



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

2 March 2022

Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation (“Prüm II”)

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation (EU) 2018/1725 ‘With respect to the processing of personal data... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies’, and under Article 52(3) ‘...for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data’.

Wojciech Rafał Wiewiorowski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under Article 42(1) of Regulation (EU) 2018/1725, the Commission shall ‘following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals’ rights and freedoms with regard to the processing of personal data’ and under Article 57(1)(g), the EDPS shall ‘advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons’ rights and freedoms with regard to the processing of personal data’.

This Opinion relates to the EDPS' mission to advise the EU institutions on coherently and consistently applying the EU data protection principles. This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725.

Executive Summary

The European Commission adopted on 8 December 2021 a Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council (the so-called ‘Prüm Decisions’). The Proposal is part of a larger legislative package, referred to as ‘EU Police Cooperation Code’, which also includes a Proposal for Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States (subject to a separate EDPS opinion), and Proposal for Council Recommendation on operational police cooperation.

The objective of the Proposal is to enhance law enforcement cooperation and in particular the information exchange between the competent authorities responsible for the prevention, detection and investigation of criminal offences, by laying down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data (fingerprints), facial images, police records and certain vehicle registration data, as well as the exchange of data following a match.

While the EDPS understands the need for the law enforcement authorities to benefit from the best possible legal and technical tools to detect, investigate and prevent crimes, he notes that the proposed new Prüm framework does not clearly lay down essential elements of the exchange of data, such as the types of crimes, which may justify a query, and is not sufficiently clear about the scope of data subjects affected by the automatic exchange of data, e.g. whether the databases, subject to a query, contain data only of suspects and/or convicted persons, or also data of other data subjects, such as victims or witnesses.

The EDPS considers in particular that the automated searching of DNA profiles and facial images should be possible only in the context of individual investigations into serious crimes, instead of any criminal offence, as provided for in the Proposal. Furthermore, the EDPS considers necessary to introduce in the Proposal common requirements and conditions concerning the data in the national databases that are made accessible for automated searches, taking due account of the obligation under Article 6 of the Law Enforcement Directive 680/2016 (LED) to make a distinction between different categories of data subjects (i.e. convicted criminals, suspects, victims, etc.).

The EDPS is also concerned about the implications for the fundamental rights of the concerned individuals by the proposed automated searching and exchange of police records. He considers that the necessity of the proposed automated searching and exchange of police records data is not sufficiently demonstrated. If such a measure is nevertheless adopted, even on voluntary basis, then additional strong safeguards would be required to comply with the principle of proportionality. In particular, given the data quality challenges, the future Regulation should, inter alia, explicitly define the types and/or the seriousness of crimes that may justify an automated query in the national police records.

Regarding the inclusion of Europol within the Prüm framework, the EDPS considers that his comments and recommendations in Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation remain fully valid in the context of Prüm cooperation, in particular those related to the

so-called “big data challenge”, i.e. processing by the Agency of large and complex datasets. The EDPS would like to recall two of the key messages in the Opinion on Europol: with stronger powers should always come a stronger oversight, and, equally important, any applicable exceptions in the form of derogations should not be allowed to become the rule.

The Proposal provides for a complex architecture for the automated searching and exchange of data within the Prüm framework with three separate technical solutions, developed and maintained by three different entities. The EDPS considers that the Proposal should be more explicit regarding the responsibility for the processing of personal data, in particular in EUCARIS, which is not based on EU law and has an intergovernmental nature. In addition, the EDPS is of the opinion that, given the scale and the sensitivity of the personal data processing, the proposed horizontal governance model of the Prüm framework is not suitable and should be further strengthened, e.g. by assigning a central coordination role to an EU entity, e.g. the Commission.

In addition, in the interest of legal certainty, the EDPS considers that the relationship of the data protection rules in the Proposal with the existing legal framework on data protection in the EU, in particular the LED and the Regulation (EU) 1725/2018 (EUDPR), should be explicitly clarified.

The Opinion also analyses and provides recommendations on a number other specific issues, such as the link of the Prüm framework with the interoperability framework, the transfer of data to third countries and international organisations, or the supervision of the processing operations for the purposes of Prüm cooperation.

Table of Contents

1. Introduction	5
2. General Comments.....	6
3. Specific Comments.....	7
3.1. Relationship with the existing legal framework on data protection ..	7
3.2. Scope of the Proposal.....	8
3.3. Automated searching of DNA profiles	9
3.4. Automated searching of facial images	10
3.5. Automated searching and exchange of police records	11
3.6. The role of Europol.....	12
3.7. Transfer of personal data to third countries and international organisations	14
3.8. Technical solutions for exchange of data and governance model.....	14
3.9. Interoperability	15
3.10. Supervision	16
4. Conclusions.....	17

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data¹, and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. On 8 December 2021 the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council (the ‘Proposal’)².
2. The Proposal is part of a larger legislative package, referred to as ‘EU Police Cooperation Code’, which also includes:
 - a Proposal for Directive of the European Parliament and of the Council on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA³, and
 - a Proposal for Council Recommendation on operational police cooperation⁴.
3. The objective of the EU Police Cooperation Code, as stated by the Commission, is to enhance law enforcement cooperation across Member States and in particular the information exchange between the competent authorities⁵. In this regard, the Proposal lays down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data (fingerprints), facial images, police records and certain vehicle registration data and the exchange of data following a match between authorities responsible for the prevention, detection and investigation of criminal offences.
4. The Proposal, as well as the EU Police Cooperation Code more generally, is linked to the policy goals of several EU strategic documents in the area of Justice and Home Affairs, in particular the EU Security Union Strategy⁶, the EU Strategy to tackle Organised Crime 2021-2025⁷ and 2021 Strategy on Schengen area⁸. Moreover, the proposals establishing the Police Cooperation Code should be considered in the light of the ongoing reform of Europol and the growing role of the Agency as a central criminal information hub of the Union, collecting and processing ever-increasing amounts of data⁹.

5. The Commission consulted the EDPS on the Proposal for Regulation Prüm II on 5 January 2022, pursuant to Article 42(1) of Regulation (EU) 2018/1725. The comments and recommendations in this Opinion are limited to the provisions in the Proposal that are most relevant from data protection perspective.

2. General Comments

6. Terrorism and serious crime pose a serious threat within the European Union and globally and their detection, prevention and prosecution undoubtedly represents an important objective of the general interest, which may justify limitations on the exercise of the fundamental rights and freedoms of the individual, in accordance with Article 52(1) of the EU Charter of Fundamental Rights.
7. The EDPS understands the need for the law enforcement authorities to benefit from the best possible legal and technical tools to accomplish their tasks, which are to detect, investigate and prevent crimes and other threats to public security. In this regard, Article 87 TFEU recognises police cooperation, including exchange of relevant information between the law enforcement authorities, as an important instrument for the establishment of an area of freedom, security and justice.
8. The aim of the current Opinion is to provide a fair and objective assessment of the necessity and proportionality of the proposed measures, accompanied by a number of specific recommendations for ensuring the right balance between the values and interests at stake.
9. The EDPS has already commented on the issue of automated data exchange in his 2007 Opinion on the legislative initiative of 15 Member States for adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime¹⁰. Already then the EDPS pointed out the quite unusual legislative procedure followed for the adoption of the Prüm legal framework, which had raised questions about its transparency and democratic legitimacy. The cross border exchange of information, in particular DNA and fingerprints, was first stipulated as an intergovernmental treaty, the Prüm Convention of 2005. Its subsequent integration in the EU legal framework in 2008 as Council Decisions 2008/615/JHA and 2008/616/JHA actually avoided the standard legislative procedures and instead was based on initiatives by certain Member States. Hence, it could be concluded that with Proposal for Regulation Prüm II, this specific form of police cooperation will for the first time be subject to a proper legislative scrutiny.
10. The EDPS notes with regret that 15 years after the first Opinion, his main concerns regarding the necessity and proportionality of the initiative are still valid and are even further exacerbated by the proposed significant extension of the scope of the automated exchange of data. Neither further increase of security threats, nor development of European and international law as well as no new technology implemented since 2007, changed the principal concerns of the EDPS. In particular, the proposed legal framework does not clearly lay down essential elements of the exchange of data, such as the types of crimes, which may justify a query (search), especially of DNA profiles, i.e. any criminal offence or only more serious crimes. In addition, the Proposal is not clear about the scope of data subjects affected by the automatic exchange of data, i.e. whether the databases, subject to a query (search), contain (biometric) data only of suspects and/or convicted persons, or also data of other data subjects, such as victims or witnesses.

11. These two elements play a very substantial role for the assessment of the proportionality of Prüm framework, therefore they are subject to a detailed analysis in following part of this Opinion, together with other aspects of Proposal that are considered relevant from data protection perspective.

3. Specific Comments

3.1. Relationship with the existing legal framework on data protection

12. According to the Explanatory Memorandum, the legal basis for the Proposal are the following provisions of the Treaty on the Functioning of the European Union (TFEU): Article 16(2), Article 87(2)(a) and Article 88(2). Article 87(2)(a) refers to measures on the collection, storage, processing, analysis and exchange of relevant information to ensure police cooperation among Member States' competent authorities in relation to the prevention, detection and investigation of criminal offences. Article 88(2) refers to Europol's structure, operation, field of action and tasks.
13. Under Article 16(2), the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law,
14. In line with the jurisprudence of the CJEU, Article 16 TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature¹¹. At the same time, a comprehensive data protection framework adopted on the basis of Article 16 TFEU already exists, consisting of Regulation (EU) 2016/679 (GDPR), of Regulation (EU) 2018/1725 (EUDPR) and the Law Enforcement Directive (LED)¹². Therefore, in the interest of legal certainty, the relationship of the Proposal with the existing legal framework on data protection in the EU should be explicitly clarified.
15. The EDPS notes that the Explanatory Memorandum to the Proposal states that “[a]s regards Prüm, the applicable data protection legislation is Directive (EU) 2016/680”¹³. Furthermore, according Commission Communication of 24 June 2020 on the way forward on aligning the former third pillar acquis with data protection rules, one of the objectives of the revision of the Prüm Decisions is to ensure “full alignment of the new Prüm Framework with the LED, especially regarding the data protection safeguards”¹⁴.
16. The EDPS notes that Chapter 6 of the Proposal is specifically dedicated to data protection, with legal provisions related to purpose limitation, accuracy, data retention, security, supervision, penalties and others. Most of these provisions correspond to similar legal rules in the LED and, respectively, in Chapter IX of the EUDPR. However, a clarification of the relationship between the data protection rules in the Proposal for Regulation Prüm II, on the one hand, and the horizontal rules of the LED (or the EUDPR with regard to Europol and eu-LISA), on the other hand, is not provided for - neither in the recitals, nor in the operative part of the Regulation. The EDPS stresses that the lack of legal clarity is not an abstract question of legal technique but a substantial issue, which may have direct impact on the practical implementation and enforcement of the data protection rules.

17. Therefore, in the interest of clarity and certainty, **the EDPS recommends specifying in the Proposal that the provisions of Chapter 6 are without prejudice to the application of both the LED and the EUDPR as regards the processing of personal data in the context of law enforcement cooperation under Prüm framework.**

3.2. Scope of the Proposal

18. According to Article 1, the Proposal would establish a framework for the exchange of information between authorities responsible for the prevention, detection and investigation of criminal offences. Pursuant to Article 3 of the Proposal, it would apply to the national databases used for the automated transfer of the categories of DNA profiles, dactyloscopic data, facial images, police records and certain vehicle registration data.
19. In order to assess the necessity and proportionality of the interference with the fundamental right to the protection of personal data, in the light of Article 52(1) of the Charter, it is essential to identify the personal and the material scope of the measures, i.e. the categories of data subjects who will be directly affected, and the objective conditions which may justify an automated query in the respective database of other Member States or of Europol.
20. Article 25, Article 33 and Article 39 of the Proposal refer to categories of data subjects whose personal data may be subject to specific processing operations within the scope of Prüm framework, namely ‘suspects’, ‘criminals’ or ‘perpetrators’. The EDPS notes that the Regulation does not provide definitions of the categories of ‘suspects’, ‘criminal’ and ‘perpetrator’. Moreover, these terms deviate from the data subject categories laid down in the Europol Regulation (‘persons who are suspected of having committed or taken part in a criminal offence, or who have been convicted of such an offence’ and ‘persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences’¹⁵), or in the Law Enforcement Directive (‘persons convicted of a criminal offence’¹⁶).
21. The EDPS underlines the importance of clearly defining the categories of data subjects, in particular, where there is an intention to limit processing to specific data subject categories due to the particularly intrusive nature of the measure, e.g. sharing of DNA profiles or police records. Therefore, **the EDPS considers that the data subject categories should be aligned with the Law Enforcement Directive and the Europol Regulation in order to avoid inconsistencies in application. In this context, references to ‘criminals’ or ‘perpetrators’ should therefore be replaced by ‘persons convicted of a criminal offence’.**
22. Article 33 of the Proposal would require Member States’ competent authorities and Europol to keep a justification of the queries entered under the Prüm framework. The justification should include the purpose of the query, link to the specific case or investigation and indication on whether the query concerns a suspect or a ‘perpetrator’ of a criminal offence (the latter understood as a ‘person convicted of a criminal offence’).
23. However, there is no obligation to provide, as part of the justification, a reference to the specific criminal offence to which the individual is suspected of having committed, or been convicted. As explained later on in the Opinion, in line with the case law of the CJEU, a serious interference with fundamental rights could be justified only if related to a serious crime¹⁷. Therefore, in order to ensure the necessity and proportionality of the processing, and reduce the risks of possible abuse, **the EDPS recommends adding to the justification required under Article 33(2) information about the specific criminal offence.**

3.3. Automated searching of DNA profiles

24. One of the key novelties in the field of police cooperation, introduced with the Prüm framework (the Prüm Convention and the Prüm Decisions), has been the automated searching of DNA profiles. The EDPS already observed in his 2007 Opinion that in fact the Prüm Convention had been set up as a ‘laboratory’ for cross border exchange of information, in particular DNA analysis files, which had enabled the Member States to experiment with such exchange¹⁸.
25. According to Article 4 of the Proposal, ‘DNA profile’ means a letter or number code, which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, the particular molecular structure at the various DNA locations; where ‘non-coding part of DNA’ means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism. Respectively, the DNA profiles exchanged under the Prüm framework represent biometric data. In this regard, the EDPS recalls his consistent position that the collection and storing of biometric personal data, given their very nature and sensitive character, entails higher risks for data subjects and should always be accompanied by stringent safeguards¹⁹.
26. The EDPS is particularly concerned by the fact that the Proposal fails to clearly spell out common conditions and requirements with regard to the justification of an automated searching of DNA profiles. Article 6 of the Proposal defines the scope generally to “investigation of criminal offences” and refers to the compliance with national law. However, assessments by both the Council²⁰ and the European Parliament²¹ have revealed significant discrepancies among Member States regarding the material and personal scope of their national DNA databases. For instance, while the majority of Member States allow access to DNA data of convicted criminals and suspects, there are some countries, which extend the scope also to data of crime victims and relatives of missing persons²².
27. In addition, the case law of the European Court of Human Rights (ECtHR) reveals considerable differences in the national practices concerning the retention periods of the DNA profiles²³. In fact, the legislation of two current EU Member States even provide for indefinite retention of DNA profiles following a conviction for a minor criminal offence²⁴.
28. The Explanatory Memorandum to the Proposal recalls the case law the Court of Justice of the EU (CJEU), according to which the right to the protection of personal data is not an absolute right but must be considered in relation to its function in society²⁵. It also refers to the criteria in Article 52(1) of the EU Charter of Fundamental Rights regarding possible limitations on the exercise of the fundamental rights and freedoms, in particular the requirements of necessity and proportionality²⁶.
29. The EDPS agrees that the investigation of criminal offences represents an important objective of general interest, which may justify such limitations. At the same time, he recalls that the principle of proportionality requires that serious interference with fundamental rights – in this case access to highly sensitive category of biometric data like DNA – can only be justified in situations where the crime is also be considered ‘serious’²⁷.
30. Therefore, the EDPS considers that the envisaged Regulation should introduce common conditions and requirements for automated searching of DNA profiles, which correspond to the sensitive nature of the processed data and level of intrusiveness of this form of police cooperation. **The EDPS considers in particular that the automated searching of DNA**

profiles should only be possible in the context of individual investigations of serious crimes, and not of any criminal offence, as provided for in the Proposal. Furthermore, taking due account of the obligation under Article 6 of the Law Enforcement Directive 680/2016 (LED) to make a distinction between different categories of data subjects (i.e. convicted criminals, suspects, victims, etc.). The Proposal should specify the categories of data subjects whose DNA profiles, stored in the national DNA databases, would be made accessible for automated searches. It is the view of the EDPS that access to data of other categories than convicted criminals or suspects requires a detailed justification, as data from such other categories are usually collected for limited purposes.

3.4. Automated searching of facial images

31. The Proposal aims to extend the scope of automated searches by introducing the exchange of facial images in the Prüm framework²⁸. The definitions in Article 4(10) and 4(11) clarify that “facial image” means digital image of the face and thus biometric data. Hence, the already made observations about the sensitive character of biometric data, the higher risks for data subjects and the need for stringent safeguards fully apply in the case of automated searching of facial images in the context of Prüm.
32. The exchange of facial images in the Prüm framework for police cooperation raises additional challenges, which are specific for this type of biometric data. The EDPS recalls the concerns of the EDPB, expressed in 2020 in a letter to Members of the European Parliament²⁹, about the “*great risk that Member States could disproportionately collect and process vast amount of facial recognition data, as the difference between DNA and fingerprint data on the one hand and facial recognition data on the other is, inter alia, that the latter data can be collected much more easily and also without the knowledge of the data subjects.*” In this regard the EDPB called for a thorough impact assessment, in order to ensure that the necessity and proportionality of such measure, and the essence of the fundamental right to data protection are respected.
33. The above-mentioned study by the EP LIBE committee³⁰ reached similar conclusions about the “*acute fundamental rights implications of searches by facial images*”, recommending, *inter alia*, clarity about the sources of facial images and data protection safeguards ensuring that “the quality of facial images is high enough to prevent the risk of increased false matches, which may lead to discriminatory practices”. In addition, the study urged that “the specific purposes for searching facial images should also be circumscribed so as to prevent wide-ranging surveillance practices at the national level”.
34. The EDPS notes the assurances by the Commission in the Impact Assessment Report accompanying the Proposal³¹, such as that “the exchange of facial images under the Prüm framework does not provide for a remote biometric identification system to be used in publicly accessible spaces”³² and that “there would be no profiling entailed”. However, none of these safeguards is provided for in the Proposal itself, which only refers to the “compliance with the national law of the requesting Member State”.
35. The EDPS also notes that automated searching of facial images is not limited only to serious crimes but could be carried out for the prevention, detection and investigation of any criminal offences, even a petty one. Given the risks for the fundamental rights and freedoms of the affected individuals, already explained above, the EDPS has serious doubts whether this type

of exchange of biometric data in its current form could meet the requirements of necessity and proportionality.

36. Therefore, **the EDPS considers that the Proposal should be further developed for what concerns the safeguards for the fundamental rights of the data subjects in the case of exchange of facial images, by laying down common requirements and conditions concerning the automated searching of facial images stored in national databases. In particular, in line with the obligation under Article 6 LED to make a distinction between different categories of data subjects, only the facial images of convicted criminals and suspects should be made available for queries. In addition, automated searching of facial images must be limited only to individual investigations of serious crimes, and not of any criminal offence, as provided for in the Proposal.**

3.5. Automated searching and exchange of police records

37. The Proposal would bring about another substantial change of the Prüm framework, namely is the possibility for automated searching and exchange of police records³³. While this element does not concern biometric data, such as DNA or facial images, it nevertheless raises serious concerns with regard to the impact on the fundamental rights and freedoms of the affected individuals.
38. In this context, issues of particular importance for the assessment of the necessity and proportionality of the initiative are the definition of what constitutes a police record; the amount of information included in the index; the retention period of a police record; the purposes for which it may be used; and the authorities that could access such it³⁴.
39. The definition in Article 4(16) of the Proposal defines police records as “any information available in the national register or registers recording data of competent authorities, for the prevention, detection and investigation of criminal offences”. The criteria for entering and storing data about an individual in a police record are left entirely to Member States’ and their national rules. The fact that pursuant to Article 25(1) of the Proposal the automated exchange of police records under Prüm would be limited to “biographical data of suspects and criminals from their national police records indexes established for the investigation of criminal offences” does not provide more clarity about the material and personal scope of the proposed personal data processing.
40. The EDPS notes once again that the proposed automated exchange is not related and conditioned to the seriousness of the criminal offence, i.e. it might be justified by both an investigation of a terrorist act and of a (minor) traffic violation, if criminalised under national penal law. Furthermore, the Impact Assessment accompanying the Proposal does not mention any study about the quality of the data in the national police records, in particular to what extent the data are adequate, relevant and not excessive in relation to the purposes for which they are processed.
41. The EDPS recalls that, in accordance with Article 7 LED, the competent law enforcement authorities have to distinguish between personal data based on facts, as far as possible, from personal data based on personal assessments. In the same vein, in all cases of transmission of personal data, the necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date, should be added.

42. Moreover, it should be borne in mind that national police records may contain data that have not been reviewed by a judicial authority, e.g. criminal intelligence about a potential ‘suspect’ in a crime, which may have not been further pursued and formally investigated for various reasons. Thus the proposed exchange of data from police records differs substantially from the existing system for exchange of information about convictions from the national criminal records - the European Criminal Records Information System (ECRIS)³⁵.
43. The risks for the fundamental rights of the affected individuals by the processing of data in the national police records have been examined by the ECtHR, which have found in a number of cases violation of Article 8 ECHR³⁶. Therefore, the EDPS believes that the proposal to expand the Prüm framework with automated searching and exchange of police records should be subject to a more detailed and thorough impact assessment. The fact that the participation in the exchange of police records is voluntary, subject to the decision of each Member State³⁷, is not sufficient to mitigate the risks for the data subjects, and might even be interpreted as an indication of the doubts the Commission itself has about this aspect of the Proposal.
44. The EDPS positively notes the proposed use of pseudonymisation for the purpose of automatic exchange of police records. According to Article 25 (2) of the Proposal, all search data apart from the date of birth and gender would be pseudonymised. While the EDPS welcomes the envisaged practical application of the principles of data protection by design, he nevertheless reminds that pseudonymised data are still personal data and need to comply with the rules on data protection.
45. The EDPS draws the attention on another important aspect, which may have an impact on the right to protection of personal data, namely the quality of matches as a result of automatic searching of police records. Since most of the data would be pseudonymised and there would be obligatory and optional search fields³⁸, the EDPS highlights the need for effective tools and measures to assess and guarantee the quality of matches, thus avoiding, *inter alia*, false hits. In addition, the EDPS invites the Commission to provide more information on the pseudonymisation method(s) (e.g. in the implementing act stipulated in Article 44(7) of the Proposal)³⁹.
46. In view of all these considerations, **the EDPS considers that the necessity of the proposed automated searching and exchange of police records data is not sufficiently demonstrated. In this regard, the Impact Assessment accompanying the Proposal does not provide convincing evidence that this measure will be genuinely effective and the least intrusive for the fundamental rights at stake, including the data protection risks introduced by the proposed new processing activity⁴⁰.**
47. If the co-legislators nevertheless decide that it should become part of the Union law, even on voluntary basis, then **additional strong safeguards are likely to be required to comply with the principle of proportionality⁴¹. While technical measures like pseudonomysation are welcome, they are not sufficient. The future Regulation should at least lay down the types and/or seriousness of crimes that may justify an automated search in the national police records, without prejudice to the need for additional safeguards to address the data quality challenges that would inevitably arise.**

3.6. The role of Europol

48. Chapter 5 of the Proposal provides for the inclusion of Europol within the Prüm framework, enabling Member States to access third country-sourced biometric data stored by Europol

(Article 49) and enabling Europol to check third-country sourced data against the national databases of Member States (Article 50). Furthermore, Europol would be responsible for the development and the technical management of the European Police Records Index System (EPRIS) - the tool for automated searching of police records (Article 64).

49. According to Recital 13 of the Proposal, “[i]n recent years, Europol has received a large amount of biometric data of suspected and convicted terrorists and criminals from several third countries. Including third country-sourced data stored at Europol in the Prüm framework and thus making this data available to law enforcement authorities is necessary for better prevention and investigation of criminal offences”.
50. The EDPS recalls the ongoing legislative process aimed at strengthening and expanding the mandate of Europol, which has entered its final stage⁴². The EDPS provided his comments and recommendations in Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation⁴³, as well as in the subsequent remarks to the co-legislator⁴⁴. **Those recommendations remain fully valid in the context of the envisaged participation of Europol in the Prüm framework, in particular those related to the so-called “big data challenge”, i.e. processing by the Agency of large and complex datasets. The EDPS would like to recall two of the key messages in the Opinion on Europol: That is, on the one hand, that with stronger powers there should always come a stronger oversight, to be provided for by the co-legislators. On the other hand, and equally important, the exceptions and derogations granted to Europol should not be allowed to become the rule.**
51. Furthermore, according to Article 49(1) of the Proposal, Member States will have access to and be able to search biometric data, which has been provided to Europol by third countries for the purposes of Article 18(2), points (a), (b), and (c) of the Europol Regulation. The EDPS notes that almost all personal data provided by third countries to Europol would fall under one of the purposes listed under Article 18(2), points (a), (b) and (c) and therefore this condition serves as no limitation to searches by Member States. Access should, however, be compliant with the conditions under which third countries have shared personal data with Europol (e.g. prior authorisation for onward transmission, where relevant), therefore Article 49 should include a reference to this requirement.
52. In addition, as third countries may share biometric data with Europol on a wider set of data subject categories (contacts, associates, victims), **the EDPS recommends clarifying the personal scope, i.e. specifying the data subject categories subject to queries under Article 49 and Article 50.**
53. The Proposal would lay down provisions for the keeping of logs by Member States and Europol of data processing operations under the Prüm framework (Articles 20, 40, 45) as well as a record of the justifications of the queries that competent authorities and Europol make (Article 33). Logs provide for data protection monitoring, checking the admissibility of a query and the lawfulness of data processing, including by the supervisory authorities and the EDPS in accordance with Article 56, 60 and 61 of the Proposal. The Proposal stipulates that the above-described logs and justifications should be erased one year after their creation. Where those Articles concern Europol, the EDPS notes that this retention period deviates from the three-year retention period accorded to logging and documentation laid down in Article 40 of the Europol Regulation. **The EDPS recommends alignment of the retention periods for logs, in order to ensure consistency with the Europol Regulation and to allow for effective supervision and investigation of data subject complaints.**

3.7. Transfer of personal data to third countries and international organisations

54. According to Article 62 of the Proposal, “[d]ata processed in accordance with this Regulation shall not be transferred or made available to third countries or to international organisations in an automated manner”. Taking into account the comments under 3.1 above about the relationship between the data protection safeguards in the Proposal and the general data protection legal framework of the EU, **the EDPS stresses that any transfer to a third country or an international organisation must be in full compliance with Chapter V of the LED and the relevant provisions of Regulation (EU) 2016/794.**

3.8. Technical solutions for exchange of data and governance model

55. The Proposal envisages a complex architecture for the automated searching and exchange of data within the Prüm framework with three separate technical solutions:

- a central router for exchange of DNA profiles, dactyloscopic data and facial images;
- European Police Records Index System (EPRIS) for exchange of police records; and
- European Vehicle and Driving Licence Information System (EUCARIS) for the exchange of vehicle registration data.

56. Each of the above-mentioned tools would be developed and maintained by a different entity: the router by the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) and the EPRIS by Europol. The EUCARIS is already existing and, unlike the previous two systems, is not based on EU legal act but has an intergovernmental nature - the EUCARIS Treaty⁴⁵.

57. The EDPS notes that the Proposal attempts to address the complexity of the governance model in Chapter 7, dedicated specifically on the responsibilities of the various actors. In addition, according to Article 53, eu-LISA and Europol are declared as processors, respectively for the router and EPRIS. The EDPS considers that the current provisions are not sufficient and should be further developed.

58. The EDPS underlines the need for a clear distinction of data protection roles. While Member States and Europol will retain ‘ownership’²⁴⁶ of the exchanged personal data (as controllers), there could be situations where the Agency and one or more Member States would act as joint controllers. Furthermore, proposed assignment of eu-LISA and Europol as processors creates uncertainty about the responsibilities in case of personal data breach, e.g. which supervisory authority should be informed, but also who should inform the data subjects, if needed. The EDPS reminds that biometric data are of sensitive nature and in case of a personal data breach, it would most probably result in high risk for the data subjects. Notwithstanding any legal basis to delay, restrict or omit notification to the data subjects, e.g. to avoid obstructing investigations, the data breach notifications to the data subjects should be thoroughly assessed, documented and followed upon.

59. The EDPS also notes the provision of Recital 9, last sentence, that there will be no central component needed for the communication via EUCARIS as each Member State will communicate directly to the other connected Member States, as well as Article 19(2), according to which the information exchanged via EUCARIS should be transmitted in encrypted form.

However, **the EDPS considers that the Proposal should explicitly lay down the responsibility for the processing of personal data in EUCARIS.**

60. In addition, **the EDPS is convinced that, given the scale and the sensitivity of the personal data processing, the current horizontal governance model of the Prüm framework is not suitable and should be further strengthened, e.g. by assigning a central coordination role to a EU entity, such as the Commission.**

3.9. Interoperability

61. Another important element of the Proposal which requires careful analysis of its fundamental rights implications, is the alignment of the Prüm framework with the interoperability framework of the EU information systems in the area of justice and home affairs⁴⁷.
62. Interoperability is the ability of the information systems to exchange data and share information. To this end, the interoperability regulations introduced several new components, including Common Identity Repository (CIR) and European Search Portal (ESP). The CIR would store the personal data that are necessary to enable the identification of the individuals whose data are stored in the interoperable systems, including their identity data, travel document data and biometric data, regardless of the system in which the data were originally collected. The ESP would act as a single window or ‘message broker’ to search the various central systems and retrieve the necessary information.
63. The EDPS is convinced that interoperability should be viewed first and foremost as a policy choice, not as a technological solution, due to its far-reaching legal and societal consequences. As we live in a data-driven world, it is not surprising that the Union policy in the area of freedom, security and justice rely more and more on effective and efficient information sharing. However, the EU legal framework must ensure that any limitations to the fundamental rights of all affected individuals apply only in so far as is strictly necessary.
64. Pursuant to Article 39 of the Proposal, the users of the router referred to in Article 35 of the Proposal may launch a query to Member States’ databases and Europol data simultaneously with a query to the Common Identity Repository where the relevant conditions under Union law are fulfilled and in accordance with their access rights. For this purpose, the router shall query the Common Identity Repository via the European Search Portal. The simultaneous queries may only be launched in cases where it is likely that data on a suspect, perpetrator or victim of a terrorist offence or other serious criminal offences are stored in the Common Identity Repository.
65. The EDPS recalls that the Common Identity Repository contains the identity data (alphanumeric information) of the data subjects, logically separated per originating IT system, while biometrics are stored in the shared Biometric Matching Service (sBMS). The latter stores only fingerprints and facial images, not DNA profiles. This fact should be taken into account by eu-LISA when developing the communication infrastructure between the Prüm framework and the interoperability architecture.
66. Furthermore, the EDPS draws the attention to the fact that facial images from the national databases, subject to automated searches in the context of Prüm, may differ from the ones stored in the EU large scale IT systems (e.g. VIS, EES) in terms of format and quality. In this regard, there are questions about the performance of the biometric matching algorithm of sBMS when matching facial images of data of suspects captured under different conditions,

e.g. by a security camera, with facial images taken in controlled environment, e.g. in a booth during visa procedure. Appropriate measures should be **developed and implemented to address the risks stemming from low performance of matching algorithms.**

67. Finally, the EDPS notes that Article 30 of the Proposal, which delegates to the Commission the power to adopt implementing acts in order to specify the technical arrangements, does not include the interoperability element under Article 39. **Therefore, the EDPS invites co-legislator to consider the need for a specific implementing or delegated act on interoperability.**

3.10. Supervision

68. The exchange of data, including biometric data, under the Prüm framework represents serious interference with the right to protection of personal data and obliges strict and effective supervision at national and Union level. **The EDPS therefore welcomes the approach in Article 61 of the Proposal, which refers to the coordinated supervision model between the national supervisory authorities and the EDPS, established with Article 62 of Regulation (EU) 2018/1725.** The latter provides for regular and structured cooperation within the framework of the European Data Protection Board.
69. The EDPS also positively notes the obligation under Article 60(1) of the Proposal for regular audits of the personal data processing operations by eu-LISA and Europol for the purposes of the Regulation Prüm II. At the same time, he considers that **the requirement for regular audits should be extended and should cover also personal data processing operations at national level.** In this regard, in order to guarantee the effectiveness of the supervision, **the EDPS recalls the need for the supervisory authorities to be provided for with sufficient human and technical resources⁴⁸.**
70. The EDPS notes that Article 60(2) of the Proposal refers to some of the supervisory powers of the EDPS vis-a-vis eu-LISA and Europol, namely unrestricted access to documents and premises. However, in the absence of clear provisions on the relationship between this Regulation and the existing data protection legal framework, in particular the EUDPR and the LED, as explained under 3.1 above, there is a risk for restrictive interpretation of the powers of the EDPS. Therefore, **Article 60(2) of the Proposal should be amended to refer to the powers of the EDPS pursuant to Article 58 EUDPR in general, and not only to some of them.**
71. Chapter 9 of the Proposal would lay down provisions for the authorities concerned to obtain reports and statistics in order to assess the efficiency of cooperation under the framework. Statistics should include, in particular, the numbers of queries and the numbers of matches. **The EDPS believes that reporting on the accuracy of hits by the requesting Member State/Europol, would be highly valuable to measure the effectiveness of Prüm, particularly where it concerns matches of biometric data, such as facial images. Therefore, he recommends including explicitly this element in the statistics.**
72. According to Article 55 of the Proposal, eu-LISA and Europol have to notify CERT-EU of any security incidents involving significant cyber threats, vulnerabilities or incidents. In this regard, **the EDPS reminds that this obligation is without prejudice to the obligation of the EU institutions, bodies and agencies to notify personal data breaches to the EDPS, pursuant to Article 92 and 34 of the EUDPR.**

4. Conclusions

73. The proposed new Prüm framework does not clearly lay down essential elements of the exchange of data, such as the types of crimes, which may justify a query (search), especially of DNA profiles, i.e. any criminal offence or only more serious crimes. In addition, the Proposal is not clear about the scope of data subjects affected by the automatic exchange of data, i.e. whether the databases, subject to a query, contain data only of suspects and/or convicted persons, or also data of other data subjects, such as victims or witnesses.
74. In order to ensure the necessity and proportionality of the interference with the fundamental right to the protection of personal data, in the light of Article 52(1) of the Charter, it is essential to clarify the personal and the material scope of the measures, i.e. the categories of data subjects who will be directly affected, and the objective conditions which may justify an automated query in the respective database of other Member States or of Europol.
75. The EDPS considers in particular that the automated searching of DNA profiles and facial images should only be possible in the context of individual investigations of serious crimes, and not of any criminal offence, as provided for in the Proposal. Furthermore, in line with the obligation under Article 6 LED to make a distinction between different categories of data subjects, the Proposal should provide for a limitation of the categories of data subjects whose DNA profiles and facial images, stored in the national databases, should be made accessible for automated searches, considering especially the inherent purpose limitation for data from other categories than convicted criminals or suspects.
76. The EDPS considers that the necessity of the proposed automated searching and exchange of police records data is not sufficiently demonstrated. If such measure is nevertheless adopted, even on voluntary basis, then additional strong safeguards would be required to comply with the principle of proportionality. In particular, given the data quality challenges, which cannot be solved by technical measures like pseudonymisation alone, the future Regulation should as a minimum lay down the types and/or seriousness of crimes that may justify an automated search in the national police records.
77. Regarding the inclusion of Europol within the Prüm framework, the EDPS considers that his comments and recommendations in Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation remain fully valid in the context of Prüm cooperation, in particular those related to the processing of large datasets by the Agency. In addition, the EDPS recommends clarifying the personal scope, i.e. specifying the data subject categories subject to queries under Article 49 and Article 50, as well as alignment of the retention periods for logs, in order to ensure consistency with the Europol Regulation.
78. The Proposal provides a complex architecture for the automated searching and exchange of data within the Prüm framework with three separate technical solutions, developed and maintained by three different entities. Moreover, one of them - EUCARIS - is not based on EU legal act but has an intergovernmental nature. Therefore, the EDPS considers that the Proposal should explicitly address the responsibility for the processing of personal data in EUCARIS. In addition, the EDPS considers that, given the scale and the sensitivity of the personal data processing, the current horizontal governance model of the Prüm framework is not suitable and should be further strengthened, e.g. by assigning a central coordination role to a EU entity, such as the Commission.
79. Another important element of the Proposal, which requires careful analysis of its fundamental rights implications, is the alignment of the Prüm framework with the interoperability

framework of the EU information systems in the area of justice and home affairs. The EDPS invites co-legislator to consider the need for a additional rules in this regard, e.g. in an implementing or delegated act, which should address specific challenges such as the quality and the performance of the matching algorithms for facial images.

80. Taking into account that the legal basis of the Proposal includes, *inter alia*, Article 16 TFEU, in the interest of clarity and certainty, the EDPS recommends specifying in the Proposal that the data protection provisions in Chapter 6 are without prejudice to the application of the LED and the EUDPR, as regards the processing of personal data in the context of law enforcement cooperation under Prüm framework.
81. Furthermore, the EDPS considers that the requirement for regular audits of the personal data processing operations for the purposes of the Regulation Prüm II should be extended and should cover also personal data processing operations at national level. In this context, the EDPS recommends that Article 60 (2) of the Proposal refers generally to the powers of the EDPS, pursuant to Article 58 EUDPR, and not only to some of them.

Brussels, 2 March 2022

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

Notes

¹ OJ L 295, 21.11.2018, p. 39.

² COM(2021) 784 final.

³ COM(2021) 782 final.

⁴ COM(2021) 780 final.

⁵ https://ec.europa.eu/home-affairs/news/boosting-police-cooperation-across-borders-enhanced-security-2021-12-08_en

⁶ Communication from the Commission on the EU Security Union Strategy, COM/2020/605 final.

⁷ Communication from the Commission on the EU Strategy to tackle Organised Crime 2021-2025, COM/2021/170 final

⁸ Communication from the Commission “A strategy towards a fully functioning and resilient Schengen area”, COM/2021/277 final.

⁹ For more information see the EDPS Opinion 4/2021, https://edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf

¹⁰ EDPS Opinion on the legislative initiative of 15 Member States for adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, available at https://edps.europa.eu/sites/default/files/publication/07-04-04_crossborder_cooperation_en.pdf.

¹¹ Opinion of 26 July 2017, PNR Canada, Opinion procedure 1/15, ECLI:EU:C:2017:592, paragraph 96. See also EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, paragraph 11.

¹² 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, OJ L 119, 4.5.2016, p. 89–131.

¹³ Explanatory memorandum, p. 8.

¹⁴ COM(2020) 262 final, p. 8

¹⁵ See Article 18 (1)(a) of Regulation (EU) 2016/794.

¹⁶ See Article 6(b) of Directive (EU) 2016/680.

¹⁷ See CJEU Judgment of 2 October 2018 (Grand Chamber), Ministerio Fiscal (C-207/16, EU:C:2018:788), para. 58.

¹⁸ EDPS Opinion on the legislative initiative of 15 Member States for adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, paragraph 10.

¹⁹ See also EDPS Opinion 07/2016 on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations); Opinion 06/2016 on the Second EU Smart Borders Package Recommendations on the revised Proposal to establish an Entry/Exit System; Opinion 3/2016 on the exchange of information on third country nationals as regards the European Criminal Records Information System (ECRIS).

²⁰ Council Document 5197/1/20 REV 1, available at <https://data.consilium.europa.eu/doc/document/ST-5197-2020-REV-1/en/pdf>

²¹ EP Study “Police Information Exchange - The future developments regarding Prüm and the API Directive”, commissioned by LIBE, available at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658542/IPOL_STU\(2020\)658542_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658542/IPOL_STU(2020)658542_EN.pdf)

²² EP Study “Police Information Exchange - The future developments regarding Prüm and the API Directive”, page 20, p. 2.3.2.

²³ See e.g. ECtHR case Gaughran v. United Kingdom, judgment of 13 February 2020; ECtHR case Aycaguer v France, judgment of 22 June 2017; ECtHR case S. and Marper v. the United Kingdom, judgment of 4 December 2008;

²⁴ See ECtHR judgment in Gaughran v. United Kingdom, para. 53.

²⁵ CJEU judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

²⁶ For more information see EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf

²⁷ CJEU Judgment of 2 October 2018 (Grand Chamber), Ministerio Fiscal (C-207/16, EU:C:2018:788), para. 58.

²⁸ See Chapter II, Section 4 of the Proposal.

²⁹ EDPB letter of 28 July 2020, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0090-prumframework.pdf

³⁰ EP Study “Police Information Exchange - The future developments regarding Prüm and the API Directive”, page 51, 52.

³¹ SWD(2021) 378 final, page 25.

³² See EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), available at https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

³³ See Chapter 2, Section 5 and Chapter 3, Section 2 of the Proposal.

³⁴ See EP Study “Police Information Exchange - The future developments regarding Prüm and the API Directive”, page 52.

³⁵ For more information see https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en#background

³⁶ See ECtHR case *Khelili v. Switzerland*, judgment of 18 October 2011, ECtHR case *Segerstedt-Wiberg and Others v. Sweden*, judgment of 6 June 2006, ECtHR case *Cemalettin Canlı v. Turkey*, judgment of 18 November 2008.

³⁷ See Recital 12 of the Proposal.

³⁸ See Article 43 (1) and (2) of the Proposal.

³⁹ For instance, hash functions could enable irreversible encryption of personal data and at the same time allow for comparisons of two datasets given that both parties (requester and receiver) will use the same algorithm and same key to create the hash values.

⁴⁰ For more information about assessing of necessity of legislative measures see EDPS Necessity Toolkit, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf

⁴¹ See also the EDPS Guidelines on Proportionality, available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en

⁴² For more information see <https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-strengthening-of-europol-s-mandate/01-2022>

⁴³ https://edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf

⁴⁴ https://edps.europa.eu/system/files/2022-02/2022-02-01-remarks_at_the_libe_committee_on_europol_en.pdf

⁴⁵ For more information see <https://www.eucaris.net/general-information/legal-basis/>

⁴⁶ Explanatory Memorandum, p. 6.

⁴⁷ Established with Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA; and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

⁴⁸ See Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, para. 14, available at https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf