

## **EDPS formal comments on the draft Commission Implementing Decision laying down measures necessary for the technical implementation of the European Criminal Records Information System (ECRIS)**

### **THE EUROPEAN DATA PROTECTION SUPERVISOR,**

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 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 Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')<sup>1</sup>, and in particular Article 42(1) thereof,

**HAS ADOPTED THE FOLLOWING FORMAL COMMENTS:**

#### **1. Introduction and background**

1. On 27 February 2026, the European Commission consulted the EDPS on the draft Commission Implementing Decision laying down measures necessary for the technical implementation of the European Criminal Records Information System (ECRIS) ('the draft Implementing Decision').
2. The objective of the draft Implementing Decision is to lay down the necessary technical specifications for the standardised format referred to in Article 11(3) of Council Framework Decision 2009/315/JHA<sup>2</sup> ('the basic act'), including as regards:
  - information on the offence giving rise to the conviction and information on the content of the conviction;
  - the rules concerning the technical implementation of ECRIS and the exchange of fingerprint data; and
  - any other technical means of organising and facilitating exchanges of information on convictions between central authorities of the Member States<sup>3</sup>.
3. The draft Implementing Decision is issued pursuant to Article 11b(1) of Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.

---

<sup>1</sup> OJ L 295, 21.11.2018, p. 39.

<sup>2</sup> Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, p. 23–32, as amended.

<sup>3</sup> Recital 5 of the draft Implementing Decision.

4. The present formal comments of the EDPS are issued in response to a consultation by the European Commission pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in Recital 18 of the draft Implementing Decision.
5. These formal comments do not preclude any additional comments by the EDPS in the future, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of other related Implementing or Delegated acts<sup>4</sup>. Furthermore, these formal comments are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of the EUDPR and are limited to the provisions of the draft Implementing Decision that are relevant from a data protection perspective.

## **2. Comments**

### **2.1. General comments**

6. The EDPS recalls that the personal data exchanged in the context of the ECRIS are of a particularly sensitive nature, since they concern criminal records (convictions). These data are not public and if revealed to unauthorised persons could result in significant risks to the rights and freedoms of natural persons, including risks of material or non-material damage, discrimination, damage to the reputation, etc. The sensitive nature of these personal data calls for appropriate security measures, including during the transmissions between the central authorities of the Member States.
7. In addition, the exchanged data may contain fingerprint data and/or facial images that constitute biometric data (e.g. a special categories of data) that should be robustly and effectively protected since loss of their confidentiality could result in permanent impact to the affected natural persons.
8. It is the understanding of the EDPS that the implementing act should define the architecture of the system at a functional level, including the core security objectives and mechanisms necessary to ensure the protection of sensitive information exchanged between Member State authorities.
9. In particular, the implementing act should establish requirements ensuring that the system guarantees confidentiality, integrity, availability, authenticity, and traceability of data and communications, in line with a risk-based approach and taking into account the state of the art. In this context, it should describe, in a

---

<sup>4</sup> In case of other Implementing or Delegated acts with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the EDPS would like to remind that he needs to be consulted on those acts as well. The same applies in case of future amendments that would introduce new or modify existing provisions that directly or indirectly concern the processing of personal data.

sufficiently abstract and technology-neutral manner, the categories of security measures to be implemented. These should include, inter alia, secure authentication and authorisation mechanisms, encryption of data in transit and at rest, logging and monitoring capabilities, incident detection and response, and appropriate access control policies.

10. To avoid the disclosure of sensitive technical details that could undermine the system's security, the detailed technical specifications and operational security measures could be defined in separate, non-public documents or governance frameworks, which can be updated as necessary to address evolving threats and technological developments.
11. The EDPS also recalls that Regulation (EU) 2019/816<sup>5</sup> has established a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons ('ECRIS-TCN'). While the technical architecture and the purposes of ECRIS and ECRIS-TCN may differ, due to the same sensitive nature of the personal data processed in those Union systems, i.e. data relating to criminal convictions and offences, and biometric data, the EDPS considers that, as a general rule, the data security standards and measures applicable to them should be aligned to the extent possible. Such alignment seems even more relevant and feasible given that the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is entrusted with the task of developing and maintaining the principal components of both systems<sup>6</sup>.

## 2.2. Specific comments

### 2.2.1. Communication Architecture (Article 4)

12. The EDPS recalls that pursuant to Article 11a(1), second subparagraph of Framework Decision 2009/315/JHA, 'to ensure the confidentiality and integrity of criminal records information transmitted to other Member States, appropriate technical and organisational measures shall be used, taking into account the state of the art, the cost of implementation and the risks posed by the processing of information'. This provision should also be read in the light of the requirements for security of processing of operational personal data laid down in Article 91 EUDPR.
13. To this end, the EDPS considers that the draft Implementing Decision should provide for the use of a secure and closed communication infrastructure at Union level,

---

<sup>5</sup> Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

<sup>6</sup> Recital 4 of the draft Implementing Decision.

ensuring that only duly authorised national authorities can connect to the network, and that communications are protected against unauthorised access, interception and alteration, instead only referring to a common communication infrastructure, as this is crucial element for the confidentiality of the exchanged data<sup>7</sup>.

14. The EDPS also considers that the communication architecture should specify, at a functional level, the standardised format of the information exchanged through ECRIS. Moreover, the EDPS recommends providing greater clarity as regards the different types of calls, including a clear description of their purpose and their correspondence to the relevant provisions governing exchanges under Council Framework Decision 2009/315/JHA. In addition, the implementing act should clarify the circumstances under which synchronous or asynchronous communication modes are to be used.
15. In addition, instead of merely referring to the use of XML Schema Definition (XSD) technology, the EDPS recommends specifying the applicable schema and define the minimum validation requirements to be applied to exchanged data. The schema should also include a clear functional description of each type of request and response, including distinctions between different categories of messages (such as “denial” and “problem” messages), in order to ensure that data processing remains consistent, transparent and traceable.

### **2.2.2. Data Encryption (Article 5)**

16. The EDPS welcomes the requirement in Article 5(1) of the draft Implementing Decision that all ECRIS messages must be encrypted. At the same time, he recommends using two-way server authentication instead of the envisaged one-way authentication, given the sensitive nature of both requests and responses. Furthermore, to keep pace with evolving threats, the Commission and eu-LISA should ensure the continued use of up-to-date encryption standards. This includes defining minimum requirements for secure communication protocols (such as TLS), or, alternatively, establishing clear procedures and responsibilities for determining and updating those requirements on the basis of regular risk assessments.
17. The EDPS also invites the Commission to consider aligning the management of certificates with the principles and requirements of the eIDAS Regulation<sup>8</sup> framework, in particular as regards trust, assurance levels, governance and supervision. This should not preclude the use of certification authorities operated by public authorities, provided that they meet equivalent security, audit and trust requirements. In addition, the security lifecycle should be completed by establishing

---

<sup>7</sup> It is the understanding of the EDPS that ECRIS already uses such system for the exchange of data, namely the Trans European Services for Telematics between Administrations (sTESTA).

<sup>8</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73–114, as amended.

clear protocols for certificate revocation and expiration, in order to mitigate the risk of unauthorised access or data breaches during transmission.

### **2.2.3. Logs (Article 11)**

18. The EDPS welcomes the requirement in Article 11(1) of the draft Implementing Decision that all data processing operations of the ECRIS reference implementation and of the national ECRIS implementation software must be logged.
19. At the same time, the EDPS notes that Article 11(5) of the implementing act leaves to Member States to define the maximum retention period of the logs. The EDPS recommends aligning the retention period of logs in ECRIS with the retention period applicable to ECRIS-TCN pursuant to Article 31(4) Regulation 2019/816 (i.e., a 3 years retention period).

Brussels, 26 March 2026

*(e-signed)*

Wojciech Rafał WIEWIÓROWSKI