Statement

# Statement 03/2022 on the European Police Cooperation Code

## Adopted on 12 September 2022

**The European Data Protection Board has adopted the following statement:**

On 8 December 2021, the European Commission proposed an 'EU Police Cooperation Code', which aims to 'enhance law enforcement cooperation across Member States and in particular the information exchange between competent authorities'. In this Statement, the EDPB recalls the EDPS Opinions[1] regarding the EU Police Cooperation Code and reiterates some of its specific concerns regarding the Proposal for a reformed Prüm Regulation (Prüm II)[2] and the proposal for a Police Information Exchange Directive[3] on the rights of individuals.

**Proposal for a Prüm II Regulation**

The Prüm II Proposal lays down conditions and procedures for the cross-border automated searching of DNA profiles, dactyloscopic data (fingerprints), facial images, police records and certain vehicle registration data, as well as the exchange of this data following a match between the data used for the search or comparison and data held in the database of the requested Member State(s).

*General concerns regarding the expansion of the automated data exchange*

The EDPB acknowledges that police cooperation, including exchange of relevant information between law enforcement authorities, is a key element for the establishment of a well-functioning Area of Freedom, Security and Justice. At the same time, there are high risks associated with the processing of individuals' personal data in criminal matters, especially so where this concerns special categories of personal data such as biometrics. Therefore, the Prüm II Regulation should lay down a number of

[1] EDPS Opinion 4/2022 on the Proposal for a Regulation on automated exchange for police cooperation (Prüm II) and EDPS Opinion 5/2022 on the Proposal for a Directive on information exchange between law enforcement authorities of Member States, published respectively on 2 and 7 March 2022.
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0784
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:782:FIN

essential safeguards to ensure that the processing of personal data remains necessary and proportionate in light of its objectives[4].

First, the future Regulation should at least lay down the types[5] and seriousness of crimes that could justify an automated search in the databases of other Member States, in light of the intrusive nature of the envisaged form of cooperation, e.g. the intensified sharing of DNA profiles[6], the inclusion of facial images, or the proposed automated exchange of police records. Contrary to what is provided for in the Proposal, the EDPB's opinion is that the **automated searching of biometric data or police records** should not be possible in relation to all criminal offences, but only in the context of individual investigations of serious crimes. The EDPB considers that a threshold of severity should be defined that excludes offences that amount only to ordinary crime (having regard to the particular features of the respective criminal justice system e.g. by reference to the applicable minimum penalty or by an individual assessment of the particular features of a given case)[7].

Second, according to Article 6 of the LED, where applicable and as far as possible, a clear distinction must be made between the personal data of different categories of data subjects, such as convicted criminals, suspects, victims or witnesses. The future Regulation should follow this regime and clarify the categories of data subjects affected. It should ensure that requests for searching and sharing individuals' personal data other than convicted criminals or suspects, if permitted in the first place, are always accompanied by a specific and objective justification. The proposal should also make a distinction where information is exchanged in response to an automated query. Therefore, the EDPB is concerned that the necessary safeguards for the processing of the personal data of victims and witnesses are not ensured.

Furthermore, the EDPB considers that further clarification is needed on the relationship between the proposal and the existing data protection framework, including the Law Enforcement Directive (LED), the Europol Regulation and Regulation 2018/1725. This is for example the case where the Proposal

[4] See for example:
- CJEU Judgment of 21 June 2022 (Grand Chamber), Ligue des droits humains ASBL v Conseil des ministres (C-817/19, ECLI:EU:C:2022:491), para. 148 where the CJEU held that "[...] it is important also to bear in mind that, although, in accordance with the principle of proportionality, the objective of combating serious crime is capable of justifying the serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which the PNR Directive entails, the same is not true of the objective of combating criminality in general, since the latter objective may justify solely non-serious interferences (see, by analogy, judgment of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited). Thus, that directive must ensure, by means of clear and precise rules, that the application of the system established by the said directive is limited to offences amounting to serious crime and thereby excludes those amounting to ordinary crime."
- CJEU Judgement of 2 October 2018 (Grand Chamber), Ministerio Fiscal (C-207/16, EU:C:2018:788), para. 56 where the CJEU held that "In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'."

[5] Such as a list pointing out which specific crimes could justify an automated search.

[6] For the processing of DNA profiles and fingerprints, the EDPB refers in particular to sections 3.3 and 3.4 of EDPS Opinion 4/2022 on the Proposal for a Regulation on automated exchange for police cooperation (Prüm II).

[7] See CJEU Judgement C-817/19, para. 148 ff.

refers to the data subject categories of 'perpetrator' and 'criminal', which are terms not aligned with those in the LED and the Europol Regulation.

*Exchange of police records information*

The Proposal also creates serious concerns, where it envisages **automated searching and exchange of police records by introducing the European Police Records Index System** (EPRIS). The current Proposal neither sufficiently substantiates why the envisaged cross-border access to police records is necessary, nor provides sufficient safeguards to be implemented by those Member States that choose to participate in such access[8]. As mentioned previously, the Proposal also lacks a clear definition of the minimum prerequisites that may justify the automated search and exchange of police records.

Furthermore, the EDPB recalls that information in national police records is often neither sufficiently, nor independently verified. This is for example the case for criminal intelligence about a potential 'suspect' for a crime, which has 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 official information about convictions from the national criminal records, the European Criminal Records Information System (ECRIS).

In addition, with regard to the retention of personal data, while there has certainly been a degree of harmonisation of retention periods at national level, time limits for the storage and review of personal data still vary widely between Member States, as noted as well by the Commission in its first report on the application and functioning of the LED[9]. In some Member States, there are as of yet no legally imposed criteria for periodic review and/or legally defined control procedures to enforce time limits for the storage of personal data. This is concerning particularly in light of the statute of limitations applying to the suspected crime for which personal data are being kept and the application of the purpose limitation principle. Where insufficient safeguards are applied in the framework of the automated exchange of police records, the accompanying risks for the data subject would now be propagated to other Member State's police record databases as well.

The EDPB considers that the necessity of the proposed automated searching and exchange of police records data is not sufficiently demonstrated. Furthermore, to assess the proportionality of the horizontal system established by this proposal and as a very first step, a thorough stocktaking of all databases concerned would have been fundamental. However, the impact assessment accompanying the proposal does not mention any study about the quality of the data in the national police records, and to what extent the data are adequate, relevant and not excessive to the purposes for which they are processed. The EDPB would like to recall that the circumstances under which national databases are created and kept (still) differ substantially from Member State to Member State, especially with regard to data sources, categories of personal data (including special categories) and data subjects. In addition, the circumstances of the data collection, purpose(s), the distinction between personal data based on facts from data based on personal assessments, technical and organisational measures and

[8] The EDPB refers also to section 3.5 and in particular paragraph 40 of EDPS Opinion 4/2022 on the Proposal for a Regulation on automated exchange for police cooperation (Prüm II).
[9] Communication from the Commission to the European Parliament and the Council on the first report on the application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM(2022) 364 final, page 13.

retention periods will vary depending on the Member State. It becomes clear that a system relying on such fragmented law enforcement environments will suffer from serious data quality issues.

Should the co-legislators nevertheless decide that EPRIS should become part of the Union law, even on a voluntary basis, then appropriate common safeguards must be introduced to comply with the principle of proportionality. The co-legislators should also reserve the right for and enable Member States to uphold or introduce higher standards of protection of individuals' fundamental rights and freedoms, in particular such as existing safeguards for the processing (especially the collection and the storage) of personal data by law enforcement authorities. In this regard, technical measures like pseudonymisation, while certainly welcomed, cannot be seen as sufficient to mitigate the various risks for individuals.

**Proposal for a Police Information Exchange Directive**

The Proposal for the Information Exchange Directive aims at providing equivalent access for any Member State's law enforcement authorities to information available in other Member States through Single Points of Contacts (SPOCs). The Proposal seeks to establish the trusted Secure Information Exchange Network Application (SIENA), managed by Europol, as the default channel of communication for cross-border law enforcement exchanges (excluding those situations where other channels are required by EU law, e.g. in the context of the Schengen Information System).

The EDPB notes that the mandatory use of SIENA would be coupled with an obligation for Member States to send copies of the following information to Europol if such information concerns offences falling within the scope of the objectives of the Agency in accordance with the Europol Regulation: requests for information; information provided in response to a request; information provided on their own initiative.

The EDPB recalls that law enforcement authorities are under the obligation to determine the exact purpose of processing and to assess whether all the prerequisites for sending information to Europol are met, prior to sharing personal data with the Agency. This is an explicit requirement under Article 19 of the Europol Regulation. The copying in of Europol according to Article 12 of the Proposal, without fulfilling the requirements of the Europol Regulation, opens the door to indiscriminate sending of personal data to Europol that may even fall outside its mandate[10].

In this context, the EDPB strongly disagrees with Recital 18 of the Proposal, which suggests that the obligatory assessment described above could be done through pre-ticked boxes in the SIENA interface.

The EDPB's opinion is that the use of pre-ticked boxes cannot be a valid way of confirming that a national single point of contact or law enforcement authority has conducted the necessary assessment to verify whether the personal data can be shared with Europol. The reason for that opinion is that silence or inactivity on the part of a national single point of contact or law enforcement authority cannot be regarded as an active assessment to share data with Europol.

[10] See also section 3.4 of EDPS Opinion 5/2022 on the Proposal for a Directive on information exchange between law enforcement authorities of Member States.

The EDPB therefore calls on the co-legislators to address the issues identified in this Statement and the relevant EDPS Opinions as regards the Police Cooperation Code and thereby contribute to a strong protection of individuals' fundamental rights and freedoms in the European Union.

For the European Data Protection Board

The Chair

(Andrea Jelinek)