confirming receipt of parcels.

- Q46: Have you identified any important problems regarding the transposition of the LED in your Member State?
  - Yes
  - No

- Q46.1: Please explain.
According to the Directive 2016/680 Member States should have adopted and published, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. However, this occurred with a delay in the Polish legal system, as the Act on the Protection of Personal Data Processed in Relation to the Prevention of and Fighting Crime (the Act) was enacted on 14 December 2018 and entered into force on 6 February 2019. Subsequently, on the basis of the Act of 14 December 2018, the Prime Minister’s Regulation on the procedure and manner of performance of tasks by the Data Protection Officer was issued on 31.05.2019.

It should be noted that the Personal Data Protection Office does not have a legislative initiative. The Polish DPA has submitted its position on the draft Act during the consultation stage of the legislative work.

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

- Yes
- No