WHAT IS THE EU LAW ENFORCEMENT DIRECTIVE?

HOW LAW ENFORCEMENT AUTHORITIES (SHOULD) PROTECT PERSONAL DATA

Jelena Pejić

Belgrade Centre for Security Policy

BCSP

WHAT IS THE EU LAW ENFORCEMENT DIRECTIVE?
How Law Enforcement Authorities (Should) Protect Personal Data

Publisher:
Belgrade Centre for Security Policy
Đure Jakšića 6/5 11000 Belgrade
Author:
Jelena Pejić
Translation:
Ivan Kovanović
Design:
DTP studio
Print:
Unagraf
Copies: 200
ISBN: 978-86-6237-194-2

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

351.861(036)
342.738(036)
PEJIĆ, Jelena, 1991-

What is the EU Law Enforcement Directive? : How Law Enforcement Authorities (Should) Protect Personal Data / Jelena Pejić ; [translation Ivan Kovanović]. - Belgrade : Belgrade Centre for Security Policy, 2019 (Belgrade : Unagraf). - 18 str. ; 25 cm

Tiraž 100. - Napomene i bibliografske reference uz tekst.

ISBN 978-86-6237-194-2

а) Полицијска директива ЕУ -- Приручници б) Право на заштиту података о личности -- Приручници в) Безбедносни сектор -- Приручници

COBISS.SR-ID 281117196

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

The production of this backgrounder was supported financially by the Open Society Foundation, Serbia as part of the project 'Defending the Right to Access to Information in Serbia'. The views expressed in this publication are exclusively those of the author and do not reflect the views of the Foundation.

INTRODUCTION

The aim of this backgrounder[1] is to present the new EU legislation on the protection of personal data in law enforcement in a concise and clear manner. The legislative act is known as the EU Law Enforcement Directive (LED) (known also as the EU Police Directive)[2], a twin sister to the far more widely known General Data Protection Regulation – GDPR)[3].

Both GDPR and LED are part of a new EU legislative package that has significantly improved personal data protection standards. They were adopted in the spring of 2016 and have been in force since May 2018. While the General Regulation has garnered most of the attention from the expert community, governmental and non-governmental sector, the business world and the broader public concerned with individual privacy, the Law Enforcement Directive is rather specific – for both the circumstances in which it applies and from the approaches it adopts.

This backgrounder does not cover either the General Data Protection Regulation nor the Serbia's 2018 Law on Personal Data Protection, as they have been covered and analysed elsewhere.[4] However, the backgrounder does make use of official terminology used in the Law and does, for illustrative purposes, use examples from Serbia.

Why do we need the Law Enforcement Directive when we have the GDPR?

There are two reasons – the substantive and the formal – why a separate EU regulation is necessary for the protection of personal data in the law enforcement field.

First, the processing of personal data is substantially different when conducted by law enforcement agencies as opposed to other governmental authorities, private companies or non-governmental organisations. To the latter we mostly provide our personal data willingly and consent to its processing in order to exercise a certain right or access a service. On the other hand, law enforcement authorities often gather and process data without our consent, sometimes even without our knowledge, in order to pursue the public interest – such as protecting society from crime or other threats to public security.

Second, in terms of police and judicial cooperation, the powers of the European Union are newer and weaker than those that pertain to regulation of the common market, where the GDPR resides. Member states have become accustomed to a greater degree of autonomy in regulating the conduct of their police forces and other law enforcement agencies, especially

1 The author owes gratitude to Mr Juraj Sajfert, European expert on personal data protection, for clarification of dilemmas, numerous examples and suggestions on an earlier version of the text. The author's interview with Mr Sajfert was published by the Belgrade Centre for Security Policy in August 2019: <https://bit.ly/2NE0UB5>, <https://bit.ly/36lJJgb>.

2 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. Official Journal of the European Union, 4.5.2016.

3 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 4.5.2016.

4 See for example, Krivokapić, Danilo et al. *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR. Tumačenje novog pravnog okvira* [A Guide to the Law on Personal Data Protection and the GDPR. Interpretation of the New Legal Framework], Share Foundation, Belgrade, 2019: <https://www.sharefoundation.info/Documents/Vodic_ZZPL.pdf>.

when it comes to criminal proceedings. By adopting this new legislation in the form of a directive rather than a regulation, greater flexibility has been retained at the national level. To wit, the directive provides a binding framework and guidelines that must be enforced by national legislation,[5] while the provisions of the GDPR apply directly in the member states and have direct legal effect on natural and legal persons without any intervention by the member states.

What are the main differences between the Law Enforcement Directive and the GDPR?

On the one hand, differences are evident in the looser standards in certain parts of the LED as compared with the GDPR, and on the other, in the particular approaches adapted to law enforcement context that are not contained within the GDPR.

Certain provisions of the Law Enforcement Directive are weaker or more flexible than their GDPR equivalents:

- Transparency of data processing is not required;
- The obligation to minimise the quantity of gathered personal data is weaker;
- The rights of data subjectsmay be significantly restricted;
- The powers of the member states' competent oversight authorities are only rudimentarily regulated, while the GDPR covers them in detail.

Certain provisions are specific to law enforcement and do not have their GDPR equivalents:

- The obligation to categorise persons and their personal data;
- The obligation to keep logs of each individual act of accessing and processing of data;
- The obligation to provide time-limits for the storage of personal data.

There are also differences in how the transfer of data to third countries is regulated. These differences will be covered in greater detail in this backgrounder.

Why should we learn about the EU Law Enforcement Directive in Serbia?

The LED does not apply in Serbia.[6] However, this regulation is important for Serbia for two reasons. First, Serbia aspires to EU membership and must harmonise its regulatory framework with that of the EU, which includes improving personal data protection standards.[7] Secondly, Serbian law enforcement authorities must guarantee an equal degree of personal data protection so that they are even now able to exchange data effectively with their EU counterparts in order to combat cross-border crime.

5 For an overview of transposition of the LED in member states see: European Commission. „Data Protection Law Enforcement Directive (EU) 2016/680 transposition. Updated State of play in the Member States", 12. 4. 2019, <https://bit.ly/2NpLDDS> .

6 Apart from the EU member states, the LED also applies in Norway, Iceland, Switzerland and Liechtenstein, since they are members of the Schengen Area.

7 Serbia has done so by adopting a new Law on Personal Data Protection (*Official Gazette of the Republic of Serbia*, no. 87/2018), which comprises approaches modelled on those of the GDPR and the Law Enforcement Directive. The Law has been in force since 21 August 2019.

SCOPE OF THE LAW ENFORCEMENT DIRECTIVE

The Law Enforcement Directive applies to EU member states if the general preconditions for activating its personal data protection regime are met, and if the special conditions, that depend on who is processing personal data and to what end, are fulfilled.

General preconditions for application[8]

- The processing of personal data is conducted, wholly or partly, by automated means, or by non-automated means for personal data which form part of a filing system or are intended to form part of a filing system. The directive does not apply to manual processing of data that are not structured, regardless of the fact that they may be physically located in one place.
- Processing falls under the scope of European Union law. It does not apply, therefore, to those areas where member states have not transferred competencies to the EU. The operations of security and intelligence services and the military, for example, remain beyond the scope of the directive.[9]
- The directive does not apply to EU institutions and agencies, which are covered by separate regulation.[10]

Personal Data – *any data relating to a natural person who is identified or identifiable, directly or indirectly. In addition to obvious examples such as a personal ID numbers, dates of birth, fingerprints, personal data can include the person's signature, contact details (address, telephone number or email address), a private IP address, telephone listings, medical records and so forth.*

Processing – *any automated or non-automated operation performed, amongst other things, in order to collect, record, organise, structure, store, adapt, alter, detect, transmit, use, copy, disseminate, compare, erase or destroy personal data or sets of personal data. Processing is automated if it is performed using software that quickly and effectively manipulates large data sets with minimal human intervention.*

Filing System – *any centralised or decentralised set of personal data that is structured so that it can be accessed, searched and organised according to certain criteria.*

8 Article 2 of the EU Law Enforcement Directive. (Unless otherwise stated all citations of legal articles refer to this Directive).

9 This does not, however, prevent member states from applying standards set forth by the LED or the GDPR to these agencies through national legislation.

10 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. *Official Journal of the European Union*, 21.11.2018.

Special conditions for application

When the general preconditions have been met, whether LED or GDPR is applicable depends on who is processing the personal data (personal application domain) and to what end (material application domain).

The Law Enforcement Directive is applied only by competent authorities and for the following purposes:

- Prevention of criminal offences, including threats to public security;
- Investigation and detection of criminal offences;
- Prosecution of the perpetrators of criminal offences;
- Execution of criminal penalties.

A competent authority is any public authority responsible for acting in these purposes. Additionally, a competent authority could also be a private entity entrusted by member state law to exercise public authority and public powers for the purposes listed,[11] such as, for example, private prisons.

Examples

! *The Law Enforcement Directive, known also as the Police Directive, is not applied only by the police, nor do the police apply it every situation.*

a. Competent Authorities

Typical examples of competent authorities that apply the Law Enforcement Directive are the police, prosecutors, courts and prisons. However, even these bodies do not apply only the LED in their work. Whenever they process personal data for other purposes, such as recruitment (e.g. security screening of a candidate that includes criminal conviction checks), payroll or issuing identification documents – the authorities apply the more general GDPR, rather than LED.

Since competent authorities apply both EU data protection legislative acts, depending on the purpose of data processing, it is very important to determine in each specific case where the application of one act begins and the application of the other ends.

For example, a police officer searching a database of license plate numbers in order to sanction a driver who has committed a traffic violation should apply the GDPR. As should a customs officer when scanning travel documents at a border crossing. However, if in checking these data they should encounter information matching a criminal offence, for example the vehicle is stolen or an arrest warrant has been issued for the person in question, at that moment they begin applying the Law Enforcement Directive.

11 Article 3, Item 7 and Recital 12 of the EU Law Enforcement Directive.

Conversely, the customs officer applies the Directive when processing the data of a person caught illegally crossing a border if this is a criminal offence in their country. However, if the person requests asylum, the processing of their data in that procedure will be conducted according to provisions of the GDPR.[12] At the moment when an internal police investigation of an officer shows no criminal activity but a disciplinary offence of misdemeanour, the application of the Directive is replaced by the GDPR.

The Law Enforcement Directive does not apply to misdemeanours,[13] litigation or to the issuing of fines by public companies such as parking service or public transport companies.

Some member states have compiled lists of the competent authorities to which provisions of the Directive apply (Denmark, the Czech Republic, Slovakia), meanwhile these lists are not necessarily exhaustive (United Kingdom). However, there is a danger that the scope of the LED being extended excessively to the detriment of the GDPR, whose standards of protection and control are at a higher level.

b. Private Companies

As a rule, the Law Enforcement Directive will not be applied by detective agencies or private security companies; instead they are subject to the GDPR, though this ultimately depends on the regulations of each individual member state.

Private companies that have a legal obligation to submit certain personal data to the competent authorities do not apply LED, instead this is done by the law enforcement agencies as soon as they receive the relevant data. For example, telecommunication companies are required to store the phone records of their users for a certain amount of time and to provide them on request to the police for criminal investigations.[14] In this case, the companies apply the GDPR and the police apply the Law Enforcement Directive. The same should be true of banks that pass reports of suspicious transactions to the competent authorities in accordance with anti-money laundering and terrorism financing regulations.[15]

12 Sajfert, Juraj and Quintel Teresa, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", in: Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019 (forthcoming), p. 3. <https://ssrn.com/abstract=3285873>

13 Some member states (Denmark, for example) do not separate misdemeanors, even small ones such as illegal parking, from criminal offences, which then trigger application of the Law Enforcement Directive. It should be noted that a lot depends on the classification of criminal offences in national legislation.

14 For more on electronic data retention measures see: Pejić, Jelena, *Ko nas prisluškuje? (Kako funkcioniše zakonito presretanje elektronskih komunikacija i pristup zadržanim elektronskim podacima u Srbiji)* [Who controls the wire? (How does the lawful interception of electronic communication and access to retained electronic data function in Serbia)], Belgrade Centre for Security Policy, Belgrade, 2014, <http://www.bezbednost.org/Sve-publikacije/5663/Ko-nas-prisluskuje.shtml>.

15 Recital 11.

c. Dilemmas

There are also grey areas where it is unclear which legal act should apply. Although **civilian and military intelligence services** remain beyond the scope of EU law,[16] should they participate in criminal investigations such as, for example, in Serbia, then that aspect of their activities should be subject to the Law Enforcement Directive.[17]

Similarly, it is unclear whether **financial intelligence units** (FIU) should be subject to the GDPR, because they protect the common market, or LED, because they participate in the prevention, detection and investigation of the criminal offences of money laundering and terrorism financing. These bodies within member states are usually autonomous and independent intermediaries between financial institutions and law enforcement authorities.[18] They receive reports of suspicious transactions from banks and other entities obliged by the law (insurance companies, foreign currency exchange offices, auditors, etc.), analyse them and conduct financial investigations before passing the data to the police or prosecutors if they conclude that a criminal offence may have been perpetrated. In order to apply the Law Enforcement Directive, FIUs must a) have powers to prevent, detect and investigate criminal offences and b) process data for this purpose in a given case. If either of these conditions is not met, for example if the powers of the FIU are administrative,[19] or if the case at hand is a misdemeanour rather than a criminal offence, then the GDPR applies.[20]

Who applies the Law Enforcement Directive?

The LED defines competent authorities as controllers of personal data. However, controllers can appoint other bodies or third parties to process data on their behalf. For example, a court may appoint a forensic technician or expert witness to gather or analyse evidence that contains personal data. The processor is required to apply the GDPR and, in the contract for the service provided, the controller obliges them to adhere to specific standards of LED, such as the categorisation of data subjects, and gives them other instructions for personal data processing.

Controller – *a competent authority that, alone or jointly with others, determines the purposes and means of personal data processing.*

Processor – *a public authority, natural or legal person that processes personal data on behalf of the controller.*

16 Recital 14.
17 Sajfert, Juraj and Quintel Teresa, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", op. cit. p. 4.
18 In Serbia an equivalent to such bodies would be the Administration for the Prevention of Money Laundering within the Ministry of Finance.
19 In EU member states there are three models of FIUs: administrative, police and hybrid. Quintel, Teresa, "Follow the Money, If You Can. Possible Solutions for Enhanced FIU Cooperation under Improved Data Protection Rules", University of Luxembourg Law Working Paper Series No 2019/001, p. 7, <http://orbilu.uni.lu/bitstream/10993/38829/1/SSRN-id3318299.pdf>.
20 Ibid.

PERSONAL DATA PROTECTION

To which principles do competent authorities adhere when processing personal data?

- LAWFUL AND FAIR PROCESSING (the GDPR also requires that it be transparent): data processing is regulated by law and the controllers take into account the rights and interests of the data subject;
- LIMITED PURPOSE: every processing of personal data must have a specific purpose explicitly provided for by the law;
- DATA MINIMISATION: data that is excessive, inadequate or irrelevant for the purpose should not be processed (the GDPR contains a stricter requirement – only data *limited to what is necessary* to achieve the purpose);
- ACCURACY OF DATA: data that are (or have become) inaccurate are erased or rectified;
- TIME-LIMITED STORAGE: personal data are stored only for as long as their processing requires and are subsequently erased or rendered anonymous, so that the data subject can no longer be identified;
- INTEGRITY AND CONFIDENTIALITY: the controller must undertake such organisational and technical measures as necessary to protect personal data from unauthorised and unlawful processing, from accidental loss, damage or destruction.

A competent authority may make use of data gathered for one LED purpose for another LED purpose but only if it has the power to do so under EU or member state law and if this processing is necessary and proportionate to that purpose.[21]

What types of data are processed?

Like the GDPR, the Law Enforcement Directive pays special attention to sensitive categories of personal data and offers them additional protection. These include data the processing of which carries an additional risk for the rights of the data subject, such as potential discrimination. **Sensitive data** includes data on racial or ethnic origin, political opinions and philosophical beliefs, trade union membership, genetic or biometric data, data concerning health, concerning a person's sex life or sexual orientation. These data are processed only when this is permitted by law, to protect the vital interests of this or another person or where such data were manifestly made public by the data subject.[22] Additionally, the automatic profiling of persons based on sensitive categories of data leading to discrimination is prohibited.

The directive also insists that a distinction is made between data based on fact and data based on personal assessment. The latter should undergo more frequent review.

21 Article 4. For example, in a specific case the prosecutor may, after assessing necessity and proportionality, use the personal data collected for the purpose of investigation against a suspect for informing the public. On the other hand, the judge that mentions the full name of a rape victim, noting that the offence rendered this person HIV positive, would have violated the necessity and proportionality of further processing, even if they have legal power to disclose personal data collected for the purpose of imposing a sentence.
22 Article 10.

How is personal data protected?

In contrast to earlier sets of standards, the controller must, from the very outset of planning a filing system, consider how this will impact the privacy of the data subject and devise appropriate safeguards to protect their privacy (privacy by default). Protection of privacy must be an integral part of the system, device or programme that stores or processes data (privacy by design).23 Prior to the introduction of a new technology for data processing, the controller must conduct an assessment of its impact on personal data protection.

Every controller keeps a record of all categories of processing activities and is required to appoint a data protection officer. Such an officer helps their colleagues with advice on data protection, monitors the controller's compliance with the Directive and cooperates with the independent supervisory authority.

Keeping Logs of Processing Activities

In order to prevent misuse or make it more easily detectable afterwards, the LED requires logs to be maintained of every single data processing operation in an automated system: collection, alteration, consultation, disclosure including transfers, combination and erasure.24 This is a specific provision of the Directive with no counterpart in the GDPR.25 In particular, for consultation and disclosure, including transfer to third parties, logs are required to record who accessed the data, to whom it was disclosed or transferred, when and with what justification.

The logs are kept in order to protect the integrity of the data and enable oversight of the lawfulness of processing and can be used as evidence in disciplinary and criminal proceedings against an official who has misused or exceeded their authority. Examples of such misuse of powers might include accessing the personal data of a daughter's boyfriend or the data of an opposition politician, a pop star or a relative mixed up in criminal activity.

The best approach to keeping such logs is the use of software that generates indelible logs as this cannot be corrupted.26 The Directive does not define time-limits for how long the logs should be kept.

How long is personal data stored?

The Directive does not prescribe precise time limits for the retention of data, instead it leaves the definition of that obligation to the member states. One possibility is to establish fixed time limits in advance, at the end of which the data are erased. A second approach would be to periodically review the continued storage of data, for example, checking whether the

23 Krivokapić, Danilo et al. *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR,* op. cit. p. 7.
24 Article 25.
25 Sajfert, Juraj and Quintel, Teresa, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", op.cit, p. 15-17.
26 Since the introduction of logging for existing filing systems generally entails excessive costs or can jeopardise the functioning of the filing systems, the Directive allows member states to implement this requirement with an extended deadline – until 2023 or 2026.

data are still relevant or whether the original purpose has been fulfilled. To prevent this from remaining just another measure on paper, mechanisms must be put into place to ensure compliance with time limits, such as reminders or automatic erasure of data once the time limit has expired.[27]

RIGHTS OF THE DATA SUBJECT

Whose data can be stored according to the Law Enforcement Directive?

Competent authorities must differentiate between different categories of data subjects, whenever necessary and to the extent that is practicable. The Directive distinguishes between four categories of data subjects:

a. Persons for whom there are serious grounds to suspect that they have committed or are about to commit a criminal offence;[28]
b. Persons convicted of criminal offences;
c. Victims or very probable victims of a criminal offence;
d. Other parties to a criminal offence, such as witnesses, those who can provide information of criminal offences, contacts and those with links to persons referred to in points a), b) or c).

Categorisation requires the regular updating of data and should impact the setting of time limits for data retention, their further transfer and special consideration for vulnerable groups (e.g. victims of sexual violence, human trafficking, etc.).[29]

What rights do data subjects have?

The Directive guarantees several rights for data subjects, regardless of their nationality. However, the list of rights is narrower than that provided by the GDPR and there is usually a justifiable reason for these rights to be curtailed in the interests of criminal proceedings.

The data subject has the rights listed below, in the following order:

1. **The right to be informed on the processing of personal data**

   The controller is obligated to proactively provide the data subject with general information, for example on their official website, on the type of data processed, the purposes for processing, the rights that are guaranteed, how to exercise these rights by submitting a request to the controller or by filing a complaint with the supervisory

27 Article 29 Data Protection Working Party. *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, 29.11.2017, p. 5, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178>.
28 This first category includes suspects (grounds for suspicion at pre-trial proceedings), defendants (investigated on grounds of reasonable suspicion) and indictees (against whom an indictment has been issued). In Serbia's Law on Personal Data Protection (Article 9) a fifth category is added: persons suspected of having committed criminal offences, since Serbian law makes a distinction for grounds for suspicion (initial indications) and established suspicions (more specific indications).
29 Article 29 Data Protection Working Party. *Opinion 03/2015 on Draft Police Directive,* 1.12.2015, p. 7, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640460>.

authority, stating the required contact details of both the controller and the supervisory authority.

The controller is obligated to offer specific information about the data subject's case, proactively or on request. This includes information on the legal basis for processing the data, the retention period for the data, as well as the categories of the recipients of personal data. This information should be provided without charge. Exceptionally, when the requests by the data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a fee or reject the request. The controller is obligated to inform the data subject without undue delay if there has been a breach of their personal data which is likely to pose a high risk to their rights and freedoms.

2. **Right to access**

The data subject has the right to request and be granted access to the data held about them by the controller, including sensitive data, as well as information outlined in the preceding paragraph. This right does not include access to the document in which the personal data is contained, especially if that document contains the identity of confidential sources.

3. **Right to rectification**

If they become aware that the personal data stored by the controller is inaccurate, obsolete or incomplete, the data subject has the right to request that the controller correct or complete the data. The controller is obligated to act on this request without undue delay, unless an exception is provided for (see below).

4. **Right to erasure**

The data subject has the right to request from the controller to delete their personal data if the processing of such data violates the standards of the Directive (principles relating to the processing of data, lawfulness of processing and protection of sensitive data) or if the controller is legally obliged to delete such data. The controller is obligated to act upon this request without undue delay, unless an exception is provided for (see below).

5. **Right to restriction of processing**

If the data subject claims that the personal data relating to them is incorrect but cannot prove it or the procedure for proving this is ongoing, the data subject can request that the processing of these data is restricted. The controller will restrict processing also if the personal data must be maintained as evidence in criminal proceedings. Processing is limited only to the purpose for which the data were not erased. The relevant data must be appropriately marked and separated.

When can the rights of the data subject be limited?

The controller may limit the above listed rights of the data subject, in whole or in part, i.e. refuse to act upon their request, with adequate justification. However, in certain cases, even providing justification or confirming that the data have been gathered can jeopardise the purpose of processing the data. For example, access is requested by a person suspected of a serious crime who is lawfully subject to special measures of covert data collection, such as covert surveillance and recording, for the purpose of gathering evidence for criminal proceedings. Were this person to be given such justification, the measures undertaken and their purpose would be rendered meaningless.[30] In a case such as this, the controller may provide the data subject with a neutral response stating that they cannot act upon the request and inform them of the possibility to lodge a complaint with a supervisory authority or seek judicial remedy.

a. The competent authority will not provide reasons for rejecting a request if in that particular case the following conditions are met:
   1. The limitation is provided for by law;
   2. It has a legitimate purpose, as explicitly listed in the Directive:
   3. Avoiding obstruction of the ongoing official or legal inquiries;
   4. Avoiding prejudicing prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
   5. Protection of public security;
   6. Protection of national security;
b. Protection of the rights and freedoms of others;
c. It is necessary and proportionate to the realisation of the purpose, according to the standards of democratic society, with due respect for the basic rights and legitimate interests of the data subject.[31]

The limitation of rights must always be temporary in nature. This means that at some point the personal data will no longer be concealed from the person they concern as there is no longer a purpose for their concealment. For example, the investigation has been concluded or the threat to public or national security has been neutralised. At that moment the competent authority is obligated to inform the person concerned and provide them with access to the data or allow for their rectification, erasure or restriction of their processing.

Protection from the negative consequences of automated profiling

The person has certain rights pertaining to the decisions of competent authorities that have adverse legal effects concerning them or significantly affecting them and which are based solely on automated processing of data. Automated processing, including profiling, is performed by a machine without participation by a human operative. For example, due to adverse profiling a person is denied a visa or is denied entry to a country.

30 For more on this example, see: Pejić, Jelena, *Moja prava u slučaju (ne)zakonitog prisluškivanja* [My rights in case of (il)legal wiretapping], Lawyers Committee for Human Rights and Belgrade Centre for Security Policy, Belgrade, 2019., https://bit.ly/33vYwDj.
31 Article 15.

! *In such cases, the data subject should have the right to obtain human intervention – i.e. that an authorised official of the competent authority reviews how the software reached such a profile and ascertains whether an error occurred. The data subject should be allowed to express their opinion and to receive justification of the decision and to challenge the decision, but these issues are regulated by the member states through national legislation. In the event that the minimum of these rights are not guaranteed, automated processing with adverse effects for data subjects should be prohibited.*[32]

How can a data subject exercise and protect their rights?

The first step for data subjects is to submit a **direct request to the controller**. In the event that the controller, in the aforementioned circumstances, cannot act upon a request, they must inform the data subject.

Since these situations will in all likelihood occur frequently in practice, the Directive provides that the rights of the data subject may also be exercised **through an independent supervisory authority**.[33] In the procedure upon complaint lodged by the data subject, the supervisory authority shall have access to the records of the controller and the requested personal data. Since documents containing the requested data will frequently be classified to various degrees, this task is entrusted to an official of the supervisory body who has the appropriate security clearance. The supervisory authority assesses whether the processing of data is being conducted lawfully and informs the complainant of the outcome but cannot reveal the requested data if they have been withheld justifiably. In the event that the oversight procedure reveals irregularities, the supervisory authority shall undertake corrective measures and may involve judicial authorities.

The data subject also has the right to seek judicial remedy against the decisions of a supervisory authority, the right to seek material and non-material damages that have resulted from unlawful processing, as well as the right to seek representation by an non-profit organization in proceedings with a view of protecting their rights guaranteed by the Directive against the competent authorities of the member state.

32 Article 11, Recital 38.
33 Article 17.

INTERNATIONAL DATA TRANSFERS

Transfers of personal data to third countries or international organisations are permitted only if the following conditions are met:

1. PURPOSE: the transfer is necessary for purposes set out by the Directive.
2. RECIPIENT: the recipient is a competent authority authorised to process personal data for these purposes in the third country or international organisation, or in exceptional circumstances a private company (see below).
3. LEVEL OF PROTECTION: the transferred data are guaranteed an adequate level of protection. This condition is fulfilled if the European Commission has adopted an adequacy decision for that country, a particular sector within that country or international organisation. If such a decision is absent, the competent authority shall invoke an applicable international agreement or assess whether the recipient applies appropriate safeguards, except in special and urgent cases.[34]
4. CONSENT OF THE SOURCE COUNTRY: the member state from which the personal data originate has consented to the onward transfer and each further transfer of the data. Exceptionally, consent is not necessary in urgent cases but the source country must be informed of the transfer without undue delay.

Asymmetric data transfers

The RECIPIENT may in exceptional cases be a private company in a third country. This is permitted only in individual and specific cases, under the following conditions:

- *The transfer is strictly necessary for the exercising of lawful powers by the competent authority transferring data;*
- *The public interest for which the transfer is being conducted overrides the interest of protection of rights of the data subject (upon a decision of the competent authority in the event of, for example, a threat to that person's safety or if they are preparing a terrorist attack);*
- *Transfer to the competent authority in the third country is not effective nor appropriate to the purpose, nor could be conducted in a timely manner (upon a decision of the competent authority in the event of, for example, the competent authority in the third country could not be contacted, is corrupt or is overburdened);*
- *The competent authority in the third country is informed without undue delay about the transfer, except where it would not be effective or appropriate to the purpose;*
- *The recipient is informed of the specific purpose or purposes for the processing of transferred data.[35]*

This possibility has been retained primarily to combat cybercrime, which quickly and easily crosses borders and, in practice, there is a need for direct cooperation with large companies such as Microsoft, Google, Facebook and so forth.[36]

34 Articles 36-38.
35 Article 39, Recital 73.
36 Sajfert, Juraj and Quintel, Teresa, "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities", op.cit, p. 19.

OVERSIGHT OF THE LAW ENFORCEMENT DIRECTIVE'S APPLICATION

Who oversees whether law enforcement authorities are complying with the Law Enforcement Directive?

Each member state must have at least one independent supervisory authority to oversee the implementation of the Directive.[37] It may or may not be the same body that oversees implementation of the GDPR.

The Directive requires that this body be able to independently perform its tasks without any external influence, to have the necessary resources for this but also to be subject to external financial oversight. The members of the supervisory authority are appointed by means of a transparent procedure by the highest institutions of state for a term of no less than four years. Members must have the appropriate qualifications in the area of the protection of personal data and must hold no other post. Other details are regulated by the member states.

All supervisory authorities cooperate with one another and with the European Commission and participate in the European Data Protection Board, as the highest European body in the field of data protection.

How does an independent supervisory authority conduct oversight?

The powers of the supervisory authorities are defined by the national legislation of member states. The Directive provides some guidelines, minimal standards and requires that these powers be effective.

a. Advisory: provides opinions on draft regulations and on issues within its field of expertise, as well as on introducing new filing systems by the competent authority;
b. Investigative: the controller or processor shall at a minimum ensure access to all personal data and all documentation necessary for the performance of oversight;
c. Corrective: issues warnings of potential infringements of provisions of the Directive, may require the controller or processor to adhere to the Directive within a set timeframe, may require the correction or erasure of data or the restriction of the processing thereof, temporarily or permanently, including the prohibition of a specific processing.[38]

The competent authority is obligated to inform the supervisory authority and to provide all necessary documentation:

- If a breach of personal data has occurred that is likely to result in a high risk for the rights and freedoms of the data subjects, no later than 72 hours from the breach occurring;

37 In Serbia this is the Commissioner for Information of Public Importance and Personal Data Protection.
38 Article 47.

- On the categories of international transfers that have taken place on the basis of the competent authority's assessment of the appropriate safeguards put in place by the recipient;
- On each transfer to private companies in third countries.[39]

Courts and other independent judicial bodies fall outside of the jurisdiction of the supervisory authority when processing personal data while acting in their judicial capacity.

What are the penalties for violating the Law Enforcement Directive?

The listing of violations of obligations under the LED and the penalising thereof has been left to the legislatures of the member states. The Directive only requires that those penalties be effective, proportionate and dissuasive.

39 Aricles 30, 37 and 39.