Law Enforcement Directive Implementation Country Report: Bulgaria

Liubomir Nikiforov

EDRi
European Digital Rights

Law Enforcement Directive Implementation Country Report: Bulgaria

Liubomir Nikiforov

TABLE OF CONTENTS

1. Introduction

Before the transposition of the European Union's (EU) Law Enforcement Directive 2016/680 (hereinafter "the LED"),[1] Bulgarian law enforcement authorities followed the general rules of the Council Framework Decision 2008/977,[2] as well as Directive 95/46/EC. In addition, the different law enforcement authorities had issued sectoral bylaws aimed at regulating specific aspects of their personal data processing activities.

Bulgaria transposed the LED by amending its existing Data Protection Act (ZZLD)[3] on 26 February 2019, almost a year after the transposition deadline on 6 May 2018.[4]

Unlike the EU legislature, Bulgaria chose to integrate the LED-related provisions in its general data protection law, claiming that the adoption of a separate law dedicated to law enforcement data processing would lead to an "unnecessary fragmentation", potential inconsistency and legal uncertainty for data subjects and data controllers.[5] This approach was however criticised as potentially creating confusion[6] and increasing the overall complexity of the applicable data protection framework.[7] In practice, this may have led to Bulgarian national courts struggling to apply the correct set of norms[8] – in addition to the general problems with the scope of application of the LED identified in academic literature.[9]

After its revision, the ZZLD still allows law enforcement authorities to adopt additional bylaws in order to further clarify the application of the transposed provisions.

The authority responsible for the general supervision, control, and application of the ZZLD and every related bylaw is the Commission for Personal Data Protection (KZLD),[10] which is permanent and independent. It does not, however, supervise data processing by the judiciary, following the requirement of the LED.[11] This task is allocated to the Inspectorate to the Supreme Judicial Council

[1] 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 2016 (OJ L 119/89) 89.

[2] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008 (OJ L 350) 60.

[3] Personal Data Protection Act, published in the State Gazette, issue 1 of 4 January 2002, amended and supplemented in the State Gazette, issue 17 of 26 February 2019. (Закон за защита на личните данни, обн. ДВ, бр. 1 от 4 януари 2002 г., изм. и доп. ДВ, бр. 17 от 26 февруари 2019 г.) (ZZLD). In this report, the version from 6 October 2023 is used.

[4] The transposition of the Directive was initiated only on 30 April 2018. "Council of Ministers, Website for Public Consultations of Proposed Legislative Acts", https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=3467.

[5] ibid.

[6] ibid.

[7] It is a common national practice to favour the reference to other existing norms instead of repeating them in different legal acts, which was criticised by the European Commission as pointed out in the 2019 annual report by the Commission for Personal Data Protection (KZLD), "Annual Report of the Commission for Personal Data Protection on its Activities in 2019." (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2019 г.), p. 65-66, https://Cpdp.Bg/En/Annual-Reports/.

[8] In 2024, in Decision No 7002/7.06.2024, the Supreme Administrative Court (VAS) annulled a decision of the first instance court because the latter erroneously applied the LED technical requirements to the National Revenue Agency, whose data processing is regulated by the GDPR.

[9] Magdalena Brewczyńska, "A Critical Reflection on the Material Scope of the Application of the Law Enforcement Directive and Its Boundaries with the General Data Protection Regulation" in Eleni Kosta, Ronald Leenes and Irene Kamara (eds), Research Handbook on EU Data Protection Law (Edward Elgar Publishing 2022), https://www.elgaronline.com/view/edcoll/9781800371675/9781800371675.00013.xml.

[10] Commission for Personal Data Protection (Комисия За Защита На Личните Данни) (KZLD) https://cpdp.bg/.

[11] Article 45 LED transposed in Article 10 ZZLD.

(IVSS),[12] which oversees processing operations of courts and other independent judicial authorities when acting in their judicial capacity.

This research examines the Bulgarian data protection landscape in the area of law enforcement and the applicable national laws, bylaws, relevant national and EU jurisprudence. It first addresses the situation of data subject rights in Bulgaria, before focusing on the processing of special categories of personal data, the requirement for a specific legal basis, and compliance with the LED of new technologies used by Bulgarian law enforcement. Where necessary, the national legislation has been machine translated. For the elaboration of the report, extensive correspondence with relevant institutions, including access to public information requests, has been conducted, although access to information is limited due to normative security considerations.

2. Data subject rights

Already in 2019, the European Commission had highlighted the **lack of specific provisions in the Bulgarian legislation regarding the regulation of data subjects' rights**, and in particular their restrictions, which are permissible only when provided for by law and under defined specific conditions and procedures.[13]

Since the transposition, **the Bulgarian jurisdiction had to deal with at least one case of restriction of individuals' rights by law enforcement authorities**, which led to an important preliminary ruling by the Court of Justice of the European Union (CJEU). In case C-118/22,[14] an individual filed a complaint against the National Police Directorate-General at the Bulgarian Ministry of the Interior (the DGPN) concerning their refusal to delete their file – based on their legal rehabilitation after having been convicted by final judgment – from the national records in which the Bulgarian police authorities register persons prosecuted for an intentional criminal offence subject to public prosecution. **The CJEU found that the Bulgarian national legislation, which allowed biometric and genetic data to be stored until the person's death, regardless of the circumstances of the criminal case, had an "excessively broad" retention scope** which was applied "generally and indiscriminately to any person convicted by final judgment" and therefore was not "appropriate" (as required by Article 5 LED).[15] The CJEU also confirmed that a national legislation may not prohibit a person convicted by final judgment from exercising their data subject rights, notably the right to erasure as provided for by Article 16 LED.[16]

The following section provides an in-depth analysis of Article 54 ZZLD, implementing Article 13 LED on information to be made available or given to the data subject. The report focuses on this particular provision because the right to information is the pre-condition for exercising all subsequent data subject rights, and its transposition exposes the most evident systemic transposition and implementation flaws by Bulgaria of the LED, such as a lack of development of the original text and the use of vague and undefined notions. Moreover, unlike Article 54, Articles 55-56 ZZLD (mirroring Articles 14-16 LED) have generated virtually no known KZLD decisions or substantive court rulings, offering little empirical material for analysis. Therefore, focusing on Article 13 allows this study to use concrete textual divergences and available sources to demonstrate how these deficiencies permeate the entire Bulgarian data protection framework in the law enforcement area.

[12] Inspectorate to the Supreme Judicial Council (Инспекторат Към Висшия Съдебен Съвет) (IVSS) https://www.inspectoratvss.bg/.
[13] "Annual Report of the Commission for Personal Data Protection on Its Activities in 2019." (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2019 г.), https://Cpdp.Bg/En/Annual-Reports/ (n 7)., p. 66
[14] Judgement of 30 January 2024, Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR - Sofia, Case C-118/22, EU:C:2024:97 (Court of Justice of the European Union).
[15] par. 67-70
[16] par. 71

2.1 Article 13 - Information to be made available or given to the data subject (par. 1 and 2)

Article 13 LED regulates what type of information data subjects are entitled to be given access to and the limitations to this right. Article 54 ZZLD is virtually a literal translation of Article 13 with the **added obligation to inform data subjects about their right to lodge a complaint if denied access to the additional information under par. 2 (Art. 54 (1) point 6 ZZLD).** The provision reads as follows:

(1) The controller shall provide the data subject with at least the following information: *1. The data identifying the controller and the contact details;* *2. The contact details of the data protection officer, where applicable;* *3. The purposes for which the personal data is processed;* *4. The right to lodge a complaint with the commission or, where applicable, with the inspectorate, along with their contact details;* *5. The right to request from the controller access to, correction, supplementation, or deletion of personal data, as well as the restriction of the processing of personal data related to the data subject;* *6. The possibility, in case of refusal under paragraph 3, Article 55, paragraphs 3 and 4, and Article 56, paragraphs 6 and 7, to exercise their rights through the commission or, where applicable, through the inspectorate.*

Table 1

In the subsequent paragraph, the Bulgarian legislator has transposed almost literally the text of the LED (Article 13(2)) regarding "specific cases" in which additional information has to be provided.[17]

However, **Article 54 (2) ZZLD introduces a nuance compared to the LED as regards the duty of the data controller to provide the additional information in a proactive manner.** The article reads as follows:

*(2) In addition to the information under paragraph 1, **upon request of the data subject or on its own initiative**, the controller provides the data subject, in concrete cases and for the purpose of enabling the exercise of their rights, with the following additional information:* *1. The legal basis for the processing;* *2. The period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;* *3. Where applicable, the recipients or categories of recipients of the personal data, including in third countries or international organisations;* *4. Where necessary, any other additional information, particularly in cases where the personal data has been collected without the knowledge of the data subject.*

Table 2

As a result, **the Bulgarian text is ambiguous as to whether and under which circumstances the data controller is expected to pro-actively provide the listed information or whether the data subject has to request it first**.

As noted in academic literature,[18] the wording of Article 13(2) LED suggests that the data controller should make sure that the information reaches the data subject, as opposed to the wording of paragraph 1, where the controller should simply make it available (e.g. on its website).[19] **This difference in the LED is not reflected in the Bulgarian law, as in both instances the controller is required to "provide" the information.** At the time of writing this report, it is impossible to

[17] Article 13 (2) of the LED mentions the legal basis, the storage period or the criteria used to determine that period, the recipients of the data as well as further information, particularly for cases where the data is collected without the data subject's knowledge.

[18] Gloria González Fuster, "Article 13: Information to Be Made Available or given to the Data Subject" in Eleni Kosta and Franziska Boehm (eds), The EU Law Enforcement Directive (LED): A Commentary (Oxford University Press 2024), p. 261, https://doi.org/10.1093/law/9780192855220.003.0013.

[19] "The controller to give to the data subject", Art. 13 (2), compared to Art 13 (1), "the controller to make available to the data subject".

determine the effects of this semantic divergence from the review of national law and jurisprudence.

Furthermore, because the Bulgarian legislator simply transposed the original text of the LED, **the national legislation does not develop in more detail which "specific cases" warrant data subjects' access to additional information.** The intention of Article 3(2) LED is to provide individuals further means to exercise their fundamental rights, especially when they are subject to data processing operations without their knowledge. The wording of the Bulgarian law seems to enable law enforcement authorities to provide more information on a case-by-case basis, in the absence of a defined set of cases.

The mere fact that individuals can request this information does not meet the safeguard intended by the Directive, as it is questionable that they would do so, especially when data collection is done without their knowledge. The transposed text should be deemed unclear and potentially prone to arbitrary interpretation. **As such, the Bulgarian transposition of Article 13 LED under Article 54 ZZLD appears to fall short of meeting the objective of the LED.**[20]

2.2 Restriction on the provision of information (par. 3 and 4)

As regards derogations to the controller's obligation to make available or give information to the data subject, regulated by Article 13(3) LED, **the Bulgarian legislation provides more discretion to law enforcement authorities than originally foreseen by the EU Directive.** The provision reads as follows:

(3) The controller may delay or wholly or partially refuse to provide the information under paragraph 2 when necessary to: *1. Avoid obstructing official or legally regulated inspections, investigations, or procedures;* *2. Avoid adversely affecting the prevention, detection, investigation, or prosecution of crimes or the execution of penalties;* *3. **Protect public order and security**;* *4. Protect national security;* *5. Protect the rights and freedoms of others.* *(4) Upon the cessation of the circumstance under paragraph 3, the controller shall provide the requested information without delay within the period specified in Article 53, paragraph 3.* *(5) When making a decision under paragraph 3, **the controller shall consider the fundamental rights and legitimate interests of the affected individual.***

Table 3

Contrary to the criteria of the LED, **the transposition fails to mention the principles of necessity and proportionality** when law enforcement authorities choose to restrict the disclosure of information to individuals whose personal data is processed. Article 54(5) ZZLD, however, mandates that the controller should consider the fundamental rights and "legitimate" interests of the affected data subject.

It can also be noted that **the Bulgarian legislator added "public order" as a ground for restricting the provision of information** (coupled with "public security" under point 3), whereas the LED solely mentions "public security". Based on the examination of relevant legal sources,[21] "public order" could be understood as an act against the established social and legal order, "socially dangerous",

[20] No provisions in relevant laws, such as the Law on the Ministry of the Interior (Arts. 25-28) or the Regulations for the organisation of the activities of the Inspectorate at the Supreme Judicial Council (Chapter VI (a)) could be found in order to refute this conclusion.

[21] Decision No 7 of 4 June 1996 on Constitutional Case No 1/96, Constitutional Court (Решение № 7 от 4 юни 1996 г по кд № 1/96 г, Конституционен съд); Law on Combating Antisocial Behaviour of Minors and Juveniles, published in the State Gazette, issue 13 of 14 February 1958, amended in the State Gazette, issue 101 of 27 December 2019. (Закон за борба срещу противообществените прояви на малолетните и непълнолетните, обн. ДВ, бр. 13 от 14 февруари 1958 г., изм. ДВ, бр. 101 от 27 декември 2019 г.); Criminal Code, published in the State Gazette, issue 26 of 2 April 1968, amended in the State Gazette, issue 42 of 14 May 2024. (Наказателен кодекс, обн. ДВ, бр. 26 от 2 април 1968 г., изм. ДВ, бр. 42 от 14 май 2024 г.)., Art. 325

unlawful or "morally reprehensible" because of its disrespect towards society. It is a broad term potentially encompassing a wide range of behaviours and actions. **However, there is no official legal definition of the term in national law, nor is it the case for "public security" or the combination of terms "public order and security".** The European Commission pointed out this conceptual discrepancy to the KZLD in 2019.[22]

Moreover, there is no legislation in Bulgaria determining the time period for surveillance and other law enforcement measures ensuring the protection of public order or national security. While threats to national security could theoretically be more clearly identified and consequently eliminated, threats to the public order are excessively broad and could be considered permanent. Thus, those vague provisions directly condition the exercise of data subjects' rights and place them under the discretion of law enforcement authorities.

In general, the European Commission's 2019 criticism is still valid as concerns the lack of specific provisions in the Bulgarian legislation regarding the restriction of data subjects' rights, which are permissible only when provided for in a specific law (not a bylaw, such as an instruction or ordinance) laying out the specific conditions and procedures for their application.[23] **At the time of writing, no such law or provisions in a law exist. This study did not identify any relevant national case law on the application of existing provisions or any assessment of their proportionality by relevant national bodies.**

Lastly, in accordance with Article 13(4) LED,[24] Bulgaria identified categories of processing for which the provision of additional information can be restricted in Article 4 of the Instruction No. 8121z-1280/7.10.2021.[25] However, the Instruction simply lists internal rules for databases managed by the Ministry of the Interior (MVR).[26] As a result, the Bulgarian legislator applies the possibility to restrict the provision of additional information for all databases managed by the Ministry – which likely involves a high number of data categories and of data processing operations. **Bulgaria's broad application of the possibility of restriction illustrates how the LED (notably its Article 13(4)) provides Member States with a wide discretionary power in refusing to comply with data subjects' rights.**

3. Legal basis

The requirement of the lawfulness of processing personal data for the purposes of the Directive (Article 8 LED) is transposed under a new Article 49 in the ZZLD. In its evaluation of the LED, the Commission underlined that "merely repeating the general requirements of Article 8 LED in national law cannot be considered a sufficient legal basis for a specific processing operation".[27]

---

[22] "Annual Report of the Commission for Personal Data Protection on Its Activities in 2019." (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2019 г.) Https://Cpdp.Bg/En/Annual-Reports/ (n 7)., p. 66

[23] ibid., p. 66

[24] Paragraph 4 allows Member States to adopt legislative measures determining categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

[25] In the information repositories of the Ministry of the Interior, the following categories of personal data are processed, categorised by their source:
"- data provided by the data subjects;
- data collected by Ministry of the Interior bodies in the exercise of their statutory powers;
- data received from other authorities or organisations;
- data received from other EU Member States, from the States party to the Agreement on the European Economic Area, and from the Swiss Confederation, as well as from EU bodies, institutions and agencies;
- data received from third countries or international organisations, including under international treaties to which the Republic of Bulgaria is a party."

[26] Instruction No. 8121z-1280 of 7 October 2021 on the procedure for processing personal data in the Ministry of the Interior, published in the State Gazette, issue 87 of 19 October 2021. (Инструкция № 8121з-1280 от 7 октомври 2021 г. за реда за обработване на лични данни в Министерството на вътрешните работи, обн. ДВ, бр. 87 от 19 октомври 2021 г.).

[27] "Communication from the Commission to the European Parliament and the Council, First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ("LED") COM/2022/364 Final, 25.07.22"., p. 14

Yet, **Article 49 ZZLD is an almost literal translation of Article 8 LED, as the following translation shows:**

The processing of personal data is lawful when it is necessary for the exercise of powers by a competent authority for the purposes under Article 42, paragraph 1, and is provided for in the law of the European Union or in a normative act specifying the purposes of the processing and the categories of personal data processed.

Table 4

A closer look at the wording suggests a broader interpretation of the grounds for processing by Bulgarian authorities. The Directive reads "only **if and to the extent** that processing is necessary",[28] while the national law only refers to "lawful **when** it is necessary for the exercise of powers by a competent authority". Hence, the requirement for processing under Article 8 LED seems stricter than the wording of Article 49 ZZLD.

While general purposes of data processing can be found in Article 42(1) ZZLD, each specific processing operation still requires an additional legal basis. There is no additional provision in the ZZLD which fulfils this requirement. **An exploration of relevant sectoral legislation did not lead to conclusive results.** For example, the Law on the Ministry of the Interior (ZMVR)[29] in its Article 26 does not provide any additional detail. On the contrary, Article 26(1) point 3 is equally broad as the ZZLD, stating that the police can "process all necessary categories of data" without further defining them.[30] In an access to information request, the MVR confirmed that the authority processes "all necessary" data.[31] In an additional request, the Ministry confirmed again that "all necessary categories of data" are collected without going into further detail about the categories.[32] The Instruction № 8121z-1280/7.10.2021 regulating the data processing at the MVR develops neither the categories of data nor the purposes for processing.[33]

Likewise, Article 24(1) ZMVR, which concerns "Information funds and units for collecting, processing, systematising, storing, analysing, preparing, and providing information are established within the Ministry of the Interior", fails to meet the requirements of Article 8 LED in that context. **No other relevant legislation could be found defining the specific purposes for the collection of personal data, nor the categories thereof.**

The striking absence of clearly defined purposes pursued by law enforcement authorities and the lack of explanation for the reasons why such purposes justify data processing in Bulgarian sectoral law were also part of Advocate General Pitruzzella's Opinion in case C-205/21 (discussed in more detail in the next section of this report).[34] In point 61, he indicated that: "Even if the purposes allegedly pursued by the creation of a police record appeared to be consistent with those referred to in Article 1(1) of Directive 2016/680, **national law neither established nor specified the links between the scope of the collection** – either in terms of the number of data subjects or the amount of data collected and processed – **and the purposes pursued**" (emphasis added).

When it comes to the transposition of Article 8 LED, the Bulgarian data protection and sectoral laws fail to adopt the necessary safeguards and requirements in order to comply

[28] In the Bulgarian translation of the LED, the text is literally translated from English: "само ако и доколкото то е необходимо", https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016L0680

[29] Law on the Ministry of the Interior, published in the State Gazette, issue 53 of 27 June 2014, amended and supplemented in the State Gazette, issue 19 of 5 March 2024. (Закон за Министерството на вътрешните работи, обн. ДВ, бр. 53 от 27 юни 2014 г., изм. и доп. ДВ, бр. 19 от 5 март 2024 г.) (ZMVR).

[30] Art. 26 (1) point 3 (amended - State Gazette, issue 17 of 2019) allows processing of all necessary categories of personal data. (Чл. 26 (1) точка 3 (изм. - ДВ, бр. 17 от 2019 г.) Могат да обработват всички необходими категории лични данни.).

[31] "Access to Public Information Request to the MVR Reg. No 812104-301-1/23.07.2024".

[32] "Access to Public Information Request to the MVR Reg. No 812100-14113-1/29.07.2024".

[33] Instruction No. 8121z-1280 of 7 October 2021 on the procedure for processing personal data in the Ministry of the Interior, published in the State Gazette, issue 87 of 19 October 2021. (Инструкция № 8121з-1280 от 7 октомври 2021 г. за реда за обработване на лични данни в Министерството на вътрешните работи, обн. ДВ, бр. 87 от 19 октомври 2021 г.).

[34] Opinion of Advocate General Pitruzzella delivered on 30 June 2022, VS v Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2022:507., par. 58-61.

with the standards set forth in the Directive. **This means that Bulgarian law enforcement authorities are granted a broad margin of manoeuvre when processing data.**

4. Sensitive personal data

As regards special categories of data, the Bulgarian legislator literally translated Article 10 LED in Article 51 ZZLD, which reads as follows:

1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data related to health or sexual life and sexual orientation of the person is permitted when it is absolutely necessary, appropriate safeguards for the rights and freedoms of the data subject are in place, and it is provided for under the law of the European Union or the legislation of the Republic of Bulgaria.
(2) When the processing referred to in paragraph 1 is not provided for under the law of the European Union or the legislation of the Republic of Bulgaria, the data referred to in paragraph 1 may be processed when it is absolutely necessary, appropriate safeguards for the rights and freedoms of the data subject are in place, and:
1. the processing is necessary to protect the vital interests of the data subject or of another natural person, or
2. the processing relates to data that has clearly been made public by the data subject.
(3) When processing the data referred to in paragraph 1, appropriate measures and safeguards shall be applied to prevent discrimination against natural persons.

Table 5

Additional information is contained in a section titled "Additional provisions", points 11-13, concerning "genetic data", "biometric data" and "data concerning health", which refer to the definitions in the GDPR's Article 4 (13-15). The ZMVR refers to Art. 51 ZZLD in its Art. 25a.

Most importantly, several legal proceedings in Bulgaria led to crucial interpretations of Article 10 LED by the CJEU. Indeed, cases C-205/21 and C-80/23 offered an opportunity for the Court to interpret key concepts and clarify specific requirements for the processing of sensitive data, in particular biometric and genetic data, such as the concept of "strictly necessary".

4.1 Cases C-205/21 and C-80/23

The ruling in C-205/21[35] stems from a case involving an individual accused of participating in a criminal organisation. The accused was asked to cooperate in the creation of a police record. The person refused to consent to the collection and recording of their fingerprints and photographic data, as well as their DNA profile. The police thus requested an authorisation from the referring Bulgarian court in order to enforce the collection of the data.

In this context, the Bulgarian court requested a preliminary ruling to the CJEU concerning the compatibility of the applicable national law in matters of police record creation with EU law. In particular, the referring court had doubts concerning the interpretation and application of the Bulgarian provisions transposing Article 10 LED. In addition, the national court had concerns related to the appropriate evaluation of the necessity and proportionality of the biometric and

[35] Judgement of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, Case C-205/21, EU:C:2023:49 (Court of Justice of the European Union).

genetic data collection for the purpose of police record creation, especially where those are forcibly collected.

The decision provided by the CJEU is highly relevant, not only for the interpretation of the LED, but also for the Bulgarian legislation and law enforcement's routine practice of collecting sensitive personal data for the purpose of prosecuting criminal acts. Indeed, all persons accused of intentional offences subject to public prosecution in Bulgaria were, until then, compulsorily registered in police records. In the context of such registration, all their personal data, among which, photographs, fingerprints and DNA samples, were collected **– regardless of the relevance of the biometrics collection for the criminal offences prosecuted and of their seriousness.** The Court reached three relevant conclusions for the Bulgarian law and law enforcement practices.

First, the CJEU found that the Bulgarian legislation does not need to expressly include provisions on special categories of data for the purposes of law enforcement if it already contains legal provisions that can be interpreted "in a sufficiently clear, precise and unequivocal manner" as applying to processing falling within the scope of the LED. Since the Bulgarian law was unclear about the application of existing data protection provisions to law enforcement data processing operations, the Court entrusted the Bulgarian court to interpret them as applying to such operations. As a result, the Bulgarian legislator should clarify distinctions between provisions that apply to the GDPR and provisions that transpose the LED.

Second, the Court established that if a person accused of an intentional offence subject to public prosecution refuses to have their biometric and genetic data collected for the purposes of a record, the national criminal court may authorise an enforcing measure. This may happen without reviewing the severity of the alleged grounds for the prosecution provided that an effective judicial review is guaranteed under national law afterwards.

Third, **law enforcement authorities are not allowed to carry out a systematic collection of biometric and genetic data**. According to the LED, the collection of special categories of data must indeed be "strictly necessary" for the specific objectives pursued by the public prosecution. This means that there must be no other less intrusive means to achieve such objectives just as effectively. Furthermore, the "strictly necessary" criterion requires taking into account the specific importance of the objective that the processing of sensitive data is intended to achieve and its specific circumstances.

Shortly after the publication of the ruling on C-205/21, the same judge followed up with a new request for a preliminary ruling with regard to the same proceedings.[36] In essence, what the Bulgarian court inquired in C-80/23 is, on one hand, a clarification of the decision C-205/21 concerning the requirement for "strict necessity" under Article 10 LED, and on the other hand, a clarification of paragraphs 100-101 and 132-133 of the ruling of C-205/21, which concern the potential judicial review of sensitive data collection from an accused at the investigation stage of criminal proceedings.

In its judgment, the CJEU ruled that the assessment of strict necessity must be carried out by the competent authorities (e.g. police) themselves. It confirmed that a court, which is asked by the police to enforce the data collection because the suspect has opposed it, cannot carry out that assessment in place of the police. National legislation, which fails to impose on competent authorities the obligation to verify whether and demonstrate that their collection of special categories of data is strictly necessary, does not comply with EU law (par. 58).[37]

Given that background, the following lines are divided into two parts. First, the transposition of the requirement for strict necessity will be analysed, before then exploring the respective provisions incorporating biometric and genetic data. Consequently, the Bulgarian legislator should adapt the police registration procedure to follow the principles established in the EU data protection law.

[36] Request for a preliminary ruling of 14 February 2023, VS v Ministerstvo na vatreshnite raboti, C-80/23 (Court of Justice of the European Union).
[37] Judgment of 28 November 2024, VS v Ministerstvo na vatreshnite raboti, C-80/23, ECLI:EU:C:2024:991 (Court of Justice of the European Union).

4.1.1. Strictly necessary

In Case C-205/21, the requirement of strict necessity[38] is interpreted as "establishing strengthened conditions" to process sensitive data.[39] According to the ruling, special categories of data processing require "a certain degree of seriousness" of the investigated offence.[40]

The objective that justified the processing of genetic and biometric data should, however, be defined "sufficiently precisely and specifically" in national law.[41] As confirmed in case C-205/21, this leads to the conclusion that any systematic collection of sensitive data is contrary to Article 10 LED.[42]

When it comes to the Bulgarian law, the ZZLD does not further elaborate on the original provisions of the LED. Article 25a (1) ZMVR repeats the same provisions by referring to the ZZLD, Article 51, and the GDPR, Article 9. Paragraph 2 of Article 25a ZMVR requires that "personal data under paragraph 1 is collected only in connection with other data concerning the affected individual". This, however, does not provide further elements of definition to determine the specific necessity for which sensitive data should be collected. As pointed out in the request for a preliminary ruling of the Bulgarian judge, it appears that there is a contradiction between Article 25a, which by virtue of the LED limits special categories of data processing, and Article 68 of the ZMVR, which imposes the collection of biometric and genetic data, as this is a prerequisite for the creation of police records.

The Ordinance for the Procedure of Conducting and Removing Police Registration (NRISPR) (which can be considered a sectoral bylaw) is supposed to be more specific.[43] Article 3(1) NRISPR specifies that police authorities carry out a registration of persons who have been accused of a premeditated crime of a public nature.[44] Given that the vast majority of crimes in the Bulgarian Criminal Code (NK) are of a public nature,[45] it allows authorities to include almost all suspected individuals in police records.[46] The category of "public" crimes encompasses a large spectrum of offences, such as theft and other petty crimes, tax violations and murder. Therefore, although the limitation to crimes of a public nature in the NRISPR may seem to narrow the purposes for

---

[38] The linguistic difference between the English version where "strictly" accompanies "necessary" is not discussed here because it has been done elsewhere. Provided that, according to Advocate General Pitruzzella, the use of "strictly or "absolutely" does not result in diverging interpretations of the text, this study assumes that "strict" and "absolute" necessity designate the same requirement. See Opinion of Advocate General Pitruzzella delivered on 30 June 2022, VS v Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2022:507 (n 34)., par. 49

[39] Judgement of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, Case C-205/21, EU:C:2023:49 (n 35)., par. 117

According to the Advocate General Pitruzzella's Opinion, only cases involving serious crimes allow the processing of "special categories" of data. See Opinion of Advocate General Pitruzzella delivered on 30 June 2022, VS v Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2022:507 (n 34)., par. 58

[40] Judgement of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, Case C-205/21, EU:C:2023:49 (n 35)., par. 127

[41] ibid., par. 124

[42] ibid., par. 128-130

[43] Ordinance for the Procedure for Conducting and Removing Police Registration, published in the State Gazette, issue 90 of 31 October 2014, amended in the State Gazette, issue 57 of 28 July 2015. (Наредба за реда за извършване и снемане на полицейска регистрация, обн. ДВ, бр. 90 от 31 октомври 2014 г., изм. ДВ, бр. 57 от 28 юли 2015 г.) (NRISPR).

[44] Article 3(1) Police authorities carry out police registration of persons who have been charged with committing an intentional publicly prosecutable crime. (Чл. 3. (1) Полицейските органи извършват полицейска регистрация на лица, които са привлечени като обвиняеми за извършено умишлено престъпление от общ характер.)

[45] The distinction between crimes of a public and private nature under the Bulgarian Criminal Code (NK) depends on whether the prosecution requires a complaint by the injured party. Crimes explicitly listed as requiring such a complaint are of a private nature; all others are deemed "public" and prosecuted ex officio by the public prosecutor due to their broader societal impact. Private nature offences typically involve relatively low public danger such as insult, defamation, or minor bodily harm, whereas public ones include theft, robbery, murder, possession or distribution of narcotic substances, driving a motor vehicle under the influence of alcohol or drugs, bribery, causing death by negligence, tax crimes, embezzlement, and others. The NK only contains 27 offences of a private nature, representing approximately 5% of the NK. All remaining criminal offences are "public" by default.

[46] Only minors and juveniles are not subject to police registration (Article 4 NRISPR).

biometric collection, in reality, it mandates a very broad collection of biometric data. This raises the question of compliance with the principle of necessity.

Furthermore, there is no differentiation between categories of crimes according to their "degree of seriousness" which could enable compliance with the LED requirement. There is also no provision permitting the police to assess the gravity of the case or the necessity of the processing of the data, sensitive or not, as its collection is compulsory for police registration by law (Article 68 ZMVR). Police registration is therefore inevitably carried out by law enforcement authorities whenever there is an accusation of a crime subject to public prosecution. Consequently, the Bulgarian legislator should amend the ZMVR and adapt the police registration procedure so that it follows the principles established in EU data protection law.

4.1.2 Biometric and genetic data

Police registration includes compulsory biometric and genetic data collection (Article 6(1) points 4 and 5, NRISPR), consisting of taking fingerprint impressions and oral DNA profile collection.[47] Police records contain special categories of data as defined by the ZZLD, which refers to the GDPR for the definitions of genetic and biometric data. The same procedure and the same data categories are collected anew every time "an individual is accused of intentional crime of a general nature, regardless of any previous registrations". New fingerprint impressions are taken if three years have passed since the last registration.[48] This approach is problematic for the following two reasons.

As explained in the section above, the majority of crimes under the Bulgarian Criminal Code are of a public nature. There is no differentiation during police registration between different crime categories based on their "degree of seriousness". Therefore, the (special categories of) personal data collected for police registration of a murder suspect is the same as for drink-driving. As paragraph 130 of the C-205/21 judgment states: "the mere fact that a person is accused of an intentional criminal offence subject to public prosecution cannot be regarded as a factor that in itself enables it to be presumed that the collection of his or her biometric and genetic data is strictly necessary."

The persistent data collection by Bulgarian law enforcement authorities was also declared unlawful in a national legal proceeding. Decision N°6225/26.10.2022 of the Sofia Administrative Court confirmed the illegality of the systematic and repeated sensitive data collection in a case involving an individual accused of a crime in 2020. A police record including sensitive data was created on that occasion. One year later, the person was requested to provide the same data again, but also fingerprints and DNA.

The Administrative Court's decision highlighted the lack of legal basis for the practice of repeated police record creation and therefore the non-compliance with the "absolute necessity" criterion under Article 51 (2) ZZLD. During the court hearing, the MVR claimed that the second data collection was lawful because no genetic data had been collected during the first police record. However, the Court rejected this argument.

---

[47] Ordinance for the Procedure for Conducting and Removing Police Registration, published in the State Gazette, issue 90 of 31 October 2014, amended in the State Gazette, issue 57 of 28 July 2015. (Наредба за реда за извършване и снемане на полицейска регистрация, обн. ДВ, бр. 90 от 31 октомври 2014 г., изм. ДВ, бр. 57 от 28 юли 2015 г.) (NRISPR).

[48] NRISPR Art. 13 (1) Police registration is carried out for each instance of a person being charged with committing an intentional publicly prosecutable crime, regardless of any previous registration, by completing a new police registration card and taking a new photograph. (2) New fingerprinting is conducted if more than three years have passed since the last existing registration. (Чл.13 (1) Полицейска регистрация се извършва за всяко привличане на лице като обвиняем за извършено умишлено престъпление от общ характер независимо от предишна такава, като се попълва нова карта за полицейска регистрация и се извършва ново фотографиране. (2) Ново дактилоскопиране се извършва, ако са изминали повече от три години от последната съществуваща регистрация.)

This conclusion was confirmed by the Supreme Administrative Court (VAS) in its decision N°10522/2.11.2023 on Administrative Case N°140/2023, which held that:

"... it is not the initial police registration, but the repeated one, that constitutes unlawful processing ... as there is no legal regulation for its implementation. The absolute necessity required by Article 51 in the Personal Data Protection Act for processing ... genetic data has not been established ... It should only be supplemented by the finding of the judgment of the Court of Justice of the European Union in Case C-205/21, that national regulations which provide for systematic collection, for the purposes of their registration, of biometric and genetic data from any person accused of a deliberate crime of a general nature, without providing for an obligation for the competent authority to verify and demonstrate, on the one hand, that the collection of this data is absolutely necessary for achieving the specific pursued purposes and, on the other hand, that these purposes cannot be achieved through measures that affect to a lesser extent the rights and freedoms of the respective person, are not permissible."[49]

Bulgarian courts, the KZLD and the MVR are aware of the challenges current police records regulation poses as well as its divergence from the LED requirements. It is concerning that no substantial modification to the Bulgarian legislation was made in order to achieve compliance with EU law and that the collection of special categories of data is, without evidence to the contrary, still practically systematic and generalised.

In addition, the retention of collected data is virtually indefinite in Bulgaria. This is apparent from national jurisprudence. In Decision N°6758 the Supreme Administrative Court (VAS)[50] based its conclusions on the interpretation of national law but also on the interpretation provided by the CJEU in case C-118/22.[51] The CJEU held that Article 4(1)(c) and (e) of the LED prohibits national legislation that allows indefinite storage of personal data, including biometric and genetic data, of convicted persons without periodic review or the right to erasure or restriction when the data is no longer necessary for its original purpose. The national legal provision foreseeing the deletion of personal data only at the death of the individual concerned, and even when rehabilitation has been applied, is unlawful. In this context, the VAS found that an assessment of "the nature and gravity of the crime for which the person has been convicted with an effective sentence, the context in which this crime was committed, its possible connection with other current proceedings, the background or profile of the convicted person, as well as other special circumstances which are known to the authority related to this person, including in relation to an essential necessity of prevention of dangerous acts to society" is necessary for the denial of the deletion request. The VAS's decision, dated from 4 June 2024, also points out that at the date of the decision, the principles of the LED which require data processed to be adequate, relevant and not excessive (Article 4 (1)(c)) as well as kept for no longer than necessary (Article 4 (1)(e)) had not been transposed into national legislation. The Annual Report of the KZLD from 2023 refers to a case where the data of a citizen has been unlawfully stored by the MVR for more than 15 years, and only by chance did the citizen gain knowledge of that situation.[52]

---

[49] Decision No 10522 of 2 November 2023 of the Supreme Administrative Court (VAS) on Administrative Case No 140/2023 (Решение № 10522 от 2 ноември 2023 г на ВАС по административно дело № 140/2023).
„... не първоначалната полицейска регистрация, а повторната такава представлява незаконосъобразно обработване на лични данни по смисъла на чл. 45, ал. 1, т. 1 ЗЗЛД, защото няма законова регламентация за нейното извършване. Не е установена и изискуемата абсолютна необходимост по чл. 51 ЗЗЛД за обработване генетичните данни ... Следва единствено да бъде допълнено установеното с решение на Съда на Европейския съюз по дело C-205/21, че не е допустима национална уредба, която предвижда системно събиране за целите на регистрацията им, на биометрични и генетични данни от всяко лице, привлечено като обвиняем за умишлено престъпление от общ характер, без да предвижда задължение за компетентния орган да провери и докаже, от една страна, че събирането на тези данни е абсолютно необходимо за постигането на конкретните преследвани цели и от друга страна, че тези цели не могат да бъдат постигнати чрез мерки, които засягат в по-малка степен правата и свободите на съответното лице."
[50] Decision No 6758 of 4 June 2024 of the Supreme Administrative Court (VAS) on Administrative Case No 6492/2021 (Решение № 6758 от 4 юни 2024 г на ВАС по административно дело № 6492/2021).
[51] Judgement of 30 January 2024, Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR - Sofia, Case C-118/22, EU:C:2024:97 (n 14).
[52] "Annual Report of the Commission for Personal Data Protection on Its Activities in 2023." (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2023 г.), p. 27-31, https://Cpdp.Bg/En/Annual-Reports/.

In conclusion, **the issue of unlawful data collection and retention by Bulgarian law enforcement authorities was repeatedly addressed by both national and European jurisdictions. However, the enforcement of the rulings seems to be crucially lacking as the national legislation is still not amended accordingly, and these data processing operations continue to be common practice.**

Additionally, it should be noted that while Bulgarian identification documents already contain biometric data,[53] such as the face of the person and their fingerprints,[54] this biometric data is also automatically stored in a central database, under Article 65 of the Bulgarian law on identity documents (along with other identification data collected for the purpose of issuing the identity document). Although the central database is supposed to be kept separate and independent from other databases, Article 67 of the same law introduces a possibility to derogate from this requirement, if provided for by law. This can be regarded as a broad derogation and a very low threshold for repurposing the data this database collects and stores. In fact, law enforcement authorities can access that biometric data, even though not collected for law enforcement purposes, pursuant to the LED and the ZZLD, as well as other national legislation such as the ZMVR.[55]

5. New technologies

The use of new technologies by Bulgarian law enforcement authorities suffers from a serious lack of transparency, which critically limits public scrutiny.[56] The only public document explicitly referring to new technologies is the "Concept for the development of AI in Bulgaria until 2030", published in 2020.[57] It outlines the challenges and objectives of the public administration for the adoption of artificial intelligence technologies. However, this document primarily focuses on the social and economic impacts of AI systems as well as the necessary policies to address the challenges they raise, rather than outlining any current implementation or use of new technologies by public authorities. Furthermore, information about the type of technologies or software used was not shared by the respective authorities when asked through access to information requests.

The examination of national legislation, case law and the results of access to information requests did not lead to the identification of a particular national law dedicated to regulating Big Data analytics activities or any similar technologies employed by law enforcement agencies. Thus, any

[53] Law on Bulgarian Identity Documents, published in the State Gazette, issue 93 of 11 August 1998, amended and supplemented in the State Gazette, issue 67 of 4 August 2023. (Закон за българските лични документи, обн. ДВ, бр. 93 от 11 август 1998 г., изм. и доп. ДВ, бр. 67 от 4 август 2023 г.)., Article 16 (2)

[54] Instruction No. Iz-417 of 10 March 2010 on the Organisation and Technology of Work in the Structures of the Ministry of the Interior for Issuing Bulgarian Identity Documents, published in the State Gazette, issue 22 of 19 March 2010, amended and supplemented in the State Gazette, issue 78 of 17 September 2021. (Инструкция № Із-417 от 10 март 2010 г. за организацията и технологията на работа в структурите на МВР при издаване на българските лични документи, обн. ДВ, бр. 22 от 19 март 2010 г., изм. и доп. ДВ, бр. 78 от 17 септември 2021 г.)., Article 7

[55] Article 26 ZMRV allows the police to "process all necessary categories of data", see Access to Public Information Request to the MVR Reg. No 812104-301-1/23.07.2024. In addition, Article 24(4) ZMVR states that: "The information repositories created for the administrative servicing of citizens may also be used for the purposes of protecting national security, combating crime, maintaining public order and conducting criminal proceedings." And Article 69(2) of the Law on Bulgarian Identity Documents confirms: "The use of data from the information repositories is permitted, in the manner prescribed by law, where there is a threat to national security, for the detection, prevention or suppression of criminal offences, and in cases involving breaches of public order."

[56] Unsuccessful attempts to access information for academic research purposes due to the classified nature of the information are confirmed by Deyana Marcheva and Silvia Tsoneva: "The Law of the Algorithmic State in Bulgaria" in Mauro Bussani, Angela Ferrari Zumbini and Marta Infantino (eds), The Law of the Algorithmic State in Central and Eastern Europe, vol 17 (2025), p. 528, https://www.ijpl.eu/wp-content/uploads/2025/04/IJPL-2-del-2025-Special-Issue.pdf.

[57] "Ministry of Transport, Information Technology and Communications, Concept for the Development of Artificial Intelligence in Bulgaria until 2030: Artificial Intelligence for Smart Growth and a Prosperous Democratic Society, October 2020", https://www.mtc.government.bg/sites/default/files/conceptforthedevelopmentofaiinbulgariauntil2030.pdf.

possible use of advanced technology tools has to fit within the current legal framework and existing provisions.

Nonetheless, it is worth noting that **the MVR can process personal data through automated means** pursuant to Article 2 of Instruction N°8121z-1280/7.10.2021, which is a general provision for the processing of personal data and not a specific one regulating automated processing. The Instruction also lays out procedures and rules for the restriction of the processing on the basis of administrative or judicial order and individuals' requests, among other bases.[58] It also provides the grounds for deletion (Article 21). The Law on the Ministry of the Interior (ZMVR) mentions **several automated systems**, such as the centralised electronic system and automated technical means for traffic control (Article 98), the Automated Fingerprint Identification System "EURODAC" (Article 50a, item 5), and integrated and automated systems for observation (Article 102, paragraph 1, item 14). The law on the procedure for creating and removing police registration indicates that **the police authorities use the Automated Fingerprint Identification System (AFIS), the Automated Information System (AIS), the Integrated Regional Police System (IRPS)**, and other automated information funds for use by the Ministry of the Interior. **It can therefore be inferred that Bulgarian police authorities employ facial and biometric recognition technologies and other algorithmic automation processes.**

The information collected by the MVR is placed in "information funds" which are managed by a designated person who is responsible for their supervision and their compliance with the ZZLD. More importantly, the Instruction mandates, in Article 52, to conduct an impact assessment which practically mirrors the text in Article 27 LED.

For the purposes of data processing, the MVR uses a "specialised software" whose functionalities are not made public. In an answer to an access to information request, the Ministry's data protection officer stated that there is no information concerning the use of technologies for predictive policing, artificial intelligence or Big Data by the MVR or by the counter-terrorism department.[59]

Although Bulgaria uses "various automated systems such as the AFIS database, a fully automated online search procedure, and automated searching and comparison of DNA profiles",[60] it is, at the time of writing this report, unclear if other types of advanced technologies are currently in use in the country. **It seems that Bulgaria's use of algorithmic/AI-based technologies is mainly linked to the implementation of EU law in the field of home affairs and migration control, and to its participation in police cooperation frameworks, rather than being motivated by its own national projects and initiatives.[61]**

EU financial and political support plays an important part in the development and deployment of new technologies in Bulgaria. The Border Violence Monitoring Network (BVMN) reported that "biometric data collection and database capacities were supported by EU funding. In 2016, ISF funds supported the development of the national AFIS and DNA databases."[62]

An access to public information request was launched to other institutions, which are involved in operations concerning one or more purposes pursued by the LED:

---

[58] Instruction No. 8121z-1280 of 7 October 2021 on the procedure for processing personal data in the Ministry of the Interior, published in the State Gazette, issue 87 of 19 October 2021. (Инструкция № 8121з-1280 от 7 октомври 2021 г. за реда за обработване на лични данни в Министерството на вътрешните работи, обн. ДВ, бр. 87 от 19 октомври 2021 г.).

[59] "Access to Public Information Request to the MVR Reg. No 812104-346-1/15.08.2024".

[60] Marcheva and Tsoneva (n 56)., p. 548

[61] A similar trend can be observed in the field of border control as illustrated by the research carried out by the Border Violence Monitoring Network (BVMN). In its report, the BVMN shows that Bulgarian authorities are partners to several EU-funded research projects involving new technologies such as an AI-powered autonomous border surveillance system, with other EU Member States like Greece. The report also indicates a push from the EU level as "in March 2023, the EU Commission's Directorate General for Home Affairs and Frontex encouraged Bulgarian Authorities to continue to engage in technological pilot projects in order to increase their knowledge of innovative surveillance technologies for future procurements", in Hope Barker and others, "Surveillance Technologies at European Borders Assessment of Bulgaria", p. 40, https://borderviolence.eu/uploads/document/file/443/BULGARIA-Surveillance-tech.pdf.

[62] Ibid., p. 41

- The Head of the "military police" service under the Ministry of Defence[63] replied that the body "does not have public information" concerning the use of tools for predicting policing, artificial intelligence or Big Data, thus neither denying nor confirming their use.[64]
- The military branch of the public prosecution, the Military Appellate Prosecutor's Office (responsible for prosecuting crimes committed by military service members),[65] confirmed the use of new technologies, which was declared in accordance with the law without entering into more detail.[66] The specific data collected, the purposes, techniques and other issues discussed throughout this study were not shared.

The answers to the requests submitted to the IVSS and the KZLD shed no further light on the use of new technologies by Bulgarian law enforcement authorities.

6. Conclusion

Eight years after the adoption of the Law Enforcement Directive 2016/680, and six years after its entry into force, important issues persist as indicated in the European Commission's documents and independent studies.[67]

This study revealed deficiencies in the transposition and application of the LED in Bulgaria. These are primarily linked to the unclear wording of the transposed text, the broad discretionary margins left to law enforcement authorities, the lack of clear purpose, identification and definition for data processing, and the disproportionate time limit for data retention, among other issues identified throughout the report.

The main findings of this study are briefly summarised here:

- The current single national data protection law is inadequate, since there is no clear distinction between provisions that apply to the GDPR and provisions that transpose the LED.
- The expected improvement of compliance, relief of administrative burden and simplification of the exercise of citizens' rights cannot be considered to be achieved. The Bulgarian legislator maintained the same legal approach (only one general law and bylaws), creating confusion as to the applicability of certain provisions to law enforcement data processing operations. This evidences a lack of intention to change from the previous regime to the one established with LED, which introduces specific protections and rules for law enforcement processing.
- The LED provisions lack development in national legislation due to the close mirroring of the Directive's provisions or their literal transposition.
- The national legislation is prone to arbitrariness and broad interpretation. Terms such as "national security" or "public order and security" lack legal definition in the national legal order and are thus unclear, especially when applied to restrict data subjects' rights (Art. 13 LED/ Art.54 ZZLD).
- The European Commission's recommendation, transmitted in 2019 to the national Commission for the Protection of Personal Data, that Bulgarian law enforcement authorities should lay out specific conditions and procedures for the application of restrictions to data subjects' rights, is still not implemented by the latter.

[63] Their activities fall under the scope of the LED: https://vp.mod.bg/bg/zanas/functions_and_tasks.html
[64] "Access to Public Information Request to the Ministry of Defence, Decision of the Head of Military Police Service, No ZVP-781/31.07.2024".
[65] Their activities fall under the scope of the LED: https://prb.bg/voapsofia/bg/informaciya-za-grazhdani/vprosi-i-otgovori
[66] "Access to Public Information Request to the Public Prosecution Office, Military Appellate Prosecutor's Office Answer, No 491/2024/02.08.2024".
[67] "Communication from the Commission to the European Parliament and the Council, First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ("LED") COM/2022/364 Final, 25.07.22" (n 27); Plixavra Vogiatzoglou and Thomas Marquenie, "Assessment of the Implementation of the Law Enforcement Directive" (2022) PE 740.209; TIPIK, "Report on the Transposition of Directive (EU) 2016/680" (2020) Ares(2022)7703517.

- The lack of proportionality assessment and conceivable time limits for the retention of personal data by law enforcement agencies is a persistent issue despite the rulings of the CJEU and the ensuing decisions of the national court.
- The purposes for the collection of personal data by national law enforcement authorities are too broad and not sufficiently clear, which practically leads to the processing of an unlimited set of categories of data.
- Data collection and retention happen virtually in a systematic, generalised and indefinite manner by national law enforcement agencies, including sensitive data, due to conflicting legislative obligations such as compulsory police registration, including biometric and genetic data, for the majority of the crimes subject to public prosecution.
- There is no information concerning the use of technologies for predictive policing, artificial intelligence or Big Data by the police. For the purposes of processing personal data, the police uses a "specialised software". The specific functionalities of the technologies used for the processing of personal data remain unknown, however Bulgaria uses automated means of processing such as AFIS and AIS. The compliance with the LED could not be assessed.
- **From all of the above, it ensues that law enforcement authorities in Bulgaria have a broad operational margin when collecting personal data in the exercise of their tasks, as they are largely provided with a legal basis for the indiscriminate collection, processing and storage of personal data for unclear purposes.**

7. Recommendations

The identification of deficiencies has led to the following set of recommendations:

- Reconsider the architecture of the national legislation in the area of law enforcement data protection towards a regime that adequately reflects the specificities of data processed in the area of law enforcement;
- Introduce the missing terminology and clarify existing ones, for example, "national security" and "public order";
- Adopt the recommendations made by the European Commission and the KZLD in the respective areas of application;
- Set out clear criteria for the restriction of access to personal data and data processing information;
- Introduce a clear and sound proportionality assessment mechanism and conceivable time limits for the storage of personal data by law enforcement authorities;
- Provide for an adequate protection of sensitive data;
- Adapt the police registration procedure so that it follows the principles established in EU data protection law;
- Introduce specific laws regulating personal data processing operations for law enforcement purposes by means of new technologies.

The author of this study is confident that, adopted properly, these recommendations would contribute to enhancing the level of data protection for individuals in Bulgaria and would further enhance the exercise of their fundamental rights, as well as law enforcement authorities' compliance with EU standards.

8 Annex: other relevant national legislation

Besides the ZZLD, another important document in connection with the analysis of this study is the Regulation on the Organisation of the Inspectorate to the Supreme Judicial Council (ROIVSS),[68]

[68] Regulations on the Organisation of the Activities of the Inspectorate to the Supreme Judicial Council and on the Activities of the Administration and Experts, published in the State Gazette, issue 103 of 27 December

which lays out the organisation and procedures that the Inspectorate to the Supreme Judicial Council (IVSS) follows in the exercise of its supervisory powers within the judiciary in the cases established under Art. 17 ZZLD.

Another relevant piece of legislation is the Law on the Ministry of the Interior (ZMVR). ZMVR regulates the principles, functions, activities, management and structure of the Ministry of the Interior. Along with its tasks, it contains relevant data protection provisions concerning the collection and processing of personal data by the police (Art. 25-29, Art. 68). Also, Instruction № 8121z-1280/7.10.2021 of the MVR describes the procedure for the processing of personal data in and by the Ministry, while Instruction № 8121z-748/20.10.2014 defines the storage limit. In addition, the Bulgarian personal documents law regulates the terms and conditions for the issuance, use and storage of Bulgarian personal documents. It is relevant because it describes what data national identification documents contain. Furthermore, the Ministry of the Interior issued an Ordinance for the Procedure for Conducting and Removing Police Registration (NRISPR), which establishes the procedure and the data to be collected for the creation of a police record.

The list of relevant legislation reviewed for the purpose of this study includes the Criminal Code, the Criminal Procedure Code, Law on the Judiciary, the Law on the State Agency "National Security" and Instruction No. Iz-417 on the Organisation and Technology of Work in the Structures of the Ministry of the Interior for Issuing Bulgarian Identity Documents.

9. Glossary

Acronym	Full Name
KZLD	Commission for Personal Data Protection (Комисия за защита на личните данни)
IVSS	Inspectorate to the Supreme Judicial Council (Инспекторат към Висшия съдебен съвет)
MVR	Ministry of the Interior (Министерство на вътрешните работи)
ZMVR	Law on the Ministry of the Interior (Закон за Министерството на вътрешните работи)
ZZLD	Personal Data Protection Act (Закон за защита на личните данни)
ROIVSS	Regulations on the Organisation of the Activities of the Inspectorate to the Supreme Judicial Council and on the Activities of the Administration and Experts (Правилник за организацията на дейността на Инспектората към Висшия съдебен съвет и за дейността на администрацията и на експертите)
NRISPR	Ordinance for the Procedure for Conducting and Removing Police Registration (Наредба за реда за извършване и снемане на полицейска регистрация)
LED	Law Enforcement Directive (Directive (EU) 2016/680)
GDPR	General Data Protection Regulation 2016/679
CJEU	Court of Justice of the European Union

10. Bibliography

EU Legislation

1. 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

2016, supplemented in issue 96 of 2 December 2022. (Правилник за организацията на дейността на Инспектората към Висшия съдебен съвет и за дейността на администрацията и на експертите, обн. ДВ, бр. 103 от 27 декември 2016 г., доп. бр. 96 от 2 декември 2022 г.) (ROIVSS).

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 2016 (OJ L 119/89) 89

2. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008 (OJ L 350) 60

CJEU Case Law

1. *Judgement of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, Case C-205/21, EU:C:2023:49* (Court of Justice of the European Union)
2. *Judgement of 30 January 2024, Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR - Sofia, Case C-118/22, EU:C:2024:97* (Court of Justice of the European Union)
3. *Judgment of 28 November 2024, VS v Ministerstvo na vatreshnite raboti, C-80/23, ECLI:EU:C:2024:991* (Court of Justice of the European Union)
4. *Opinion of Advocate General Pitruzzella delivered on 30 June 2022, VS v Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2022:507*
5. *Request for a preliminary ruling of 14 February 2023, VS v Ministerstvo na vatreshnite raboti, C-80/23* (Court of Justice of the European Union)

National Legislation

1. Criminal Code, published in the State Gazette, issue 26 of 2 April 1968, amended in the State Gazette, issue 42 of 14 May 2024. (Наказателен кодекс, обн. ДВ, бр. 26 от 2 април 1968 г., изм. ДВ, бр. 42 от 14 май 2024 г.)
2. Law on Bulgarian Identity Documents, published in the State Gazette, issue 93 of 11 August 1998, amended and supplemented in the State Gazette, issue 67 of 4 August 2023. (Закон за българските лични документи, обн. ДВ, бр. 93 от 11 август 1998 г., изм. и доп. ДВ, бр. 67 от 4 август 2023 г.)
3. Law on Combating Antisocial Behavior of Minors and Juveniles, published in the State Gazette, issue 13 of 14 February 1958, amended in the State Gazette, issue 101 of 27 December 2019. (Закон за борба срещу противообществените прояви на малолетните и непълнолетните, обн. ДВ, бр. 13 от 14 февруари 1958 г., изм. ДВ, бр. 101 от 27 декември 2019 г.)
4. Law on the Ministry of the Interior, published in the State Gazette, issue 53 of 27 June 2014, amended and supplemented in the State Gazette, issue 19 of 5 March 2024. (Закон за Министерството на вътрешните работи, обн. ДВ, бр. 53 от 27 юни 2014 г., изм. и доп. ДВ, бр. 19 от 5 март 2024 г.) (ZMVR)
5. Personal Data Protection Act, published in the State Gazette, issue 1 of 4 January 2002, amended and supplemented in the State Gazette, issue 17 of 26 February 2019. (Закон за защита на личните данни, обн. ДВ, бр. 1 от 4 януари 2002 г., изм. и доп. ДВ, бр. 17 от 26 февруари 2019 г.) (ZZLD)
6. Instruction No. 8121з-1280 of 7 October 2021 on the procedure for processing personal data in the Ministry of the Interior, published in the State Gazette, issue 87 of 19 October 2021. (Инструкция № 8121з-1280 от 7 октомври 2021 г. за реда за обработване на лични данни в Министерството на вътрешните работи, обн. ДВ, бр. 87 от 19 октомври 2021 г.)
7. Instruction No. Iз-417 of 10 March 2010 on the Organization and Technology of Work in the Structures of the Ministry of the Interior for Issuing Bulgarian Identity Documents, published in the State Gazette, issue 22 of 19 March 2010, amended and supplemented in the State Gazette, issue 78 of 17 September 2021. (Инструкция № Із-417 от 10 март 2010 г.

за организацията и технологията на работа в структурите на МВР при издаване на българските лични документи, обн. ДВ, бр. 22 от 19 март 2010 г., изм. и доп. ДВ, бр. 78 от 17 септември 2021 г.)

8. Ordinance for the Procedure for Conducting and Removing Police Registration, published in State Gazette, issue 90 of 31 October 2014, amended in State Gazette, issue 57 of 28 July 2015. (Наредба за реда за извършване и снемане на полицейска регистрация, обн. ДВ, бр. 90 от 31 октомври 2014 г., изм. ДВ, бр. 57 от 28 юли 2015 г.) (NRISPR)
9. Regulations on the Organisation of the Activities of the Inspectorate to the Supreme Judicial Council and on the Activities of the Administration and Experts, published in the State Gazette, issue 103 of 27 December 2016, supplemented in issue 96 of 2 December 2022. (Правилник за организацията на дейността на Инспектората към Висшия съдебен съвет и за дейността на администрацията и на експертите, обн. ДВ, бр. 103 от 27 декември 2016 г., доп. бр. 96 от 2 декември 2022 г.) (ROIVSS)

National Case Law

1. *Decision No 7 of 4 June 1996 on Constitutional Case No 1/96, Constitutional Court (Решение № 7 от 4 юни 1996 г по кд № 1/96 г, Конституционен съд)*
2. *Decision No 6758 of 4 June 2024 of the Supreme Administrative Court (VAS) on Administrative Case No 6492/2021 (Решение № 6758 от 4 юни 2024 г на ВАС по административно дело № 6492/2021)*
3. *Decision No 10522 of 2 November 2023 of the Supreme Administrative Court (VAS) on Administrative Case No 140/2023 (Решение № 10522 от 2 ноември 2023 г на ВАС по административно дело № 140/2023)*

Academic Sources

1. Barker H and others, "Surveillance Technologies at European Borders Assessment of Bulgaria", https://borderviolence.eu/uploads/document/file/443/BULGARIA-Surveillance-tech.pdf
2. Brewczyńska M, "A Critical Reflection on the Material Scope of the Application of the Law Enforcement Directive and Its Boundaries with the General Data Protection Regulation" in Eleni Kosta, Ronald Leenes and Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022), https://www.elgaronline.com/view/edcoll/9781800371675/9781800371675.00013.xml
3. González Fuster G, "Article 13: Information to Be Made Available or given to the Data Subject" in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024), https://doi.org/10.1093/law/9780192855220.003.0013
4. Marcheva D and Tsoneva S, "The Law of the Algorithmic State in Bulgaria" in Mauro Bussani, Angela Ferrari Zumbini and Marta Infantino (eds), *The Law of the Algorithmic State in Central and Eastern Europe*, vol 17 (2025), https://www.ijpl.eu/wp-content/uploads/2025/04/IJPL-2-del-2025-Special-Issue.pdf
5. TIPIK, "Report on the Transposition of Directive (EU) 2016/680" (2020) Ares(2022)7703517
6. Vogiatzoglou P and Marquenie T, "Assessment of the Implementation of the Law Enforcement Directive" (2022) PE 740.209

Other Documents

1. "Access to Public Information Request to the Ministry of Defence, Decision of the Head of Military Police Service, No ZVP-781/31.07.2024"
2. "Access to Public Information Request to the MVR Reg. No 812100-14113-1/29.07.2024"
3. "Access to Public Information Request to the MVR Reg. No 812104-301-1/23.07.2024"
4. "Access to Public Information Request to the MVR Reg. No 812104-346-1/15.08.2024"
5. "Access to Public Information Request to the Public Prosecution Office, Military Appellate Prosecutor's Office Answer, No 491/2024/02.08.2024"
6. "Annual Report of the Commission for Personal Data Protection on Its Activities in 2019. (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2019 г.) Https://Cpdp.Bg/En/Annual-Reports/"
7. "Annual Report of the Commission for Personal Data Protection on Its Activities in 2023. (Годишен Отчет На Комисията За Защита На Личните Данни За Дейността ѝ През 2023 г.) Https://Cpdp.Bg/En/Annual-Reports/"
8. "Commission for Personal Data Protection (Комисия За Защита На Личните Данни) (KZLD)", https://cpdp.bg/
9. "Communication from the Commission to the European Parliament and the Council, First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ("LED") COM/2022/364 Final, 25.07.22"
10. "Council of Ministers, Website for Public Consultations of Proposed Legislative Acts", https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=3467
11. "Inspectorate to the Supreme Judicial Council (Инспекторат Към Висшия Съдебен Съвет) (IVSS)", https://www.inspectoratvss.bg/
12. "Ministry of Transport, Information Technology and Communications, Concept for the Development of Artificial Intelligence in Bulgaria until 2030: Artificial Intelligence for Smart Growth and a Prosperous Democratic Society, October 2020", https://www.mtc.government.bg/sites/default/files/conceptforthedevelopmentofaiinbulgariauntil2030.pdf

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights