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compared with the earlier Framework Decision (which covered only transmission between Member States) that it repealed and replaced.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

---------------------------------------------------

QUESTIONNAIRE

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

* Select your Country

Netherlands

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

- Art. 5:20: the power to demand full cooperation with the supervisor, which may reasonably demand this in the exercise of its powers, within such reasonable time limit as it may specify.

Q3: Do you consider your investigation powers effective

- Yes
- No

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

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?

Multiple replies are possible

- 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
Q8: Do you consider your corrective powers effective?
- No

Q8.1: Please explain why do you do not consider your corrective powers effective?
[Multiple replies are possible]

Not with regard to administrative fines. There is a substantial discrepancy between 1) the number of provisions that are penalised in the GDPR and the transposition legislation of the LED and 2) the maximum level of penalties, as the administrative fines that can be imposed on public authorities pursuant to the GDPR and the NL legislation as transposed by the LED cannot be considered justifiable.

In the opinion of the NL DPA its corrective powers still remain insufficient and not in proportion to the DPA’s corrective powers regarding other public authorities pursuant to the provisions of the GDPR. The NL Police Data Act (i.e. one of the national transposition laws with regard to the LED) only provides for limited enforcement possibilities to impose an administrative fine in case of violations, whereas the GDPR provides for powers to impose administrative fines for – in principle – all violations of the law. Moreover, the maximum fining level to be imposed on the police for violations of provisions that have been laid down in the law, is substantially lower than that of fines the DPA can impose on public authorities based on the GDPR. This leads to the consequence – for instance – that enforcement by the DPA in case of unlawful processing by controllers of a municipality or the police respectively, can be fined by a dissuasive penalty in the first case, whereas that cannot be done in the last case, as dissuasive penalties are not foreseen in the LED/transposed national law.

Article 57 of the LED provides that ‘The penalties provided for shall be effective, proportionate and dissuasive.’ However, no detailed elaboration can be found in the LED, unlike the provisions of the GDPR, which provide for detailed effective and dissuasive measures in Article 83 GDPR. The transposed provisions in national legislation could, in principle, provide for the same level of effective, proportionate and dissuasive penalties, but this is not the case in the current Dutch legal framework.

According to the NL DPA penalties provided for should be in line with those regulated in the GDPR as no valid reasons can be attributed to this substantial difference between the two data protection regimes. Moreover, unlike Article 83 of the GDPR, several similar rules in the LED cannot be penalised at all under Dutch law. For example: the violation of the basic principles of data protection (Article 83(4)(a) GDPR) is not penalised in the NL transposed legislation. This is also the case for violating the rules on transfers of personal data to recipients established in third countries (Article 83(4)(c) GDPR). In this respect the Dutch transposition is insufficient.

With regard to the level of penalties, Dutch transposed legislation provides for two categories of penalties: infringements of a. provisions relating to the obligations of the controller and b. provisions relating to the rights of the data subject. The first category can be punished by a maximum fine of 870.000 euros and the second by a maximum fine of 87.000 euros. This can be characterised as far out of proportion compared to the maximum fines provided for by the GDPR, while the required criteria are worded in exactly the same way, as “effective, proportionate and dissuasive” penalties.

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

Q9.1.2: Art.47(2)(b): Number of cases related to the supervision of - SIS II and VIS:

Following a N.SIS inspection of the Netherlands Police the NL DPA imposed an order backed by periodic penalty payment in 2017, and again in 2018. Finally, in 2019 the DPA concluded that measures taken – after the second order – were sufficient and closed the case.

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.

Numbers of national complaints

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
<th>Requests for mediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>(not available)*</td>
<td>(not available)</td>
</tr>
<tr>
<td>2020</td>
<td>62</td>
<td>58</td>
</tr>
<tr>
<td>2021</td>
<td>(not available)</td>
<td>(not available)</td>
</tr>
</tbody>
</table>

Numbers of international complaints

<table>
<thead>
<tr>
<th>Year</th>
<th>Requests for mediation/international cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>13</td>
</tr>
<tr>
<td>2020</td>
<td>16</td>
</tr>
<tr>
<td>2021</td>
<td>27</td>
</tr>
</tbody>
</table>
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)
- 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)
- The obligation to ensure the security of processing, including data breaches (Articles 4(1)(f), 29 LED)
- Other

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

With regard to complaints and requests for mediation, these mostly related to removal and rectification of police data and access to data processed by the police about the data subject. Explanation: those involved often submitted complaints about police data the police processes in their reports and investigation files. According to the complainants, the further processing of this data has adverse consequences in their daily lives.

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

Regarding international cases complaints mainly concern the exercise of data subject’s rights of all types. Almost all SIS requests relate to lifting an entry ban.
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

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?

The exact number is not clear, but every year it is estimated about 20 legislative advices/opinions upon request are being published; not a single advice is issued on our own initiative, because of limited time and resources. For this reason we can only handle mandatory consultations.

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

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

They have for instance requested advice on how to combine the DPIA with their own internal framework for assessing new activities and how to deal with and report data breaches, and discussed with us their IT, and specifically IT security issues.

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

They have for instance requested advice on how to combine the DPIA with their own internal framework for assessing new activities and how to deal with and report data breaches, and discussed with us their IT, and specifically IT security issues.

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

We have updated the general information about the LED (and the national laws implementing it) on our website. We also organised a couple of so-called ‘round table meetings’ with authorities and processors, so that not only could they receive guidance from the DPA, but also from each other. Besides that, we have regular contacts with the Netherlands Police and the central Public Prosecutor’s Office and its DPOs. In addition, the NL DPA has set up a helpdesk by telephone and mailbox for DPOs asking for guidance on specific issues.

Q20: Have you provided training to / carried out awareness-raising activities for competent authorities and / or processors (DPOs included)?
- Yes
- No

Data breach notifications

Q21: How many data breach notifications have you received?

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>15</td>
</tr>
<tr>
<td>2019</td>
<td>178</td>
</tr>
<tr>
<td>2020</td>
<td>220</td>
</tr>
<tr>
<td>2021 (until 10/11)</td>
<td>135</td>
</tr>
</tbody>
</table>

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

In 226 cases the NL DPA performed double-checks and verifications. In none of the notification cases the NL DPA has started investigations.

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

Not applicable

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? (%)

Not applicable
Power 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? | Yes | No |
| • commence or otherwise engage in legal proceedings? | Yes | No |

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?

The NL DPA only received one request that should have been handled by applying Article 17 LED. It concerned a request based on Article 42(4) Europol Regulation, which article requires that this right shall be exercised in accordance with the national law of the Member State in which the request is made. However, Article 17 – being the article corresponding with the right described in Article 42(4) ER – was never transposed into the NL Police Data Act.

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

- 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:

As the corresponding article in the Police Data Act for assessing this case was lacking, the NL DPA applied the Dutch General Administrative Law Act to reach a decision on the data subject’s request. The NL DPA’s decision concluded that all checks of data had been carried out and were found to be lawful, and partial access to the data subject’s data was allowed.
Q28: Did encounter any particular problems?
- Yes
- No

Q28.1: Please explain.
As the corresponding article in the Police Data Act for assessing this case was lacking, the NL DPA applied the Dutch General Administrative Law Act to reach a decision on the data subject’s request. The NL DPA’s decision concluded that all checks of data had been carried out and were found to be lawful, and partial access to the data subject’s data was allowed.

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?

- 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

• 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:

In general the NL DPA frequently exchanges information with other DPA’s, mainly within the context of the EDPB (or the IMI system), as well as within the context of other coordinated supervision committees in the context of law enforcement and border control.
**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:

  This has been done in 8 cases:
  - 1 case the court was not competent;
  - 1 case was deemed inadmissible;
  - 3 cases were revoked by the other party, before the case was finalised by the court;
  - 3 cases are still pending.

38.2: What was the outcome?

Multiselection is possible

- [ ] Complaints declared inadmissible
- [ ] Decisions upheld
- [ ] 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>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
</tr>
</tbody>
</table>

The cooperation between EU/EEA DPAs in the form of the provision of mutual assistance is primarily embedded in the IMI system. This system does not provide for an avenue of cooperation/mutual assistance tailored specifically
to Article 50 LED. The possibilities for mutual assistance in the IMI system are, at least nominally, limited to formal mutual assistance under Article 61 GDPR (A61MA) and informal or voluntary mutual assistance under Article 61 (A61VMN) - though it can be argued that voluntary mutual assistance flows from Article 57(1)(g) GDPR. In practice, the type of mutual assistance provided under both mutual assistance flows in IMI (A61MA and A61VMN) is not strictly limited to matters falling under the GDPR and the requests frequently extend to cover (also) subject matter that falls under the LED. It must be remarked here that formal requests under A61MA are rare – there is an understanding between SAs that informal requests are to be used first so as not to start any legal deadlines and consequences without intending.

The provision of exact numbers of mutual assistance provided under Article 50 LED through A61MA or A61VMN in IMI is difficult, as criteria have not been set in place to determine which requests would be covered by Article 50 LED, nor have such requests been homogenously indicated as such. The same applies for other methods of cooperation (e.g. through Confluence fora, e-mail, etc.).

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

<table>
<thead>
<tr>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Requests declined</td>
</tr>
<tr>
<td>• Information provided</td>
</tr>
<tr>
<td>• Investigation carried out</td>
</tr>
<tr>
<td>• Inspection carried out</td>
</tr>
<tr>
<td>• Other</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Nbr</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Request for information</td>
</tr>
<tr>
<td>• Request to carry out investigations</td>
</tr>
</tbody>
</table>
• Request to carry out inspections  -
• Other  see table above

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

☐ Yes  
☐ No

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

As of yet, experience with this instrument is not sufficient to draw any clear conclusions as to whether there are any obstacles when providing or requesting assistance. 
The provision of formal mutual assistance under Article 61 GDPR faces some legal questions currently under review by the EDPB, who intends to issue guidance to streamline the process. At this stage it is not clear whether that guidance will also include Article 50 LED requests and/or informal mutual assistance. Should this be the case, any obstacles experienced under Article 50 LED will also be addressed by the guidance.

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></th>
<th>Number (FTE)</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>5</td>
<td>7.9</td>
</tr>
<tr>
<td>2018</td>
<td>7</td>
<td>4.6</td>
</tr>
<tr>
<td>2019</td>
<td>9</td>
<td>4.9</td>
</tr>
<tr>
<td>2020</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>2021</td>
<td>9</td>
<td>5.2</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:
At the moment, the current budget of the NL DPA for 2022 is set at 26.3 mln. Euro. This is insufficient to carry out our supervisory tasks, as was also concluded in an independent report by KPMG. In this report, it was concluded that the Dutch DPA would need to grow from its current size of 170 FTE to 470 FTE in 2025, in order to sufficiently and effectively carry out its tasks. This report covered both the tasks of the NL DPA based on the GDPR, as well as tasks based on the LED and other European Regulations in the context of law enforcement, travel and border control (such as SIS, VIS, EURODAC, CIS). In order to be a fully effective and future-proof supervisor, the NL DPA takes the position that a budget of 100 mln would be required.

While not solving our general concerns regarding a lack of resources, it should nonetheless be noted that the NL DPA will receive additional funding dedicated to a number of new (additional) tasks, following the entry into force of a number of new European Regulations (such as ECRIS-TCN, ETIAS, Interoperability Regulations, Entry Exit System).

• 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
  - Others challenges

• Q43.1.6: Other challenges - please specify.

  In general it should be noted that the NL DPA faces difficulties when hiring the required technical and legal expertise, as supervision in the context of law enforcement requires specific and high-level skills.

Horizontal questions

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

  Probably the highest impact of the LED (in combination with the GDPR) in the Netherlands is more attention and awareness of competent authorities and the general public for the protection of personal data, also because the NL DPA issued several enforcement sanctions with respect to the police. However, an –
The unwanted side-effect of the LED is that the urgency of its transposition delayed the revision of the Police Data Act and the Judicial Data and Criminal Records Act (see also under 45).

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 competent authorities are very much inclined to search for new possibilities and methods, and thus new technologies, for the purposes of the prevention, investigation, detection or prosecution of criminal offences. In that search they sometimes tend to forget, ignore or neglect the LED, if the rules laid down in the LED are felt to be hindering or obstructing those new initiatives.

- The police and other competent authorities in the Netherlands using Artificial Intelligence, algorithms and big data, like in predictive policing (for example the “Crime Anticipation System” predicting the crime risks in local areas), bodycams and “sensing instruments” to capture certain movements. A major problem of these new methods is the lack of transparency. Another risk of the application of big data by competent authorities is the presumption of innocence being put under pressure and the risk of secret mass surveillance, without having a clear and specific suspicion, and ethnic profiling. Also, sufficient attention and means for the improvement of existing devices and systems need to be in place, as a lot of systems used by the police do not comply with security standards.

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

- Yes
- No

Q46.1: Please explain.

In the Netherlands the LED was transposed into two existing laws, the Police Data Act and the Judicial Data and Criminal Records Act. An important problem constitutes that both laws have a complex structure and lack practicality – in particular for competent authorities, but also for the DPA and the public. Both laws were evaluated in 2013 and 2014 respectively and the government concluded a complete new law would be needed. But due to the short time available for the transposition of the LED, no time remained for revising these laws and preparing a complete new law. Currently the Ministry of Justice and Security is preparing a new law holding a fundamental revision of both existing laws.
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.

  • The relation between the LED and Article 10 of the GDPR

    Article 10 GDPR states that personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. The question is whether Article 10 GDPR only applies to data coming from the regime of the LED which are being further processed? Or whether Article 10 also deals with data outside that field of the LED, for example a private investigator who investigated a fraud by an employee, without any involvement of the police. This question was laid down in a Request for mutual assistance with regard to a common interpretation of ‘personal data relating to criminal acts and offences’ in Article 10 GDPR. The reactions of the other supervisory authorities were divided.

  • Creating a legal basis for joint inspections in the LED

    Where Article 62 of the GDPR provides for a detailed legal basis for performing joint operations of supervisory authorities a similar provisions is lacking in the LED. It could be beneficial for the cooperation of SAs and the EDPS in the exercise of their respective supervisory tasks to create a specific legal basis for this.