European Journal of Risk Regulation (2024), **15**, 1069–1076
doi:10.1017/err.2024.62

CAMBRIDGE UNIVERSITY PRESS

CASE NOTES

Case C-80/23: A Quest for Clarity. The Law Enforcement Directive 2016/680, a Bulgarian Court and Case C-205/21

Liubomir Nikiforov

VUB, Brussel, Belgium
Email: Lyubomir.Nikiforov@vub.be

Abstract

This contribution examines the legal intricacies surrounding law enforcement data collection practices in Bulgaria within the framework of the Law Enforcement Directive 2016/680 (LED) and relevant Court of Justice of the European Union (CJEU) rulings, particularly cases C-205/21 and C-80/23. The analysis underscores challenges in interpreting the concept of "strict necessity" and ensuring compliance with its provisions, in particular, Art. 10. Key findings reveal ambiguities in the LED's application, particularly concerning judicial review and the scope of data collection. The subsequent Case C-80/23 further seeks clarification on the strict necessity standard and the scope of judicial review in the collection of biometric and genetic data. The outcome of both cases has broader implications for EU member states, highlighting the need for legislative alignment and underscoring the complexities and challenges in balancing effective law enforcement with the protection of fundamental rights.

I. The issues raised by the Bulgarian court in light of Article 10 LED

A long-expected decision on the reference for a preliminary ruling Case C-205/21 was made public on 26 January 2023.[1] The case is relevant for the application of the Law Enforcement Directive 2016/680 (LED)[2] by national authorities, in particular, when it comes to the collection of special categories of data pursuant to Article 10 LED. After, briefly introducing Article 10 LED, I summarise the facts and the issues raised by the referring court in order to provide a commentary on the matters at stake.

The LED foresees the processing of sensitive personal data in Art. 10, where those special categories of data are exhaustively listed[3], and where their processing is "... allowed only where strictly necessary, subject to appropriate safeguards for the rights and

This article is an expanded and developed version of a preprint, which can be found at Liubomir Nikiforov, "Case C-80/23: A Quest for Clarity. The Law Enforcement Directive 2016/680, A Bulgarian Court and Case C-205/21" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4859884>.

The current version includes significant new analysis and additional sections not present in the pre-print.

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

[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 2016 (OJ L 119/89) 89.

[3] Art 10, LED, "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the

freedoms of the data subject . . . " For the sake of this contribution, it is important to highlight that biometric and genetic data are defined in Article 3 (12) and (13) contrary to the other "special categories." Catherine Jasserand explains this as an apparent distinction between sensitive data "by their nature," and "biometric data that becomes sensitive when processed to 'uniquely identify' an individual."[4] According to the author, this means that biometric data per se is not protected unless it is employed in processed with the abovementioned purpose, a conclusion that seems to find confirmation in Recital 51 GDPR, where photographs are not considered biometric data, unless used for biometric recognition purposes. The LED does not provide a similar provision.[5]

Most importantly, however, Article 10 LED sets forth the conditions for lawful processing of sensitive data. First, there are three legal grounds therefor, namely when provided in Union or national law (Article 10 (a)), when vital interest are at stake (Article 10 (b)) and finally when they are manifestly made public by the data subject (Article 10 (c)). Second, the processing of such data should be "strictly necessary," although the meaning of this phrase is not further developed the text of the Directive. Third, this processing should be subjected to "appropriate safeguards." Recital 37 LED suggests that those measures may include, among others, adequate security measures, strict access rules or a prohibition to transfer the data. Catherine Jasserand recalls that in an "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) – wp258," the WP29 also included "the prior authorisation of a court or an independent body."

After this brief introduction of the Article 10, which plays a prominent role for the matters examined, in the following lines I provide a summary of the facts and issues of C-205/21.

1. Case C-205/21

The Bulgarian authorities accused a data subject of participation in a criminal organisation with the aim of enrichment within the proceedings against two companies for tax fraud. The accused was requested to cooperate in the creation of a police record. The person completed a declaration form, acknowledging that she had been informed of the statutory basis for creating the police record. Nevertheless, she refused to consent to the collection of her fingerprints and photographic data as well as to the taking of her DNA profile. The police did not collect the data and brought the matter to the referring court in order to request the authorisation of the enforcement of collection of the data.

Confronted with the request the Bulgarian court requested a preliminary ruling to the Court of Justice of the European Union (CJEU) concerning the compatibility of the applicable national law in matters of police record creation and the EU law. In particular, the referring court had doubts concerning the interpretation and application of the national provisions transposing Article 10 LED, which allows special categories of data processing, and its connection with the GDPR (Article 9) where this is prohibited. In addition, the national court had concerns related to the appropriate evaluation of the necessity and proportionality of the biometric and genetic data collection for the purpose of police record creation, especially where those are collected forcibly. Therefore, the decision of provided by the CJEU is highly relevant not only in light of the interpretation of LED but also for Bulgarian authorities as the creation of a police record applies compulsory

purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation . . . "

[4] Catherine Jasserand, "Article 10: Processing of Special Categories of Personal Data," *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) <https://opil.ouplaw.com/display/10.1093/law/9780192855220.001.0001/law-9780192855220#>.

[5] Ibid.

to all persons accused of intentional offences subject to public prosecution and includes the collection of personal data, among which, photographs, fingerprints and DNA samples.

In C-205/21, the CJEU ruled that if the national legislation has legal provisions, which allow "in a sufficiently clear, precise and unequivocal manner" from the interpretation thereof to conclude that the processing of biometric and genetic data at issue falls within the scope of the LED, and not of the GDPR, there is no need to expressly include provisions on special categories of data for the purposes of law enforcement.

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

Finally, the national law enforcement authorities should not carry out a systematic collection of biometric and genetic data unless two conditions are met. Those are that the collection of special categories of data is "strictly necessary" for the specific objectives pursued by the public prosecution and that there are no other means, less intrusive, to achieve the same goal.

2. *Case C-80/23*

Less than a month after the publication of the ruling on C-205/21, on 14 February 2023, a new request for a preliminary ruling, Case C-80/23, was filed by the same judge from Sofia city court.[6] Both cases are virtually the same as they relate to the same criminal proceedings. In both instances, the national court addresses the CJEU with questions related to the interpretation of the Law Enforcement Directive 2016/680 provisions concerning biometric and genetic data collection for the purposes of police record creation.

In essence, what the Bulgarian court inquiries in C-80/23 is, from one side, a clarification of the decision C-205/21 concerning the requirement for "strict necessity" under Article 10 LED, and from the other, a clarification of paragraphs 100-101 and 132-133 of the ruling C-205/21, which concern the potential judicial review of sensitive data collection from an accused within the investigation stage of a crime.

First, the Bulgarian court considers that there is an ambiguity between the abovementioned paragraphs. On the one hand, in paras. 100–101, the CJEU appears to allow the collection of biometric and genetic data without court review when otherwise such review may turn out to be a hindrance for the conduct of the criminal investigation as long as the national law guarantees effective judicial review afterwards. On the other hand, the CJEU seems to require that the national court carry out a judicial review on the necessity to collect sensitive data from the accused in paras. 132–33. In addition, the national court points out that the CJEU based its rationale on case law that is foreign to Bulgarian law. The national court cannot make this judicial review of the necessity to collect the referred data because they do not have access to the file of the accused at the investigative stage of a potential crime. Therefore, the Bulgarian court cannot conduct the expected checks for the necessity of the data collection. Based on that, in a new reference for a preliminary ruling C-80/23, the Bulgarian court poses the following questions:

1. Is the assessment of "strict necessity" satisfied if it is carried out solely on the basis of the documentation accusing the person and the refusal to have his/her data collected or it is necessary for the court to have all the material in the person's file?

[6] *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).

2. In case the latter is confirmed to be the correct interpretation, can the court also assess if there are reasonable grounds to suspect that the accused committed the crime in reality?

In order to provide an interpretation to the posed questions, recent case law, together with relevant national provisions, need to be explored.

II. The C-205/21 and Bulgarian law

In Case C-205/21, the concept of "strict necessity" is examined with regards to processing sensitive data, in particular, during a police record creation. The interpretation of this requirement involves imposing stringent conditions on the processing of such data. According to the Advocate General Pitruzzella's opinion only cases involving serious crimes allow the collection and subsequent processing of "special categories" of data.[7] This suggests that conventional data processing methods may not suffice in addressing challenges stemming from certain crimes, which makes it necessary to collect sensitive data to achieve law enforcement objectives effectively. The final judgement however, lowers this bar and employs a rather ambiguous wording. According to the ruling special categories of data processing only requires "a certain degree of seriousness."[8]

While this is the first condition (degree of seriousness of the crime) that may lift the ban on sensitive data collection, there is one additional prerequisite.[9] According to Advocate General Pitruzzella for the processing to be justified, the specific objective of the processing should be clearly outlined in national legislation.[10] Again, the final judgment rather softens this conclusion and establishes that "account is to be taken of the specific importance of the objective that such processing is intended to achieve" and "in the light of the specific circumstances in which that processing is carried out."[11] In addition, the Advocate General explicitly ascertains that the legislation concerning police record creation under Bulgarian law does not precise the connection between the breadth of the collection and the objectives pursued (para. 61) and this potentially leads to indiscriminate data collection. The final ruling confirms implicitly this as ascertaining that any systematic gathering of sensitive data is deemed to contravene Art. 10 of the Law Enforcement Directive.[12]

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

[8] *Judgment of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, C-205/21, EU:C:2023:49* (n 1). Para. 127.

[9] Ibid, para 127.

[10] *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 7). Para. 58, " . . . ne sont autorisés qu'en cas de stricte nécessité pour la poursuite d'objectifs liés à la criminalité grave, que le droit national doit clairement identifier . . . " and "À cet égard, le droit national doit se conformer à l'une des finalités poursuivies par la directive 2016/680. Il doit également indiquer quels sont les objectifs concrets poursuivis susceptibles de contribuer à la réalisation de cette finalité. Doivent également être précisées de manière concrète les raisons pour lesquelles, en dépit du fait qu'il s'agisse d'une ingérence grave, le traitement de ces données, et en particulier des données génétiques, apparaît strictement nécessaire à cette fin."

[11] *Judgment of 26 January 2023, VS v Ministerstvo na vatreshnite raboti, C-205/21, EU:C:2023:49* (n 1)., para. 127.

[12] Ibid. Para. 128 " . . . it must be held that national legislation which provides for the systematic collection of the biometric and genetic data of any person accused of an intentional offence subject to public prosecution is, in principle, contrary to the requirement laid down in Article 10 of Directive 2016/680 . . . " and para. 129 "Such legislation is liable to lead, in an indiscriminate and generalised manner, to collection of the biometric and genetic data of most accused persons since the concept of 'intentional criminal offence subject to public prosecution' is particularly general and is liable to apply to a large number of criminal offences, irrespective of their nature and gravity."

Having regard to these requisites, in the next lines, I explore the Bulgarian normative landscape in order to find the corresponding provisions, which may match those conditions.

1. Necessity

As far as the necessity precondition is concerned, several documents could be pointed out. Article 51 of the Bulgarian Data Protection Act (BDPA)[13] mirrors the original provisions of the LED Directive's Art. 10. The expectation that those provisions would be developed in Article 25 of the Ministry of Interior Law[14], turns out not to provide additional clarity on the specific necessity for collecting sensitive data as it simply refers to the BDPA, Article 51, and the GDPR, Article 9.

The Order for the Procedure of Conducting and Removing Police Registration[15] aims to shed more light. According to Article 3(1), police authorities conduct police registration for individuals accused of general premeditated crimes. While this might seem like a restriction on data collection purposes, it actually affirms the broad scope of data collection.

This is because the Bulgarian Criminal Code categorises criminal cases into general and private categories based on the nature of the crime. Crimes not specifically designated as of private nature are considered general. General crimes are those affecting societal interests and thus requiring public prosecution and encompass a large spectrum of offenses such as theft, tax violations or murder. As a result, police registration is required for nearly all criminal offenses. Furthermore, there is no differentiation between categories of crimes or their "degree of seriousness" in light of the application of the LED.

2. Outlined in law

While the general objectives for data processing are outlined in the BDPA, specific personal data collected, and their purposes remain unspecified. Delving into related legislation fails to provide clarity. Sectoral laws are not more illuminating. Conversely, Article 26(3) of the Ministry of Interior Law allows the police authority to process "all necessary categories of data" without specifying purposes. Advocate General Pitruzzella, in his Opinion on C-205/21, arrives at a similar conclusion in para. 61.

Moreover, the police registration process in Bulgaria includes the collection of biometric and genetic data, such as fingerprints and oral DNA profiles.[16] Consequently, some of the data collected during a police registration falls within the realm of special categories of data under the Bulgarian data protection act, which mirrors the GDPR definitions for genetic and biometric data. This entails that the same procedure and data categories are collected each time an individual is accused of an intentional crime of a general nature, irrespective of any prior registrations.

[13] 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. (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).

[14] 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. (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).

[15] 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. (Order 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).

[16] Ibid.

This approach is problematic for the following reasons. First, the majority of crimes under the Bulgarian Criminal Code are of general nature. As highlighted in paragraph 130 of the C-205/21 judgment, the mere accusation of an intentional criminal offense subject to public prosecution does not inherently justify the collection of biometric and genetic data. Second, for the purposes of creating a police record, authorities collect personal data Bulgarian identification documents already contain biometric data, including facial images, fingerprints, and signatures. Given that there is no differentiation in "seriousness" of the crime in light of the LED, this translates into a double collection of sensitive data, which in certain cases may be necessary but for many others not. Hence, law enforcement agencies already possess biometric data, albeit not specifically for law enforcement purposes but for the maintenance of "public order." The analysis of the latter goes beyond the scope of this study, however, it would be challenging to justify the collection of special categories of data under this premise, given the lack of definition and the ambiguity of the term under Bulgarian law.

Therefore, it could not be concluded that the relevant national law meets the requirements stablished in LED and developed in case law.

III. Suggested interpretation of the questions posed in C-80/23

Based on the previous, it is sensical to give the following answers to the questions posed by the Bulgarian court[17]:

1. To the first question, whether the court needs all the information about the accused in order to allow the forced collection of special categories of data, it should be answered in the affirmative.

Paras. 100–101 indeed provide grounds for the national court to approve the collection of sensitive data without a thorough judicial review, however, this is so as long as all the other legal prerequisites are in place such as legislation that correctly transposes the relevant LED provisions. Thus, the answer to the question of the Bulgarian court could be better looked for in the paras. 130–132 of the C-205/21. In addition, Bulgarian authorities already possess the same data, which they request in the police registration procedure. The repeated collection of personal data together with the above analysis on the Bulgarian law suggest that any succinct review of a persons' refusal to be subjected to forced collection of data and subsequent approval of the collection may lead to an undue interference with fundamental rights, guaranteed by Articles 7 and 8 of the EU Charter.

2. To the second question, whether the national court can also assess if there are reasonable grounds to suspect that the accused committed the crime, it should be answered negatively.

As it was stated in judgment C-205/21, para. 134, if the national law fails to ensure a review of the measure involving the collection of biometric and genetic data, it is the referring court to uphold the full effect of Art. 10 LED. The reason for the judicial review is not to provide a judgment on the case but to assess the necessity of an intervention with a person's fundamental rights, aiming to ascertain that persons' role in a crime in order to provide a judgment afterwards. The referred in para. 131 "serious grounds" suggests that the construction of the accusation should count with sufficient valid and incriminating proofs, which lead to incrimination of the person. From the same, it could be concluded that in such a context the collection of special categories of data would be never necessary, as law enforcement authorities would already have sufficient data in order to sustain an accusation. However, there may be cases where the link between the voluntary conscious

[17] This part has been written before the publication of Advocate General's Opinion on C-80/23. Thus, sections 3.1 and 3.2 were added a posteriori as a commentary.

nature of the act and the materialisation of the same in the reality may not be clearly established. Those cases should be clearly defined and in case the reality defies the normative hypothesis, then a judge would need to determine the necessity of the sensitive data collection.

1. The Opinion of AG Richard de la Tour on Case C-80/23

In the following lines, the report published on 13 June 2024 Opinion of Advocate General Richard de la Tour on Case-80/23 is briefly summarised and commented in the light of the previous section.[18]

The Advocate General suggests that the assessment of the police record creation is "strictly necessary" for the purposes aimed with its creation must be carried out by the respective competent authorities for the creation of the record before requesting a court authorisation. Therefore, it is not sufficient that this assessment is done for the first time by the court only when the accused refuses to consent, and only based on one purpose stated in the national law supporting this collection.

On the second question, the Advocate General proposes that the preliminary ruling should establish that the review by the national court of the strict necessity does not require a review of the material grounds for the accusation, that is to say whether it is well-founded. In addition, a full disclosure of the case file is not necessary if the judicial review can be done based on the decision designating the person as accused.

2. Commentary

Reading the Advocate General Richard de la Tour (AG) conclusions an alignment could be established on key points regarding the necessity and scope of judicial review as well as the roles of competent authorities and the court.

On the first question, the AG's opinion and the proposed interpretation assert the necessity of a comprehensive review before the collection of sensitive data. While the proposed interpretation affirms that the court needs all relevant information about the accused to allow the forced collection of special categories of data, the AG state that the assessment must be carried out first by the competent authorities seeking the creation of a record before requesting court authorisation. The AG's emphasis on prior assessment by competent authorities resonates with the concern about succinct reviews potentially interfering with fundamental rights and it is implicitly supported by the Court's requirement for a thorough and prior assessment by the respective authorities.

In addition, both texts underline the potential for undue interference if the judicial review process is inadequate. The proposed interpretation warns that a succinct review could lead to such interference. Similarly, the AG highlights that the assessment of necessity must not be performed solely when the accused refuses to consent.

On the second question, both interpretations agree that the national court's role is not to evaluate the foundation of the accusation but to assess the necessity of data collection. The AG clarifies that the court's review of whether the collection of biometric and genetic data is "strictly necessary" does not require assessing the accusation's validity, aligning with the proposed interpretation's assertion that the national court should not determine if there are reasonable grounds to suspect the accused.

However, a divergence emerges regarding the extent and basis of judicial review. The AG notes that full disclosure of the case file is not required for the court to assess necessity,

[18] Opinion of Advocate General Richard de La Tour Delivered on 13 June 2024, VS v Ministerstvo Na Vatreshnite Raboti, C-80/23, ECLI:EU:C:2024:513. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62023CC0080

provided the review is based effectively on the decision designating the person as an accused. In contrast, the proposed interpretation suggests that existing data should restrict the need for further data collection if sufficient to sustain an accusation.

IV. Conclusion

In Case C-205/21 the Court established that the processing of biometric and genetic data is allowed only if it is strictly necessary for law enforcement objectives and if no less intrusive means are available. The ruling mandates a sufficiently clear, precise, and unequivocal legal framework for such data collection, ensuring effective judicial review post-collection. Bulgarian law, however, appears to fall short of these standards, particularly in the lack of specific legislative provisions detailing the necessity and proportionality of data collection. The subsequent preliminary ruling request in Case C-80/23 seeks to address ambiguities related to judicial review and the necessity assessment. The Advocate General's opinion in C-80/23 aligns with the need for a thorough necessity assessment by competent authorities before court authorisation and stresses that judicial review does not require full case disclosure but should ensure that necessity criteria are rigorously met. The examination of the challenges suggests that while the CJEU's rulings provide a robust framework for protecting fundamental rights in data processing, there remains a need for national laws to precisely reflect these higher requirements to prevent undue interference with individuals' rights.

Cite this article: L Nikiforov (2024). "Case C-80/23: A Quest for Clarity. The Law Enforcement Directive 2016/680, a Bulgarian Court and Case C-205/21". *European Journal of Risk Regulation* **15**, 1069–1076. https://doi.org/10.1017/err.2024.62