Official Journal
of the European Union

EN
L series

2024/982

5.4.2024

# REGULATION (EU) 2024/982 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 13 March 2024

## on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2), Article 87(2), point (a), and Article 88(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) The Union has set itself the objective of offering its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured. That objective is to be achieved by means of, inter alia, appropriate measures to prevent and combat crime and other threats to public security, including organised crime and terrorism, in line with the communication of the Commission of 24 July 2020 on the EU Security Union Strategy. That objective requires law enforcement authorities to exchange data in an efficient and timely manner in order to effectively prevent, detect and investigate criminal offences.

(2) The objective of this Regulation is to improve, streamline and facilitate the exchange of criminal information and vehicle registration data, for the purpose of preventing, detecting and investigating criminal offences, between Member States' competent authorities and between Member States and the European Union Agency for Law Enforcement Cooperation (Europol), established by Regulation (EU) 2016/794 of the European Parliament and of the Council ([3]), in full compliance with fundamental rights and data protection rules.

(3) Council Decisions 2008/615/JHA ([4]) and 2008/616/JHA ([5]), which lay down rules for the exchange of information between authorities responsible for the prevention and investigation of criminal offences by providing for the automated transfer of DNA profiles, dactyloscopic data and certain vehicle registration data, have proven important for tackling terrorism and cross-border crime, thereby protecting the internal security of the Union and its citizens.

(4) Building upon existing procedures for the automated searching of data, this Regulation lays down the conditions and procedures for the automated searching and exchange of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records. That should be without prejudice to the processing of such data

([1]) OJ C 323, 26.8.2022, p. 69.
([2]) Position of the European Parliament of 8 February 2024 (not yet published in the Official Journal) and decision of the Council of 26 February 2024.
([3]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).
([4]) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).
([5]) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

in the Schengen Information System (SIS), the exchange of supplementary information related to such data via the SIRENE bureaux pursuant to Regulation (EU) 2018/1862 of the European Parliament and of the Council ([6]) or the rights of individuals whose data is processed therein.

(5) This Regulation establishes a framework for the exchange of information between authorities responsible for the prevention, detection and investigation of criminal offences (the Prüm II framework). In accordance with Article 87(1) of the Treaty on the Functioning of the European Union (TFEU), it covers all the Member States' competent authorities, including but not limited to police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences. Therefore, in the context of this Regulation, any authority that is responsible for the management of a national database covered by this Regulation or that grants a judicial authorisation to release any data should be considered to be within the scope of this Regulation as long as the information is exchanged for the prevention, detection and investigation of criminal offences.

(6) Any processing or exchange of personal data for the purposes of this Regulation should not result in discrimination against persons on any grounds. It should fully respect human dignity and integrity and other fundamental rights, including the right to respect for one's private life and to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union.

(7) Any processing or exchange of personal data should be subject to the provisions on data protection of Chapter 6 of this Regulation and, as applicable, Directive (EU) 2016/680 of the European Parliament and of the Council ([7]) or Regulation (EU) 2018/1725 ([8]), (EU) 2016/794 or (EU) 2016/679 ([9]) of the European Parliament and of the Council. Directive (EU) 2016/680 applies to the use of the Prüm II framework in respect of searches for missing persons and the identification of unidentified human remains for the prevention, detection and investigation of criminal offences. Regulation (EU) 2016/679 applies to the use of the Prüm II framework in respect of searches for missing persons and the identification of unidentified human remains for other purposes.

(8) By providing for the automated searching of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records, the purpose of this Regulation is also to allow for the search for missing persons and the identification of unidentified human remains. Those automated searches should follow the rules and procedures laid down in this Regulation. Those automated searches are without prejudice to the entry of alerts on missing persons in the SIS and the exchange of supplementary information on such alerts under Regulation (EU) 2018/1862.

(9) Where Member States wish to use the Prüm II framework to search for missing persons and to identify human remains, they should adopt national legislative measures to designate the national authorities competent for that purpose and to lay down the specific procedures, conditions and criteria for that purpose. For searches for missing persons outside the area of criminal investigations, the national legislative measures should clearly set out the

([6]) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

([7]) 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).

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (OJ L 295, 21.11.2018, p. 39).

([9]) Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

humanitarian grounds on which a search for missing persons can be conducted. Such searches should comply with the principle of proportionality. The humanitarian grounds should include natural and man-made disasters and other equally justified grounds, such as suspicions of suicide.

(10) This Regulation lays down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records and the rules regarding the exchange of core data following a confirmed match on biometric data. It does not apply to the exchange of supplementary information beyond what is provided for in this Regulation, which is regulated by Directive (EU) 2023/977 of the European Parliament and of the Council ([10]).

(11) Directive (EU) 2023/977 provides a coherent Union legal framework to ensure that a Member State's competent authorities have equivalent access to information held by other Member States when they need such information to fight crime and terrorism. To enhance the exchange of information, that Directive formalises and clarifies the rules and procedures for sharing information between Member States' competent authorities, in particular for investigative purposes, including the role of each Member State's Single Point of Contact in such exchanges.

(12) The purposes of the exchanges of DNA profiles under this Regulation are without prejudice to the exclusive competence of the Member States to decide the purpose of their national DNA databases, including the prevention or detection of criminal offences.

(13) Member States should, at the time of initial connection to the router established by this Regulation, conduct automated searches of DNA profiles by comparing all the DNA profiles stored in their databases with all the DNA profiles stored in all the other Member States' databases and Europol data. The purpose of that initial automated search is to avoid any gaps in identifying matches between DNA profiles stored in a Member State's database and DNA profiles stored in all the other Member States' databases and Europol data. The initial automated search should be conducted bilaterally and should not necessarily be performed with all other Member States' databases and Europol data at the same time. The arrangements for conducting such searches, including the timing and the quantity by batch, should be agreed bilaterally in accordance with the rules and procedures laid down in this Regulation.

(14) Following the initial automated search of DNA profiles, Member States should conduct automated searches by comparing all the new DNA profiles added to their databases with all the DNA profiles stored in other Member States' databases and Europol data. That automated searching of new DNA profiles should take place regularly. Where such searches could not take place, the Member State concerned should be able to conduct them at a later stage to ensure that matches have not been missed. The arrangements for conducting such later searches, including the timing and the quantity by batch, should be agreed bilaterally in accordance with the rules and procedures laid down in this Regulation.

(15) For the automated searching of vehicle registration data, Member States and Europol should use the European Vehicle and Driving Licence Information System (Eucaris), set up by the Treaty concerning a European Vehicle and Driving Licence Information System (EUCARIS) and designed for that purpose, which connects all participating Member States in a network. No central component is needed to establish communication as each Member State communicates directly with the other connected Member States, and Europol communicates directly with the connected databases.

(16) The identification of a criminal is essential for a successful criminal investigation and prosecution. The automated searching of facial images of persons convicted or suspected of having committed a criminal offence or, where permitted under the national law of the requested Member State, of victims, collected in accordance with national law, could provide additional information for successfully identifying criminals and fighting crime. Given the

([10]) Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA (OJ L 134, 22.5.2023, p. 1).

sensitivity of the data concerned, it should only be possible to conduct automated searches for the purpose of preventing, detecting or investigating a criminal offence punishable by a maximum term of imprisonment of at least one year under the law of the requesting Member State.

(17) The automated searching of biometric data by Member States' competent authorities responsible for the prevention, detection and investigation of criminal offences under this Regulation should only concern data contained in databases established for the prevention, detection and investigation of criminal offences.

(18) Participation in the automated searching and exchange of police records should remain voluntary. Where Member States decide to participate, it should only be possible for them, in the spirit of reciprocity, to query other Member States' databases if they make their own databases available for queries by other Member States. Participating Member States should establish national police record indexes. It should be for the Member States to decide which national databases established for the prevention, detection and investigation of criminal offences to use to create their national police record indexes. Those indexes include data from national databases that the police usually check when receiving requests for information from other law enforcement authorities. This Regulation establishes the European Police Record Index System (EPRIS) in accordance with the privacy-by-design principle. Data protection safeguards include pseudonymisation because indexes and queries do not contain clear personal data, but alphanumerical strings. It is important that EPRIS prevent Member States or Europol from reversing pseudonymisation and revealing the identification data which resulted in the match. Given the sensitivity of the data concerned, exchanges of national police record indexes under this Regulation should only concern the data of persons convicted or suspected of having committed a criminal offence. In addition, it should only be possible to conduct automated searches of national police record indexes for the purpose of preventing, detecting and investigating a criminal offence punishable by a maximum term of imprisonment of at least one year under the law of the requesting Member State.

(19) The exchange of police records under this Regulation is without prejudice to the exchange of criminal records through the existing European Criminal Records Information System (ECRIS), established by Council Framework Decision 2009/315/JHA ([11]).

(20) In recent years, Europol has received a large amount of biometric data of suspects and persons convicted of terrorism and criminal offences from third-country authorities in accordance with Regulation (EU) 2016/794, including battlefield information from war zones. In many cases, it has not been possible to make full use of such data because they are not always available to the Member States' competent authorities. Including data provided by third countries and stored by Europol in the Prüm II framework and thus making those data available to the Member States' competent authorities in line with Europol's role as the Union central criminal information hub is necessary to better prevent, detect and investigate serious criminal offences. It also contributes to building synergies between different law enforcement tools and ensures that data are used in the most efficient manner.

(21) Europol should be able to search Member States' databases under the Prüm II framework with data received from third-country authorities, in full respect of the rules and conditions provided for in Regulation (EU) 2016/794, in order to establish cross-border links between criminal cases in respect of which Europol is competent. Being able to use Prüm data, in addition to other databases available to Europol, would enable a more complete and informed analysis to be carried out, thereby allowing Europol to provide better support to Member States' competent authorities for the prevention, detection and investigation of criminal offences.

([11]) 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).

(22) Europol should ensure that its search requests do not exceed the search capacities for dactyloscopic data and for facial images established by the Member States. In the event of a match between data used for the search and data stored in Member States' databases, it should be up to Member States to decide whether to supply Europol with the information necessary for it to fulfil its tasks.

(23) Regulation (EU) 2016/794 applies in its entirety to the participation of Europol in the Prüm II framework. Any use by Europol of data received from third countries is governed by Article 19 of Regulation (EU) 2016/794. Any use by Europol of data obtained from automated searches under the Prüm II framework should be subject to the consent of the Member State which provided the data and is governed by Article 25 of Regulation (EU) 2016/794 where the data are transferred to third countries.

(24) Decisions 2008/615/JHA and 2008/616/JHA provide for a network of bilateral connections between the national databases of Member States. As a consequence of that technical architecture, each Member State had to establish a connection with each Member State participating in the exchanges, which meant at least 26 connections per Member State, per data category. The router and EPRIS will simplify the technical architecture of the Prüm framework and serve as connecting points between all Member States. The router should require a single connection per Member State in relation to biometric data. EPRIS should require a single connection per participating Member State in relation to police records.

(25) The router should be connected to the European Search Portal, established by Regulations (EU) 2019/817 ([12]) and (EU) 2019/818 ([13]) of the European Parliament and of the Council, to allow Member States' competent authorities and Europol to launch queries to national databases under this Regulation at the same time as queries to the Common Identity Repository, established by those Regulations, for law enforcement purposes in accordance with those Regulations. Those Regulations should therefore be amended accordingly. Moreover, Regulation (EU) 2019/818 should be amended with a view to enabling the storage of reports and statistics of the router in the central repository for reporting and statistics.

(26) It should be possible for a reference number for biometric data to be a provisional reference number or a transaction control number.

(27) Automated fingerprint identification systems and facial image recognition systems use biometric templates comprised of data derived from a feature extraction of actual biometric samples. Biometric templates should be obtained from biometric data, but it should not be possible to obtain that same biometric data from the biometric templates.

(28) The router should rank, where decided by the requesting Member State and where applicable according to the type of biometric data, the replies from the requested Member State or Member States or from Europol by comparing the biometric data used for querying and the biometric data supplied in the replies by the requested Member State or Member States or Europol.

(29) In the event of a match between the data used for the search and data held in the national database of the requested Member State or Member States, following a manual confirmation of the match by a qualified member of staff of the requesting Member State and following the transmission of a description of the facts and an indication of the underlying offence using the common table of offence categories set out in an implementing act to be adopted pursuant to Framework Decision 2009/315/JHA, the requested Member State should return a limited set of core data, to the extent that such core data are available. The limited set of core data should be returned via the router

([12]) 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) No 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 (OJ L 135, 22.5.2019, p. 27).

([13]) 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) No 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

and, except where a judicial authorisation is required under national law, within 48 hours of the relevant conditions having been met. That deadline will ensure fast communication exchange between Member States' competent authorities. Member States should retain control over the release of the limited set of core data. Human intervention should be maintained at key points in the process, including for the decision to launch a query, the decision to confirm a match, the decision to launch a request to receive the set of core data following a confirmed match and the decision to release personal data to the requesting Member State, in order to ensure that no core data will be exchanged in an automated manner.

(30) In the specific case of DNA, the requested Member State should also be able to confirm a match between two DNA profiles where that is relevant for the investigation of criminal offences. Following the confirmation of that match by the requested Member State and following the transmission of a description of the facts and an indication of the underlying offence using the common table of offence categories set out in an implementing act to be adopted pursuant to Framework Decision 2009/315/JHA, the requesting Member State should return a limited set of core data via the router within 48 hours of the relevant conditions having been met, except where a judicial authorisation is required under national law.

(31) Data lawfully supplied and received under this Regulation are subject to the time limits for storage and review established pursuant to Directive (EU) 2016/680.

(32) The universal message format (UMF) standard should be used in the development of the router and EPRIS, in so far as applicable. Any automated exchange of data under this Regulation should use the UMF standard, in so far as applicable. Member States' competent authorities and Europol are also encouraged to use the UMF standard in relation to any further exchange of data between them in the context of the Prüm II framework. The UMF standard should serve as the standard for structured, cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs.

(33) Only non-classified information should be exchanged via the Prüm II framework.

(34) Each Member State should notify the other Member States, the Commission, the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice (eu-LISA), established by Regulation (EU) 2018/1726 of the European Parliament and of the Council ([14]), and Europol of the content of its national databases made available via the Prüm II framework and of the conditions for automated searches.

(35) Certain aspects of the Prüm II framework cannot be covered exhaustively by this Regulation given their technical, highly detailed and frequently changing nature. Those aspects include, for example, technical arrangements and specifications for automated searching procedures, the standards for data exchange, including minimum quality standards, and the data elements to be exchanged. In order to ensure uniform conditions for the implementation of this Regulation with respect to such aspects, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([15]).

(36) Data quality is of utmost importance as a safeguard and an essential prerequisite to ensure the efficiency of this Regulation. In the context of the automated searching of biometric data and in order to ensure that the data transmitted are of sufficient quality and to reduce the risk of false matches, a minimum quality standard should be established and regularly reviewed.

([14]) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 (OJ L 295, 21.11.2018, p. 99).

([15]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(37) Given the scale and sensitivity of the personal data exchanged for the purposes of this Regulation, and the existence of different national rules for storing information on individuals in national databases, it is important to ensure that the databases used for automated searching under this Regulation are established in accordance with national law and Directive (EU) 2016/680. Therefore, prior to connecting their national databases to the router or EPRIS, Member States should conduct a data protection impact assessment as referred to in Directive (EU) 2016/680 and, where appropriate, consult the supervisory authority as provided for in that Directive.

(38) Member States and Europol should ensure the accuracy and relevance of personal data which are processed pursuant to this Regulation. Where a Member State or Europol becomes aware of the fact that data which have been supplied are incorrect or no longer up to date or should not have been supplied, it should notify the Member State which received the data or Europol, as appropriate, without undue delay. All Member States concerned or Europol, as the case may be, should correct or delete the data accordingly without undue delay. Where the Member State which received the data or Europol has reason to believe that the supplied data are incorrect or should be deleted, it should inform the Member State which provided the data without undue delay.

(39) Strong monitoring of the implementation of this Regulation is of utmost importance. In particular, compliance with rules for processing personal data should be subject to effective safeguards, and regular monitoring and audits by data controllers, supervisory authorities and the European Data Protection Supervisor, as relevant, should be ensured. Provisions allowing for a regular checking of the admissibility of queries and the lawfulness of data processing should also be in place.

(40) Supervisory authorities and the European Data Protection Supervisor should ensure coordinated supervision of the application of this Regulation within the framework of their responsibilities, in particular where they identify major discrepancies between Member State's practices or potentially unlawful transfers.

(41) When implementing this Regulation, it is crucial that Member States and Europol take note of the case law from the Court of Justice of the European Union in relation to the exchange of biometric data.

(42) Three years following the start of operations of the router and EPRIS and every four years thereafter, the Commission should produce an evaluation report that includes an assessment of the application of this Regulation by the Member States and Europol, in particular of their compliance with the relevant data protection safeguards. Evaluation reports should also include an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights. Evaluation reports should also evaluate the impact, performance, effectiveness, efficiency, security and working practices of the Prüm II framework.

(43) As this Regulation provides for the establishment of a new Prüm framework, provisions of Decisions 2008/615/JHA and 2008/616/JHA that are no longer relevant should be deleted. Those Decisions should be amended accordingly.

(44) As the router is to be developed and managed by eu-LISA, Regulation (EU) 2018/1726 should be amended by adding that to the tasks of eu-LISA.

(45) Since the objectives of this Regulation, namely to step up cross-border police cooperation and to allow Member States' competent authorities to search for missing persons and identify unidentified human remains, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(46) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(47) In accordance with Article 3 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEUs, Ireland has notified its wish to take part in the adoption and application of this Regulation.

(48) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 2 March 2022 ([16]),

HAVE ADOPTED THIS REGULATION:

*CHAPTER 1*

***General provisions***

*Article 1*

**Subject matter**

This Regulation establishes a framework for searching and exchanging information between Member States' competent authorities (the Prüm II framework) by laying down:

(a) the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records; and

(b) the rules regarding the exchange of core data following a confirmed match on biometric data.

*Article 2*

**Purpose**

The purpose of the Prüm II framework is to step up cross-border cooperation in matters covered by Part III, Title V, Chapters 4 and 5, of the Treaty on the Functioning of the European Union, particularly by facilitating the exchange of information between Member States' competent authorities, in full respect of the fundamental rights of natural persons, including the right to respect for one's private life and the right to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union.

The purpose of the Prüm II framework is also to allow Member State's competent authorities to search for missing persons in the context of criminal investigations or on humanitarian grounds and to identify human remains, in accordance with Article 29, provided that those authorities are empowered to conduct such searches and to carry out such identifications under national law.

*Article 3*

**Scope**

This Regulation applies to the databases established in accordance with national law and used for the automated transfer of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records, in compliance with, as applicable, Directive (EU) 2016/680 or Regulation (EU) 2018/1725, (EU) No 2016/794 or (EU) 2016/679.

([16]) OJ C 225, 9.6.2022, p. 6.

*Article 4*

**Definitions**

For the purposes of this Regulation, the following definitions apply:

(1) 'loci' (singular: 'locus') means DNA locations containing identification characteristics of an analysed human DNA sample;

(2) 'DNA profile' means a letter or number code which represents a set of loci or the particular molecular structure at the various loci;

(3) 'DNA reference data' means a DNA profile and the reference number referred to in Article 7;

(4) 'identified DNA profile' means the DNA profile of an identified person;

(5) 'unidentified DNA profile' means the DNA profile collected during the investigation of criminal offences and belonging to a person not yet identified, including a DNA profile obtained from traces;

(6) 'dactyloscopic data' means images of fingerprints, images of fingerprint latents, images of palm prints, images of palm print latents and templates of such images (coded minutiae) that are stored and dealt with in an automated database;

(7) 'dactyloscopic reference data' means dactyloscopic data and the reference number referred to in Article 12;

(8) 'unidentified dactyloscopic data' means dactyloscopic data collected during the investigation of a criminal offence and belonging to a person not yet identified, including dactyloscopic data obtained from traces;

(9) 'identified dactyloscopic data' means the dactyloscopic data of an identified person;

(10) 'individual case' means a single file related to the prevention, detection or investigation of a criminal offence, to the search for a missing person or to the identification of unidentified human remains;

(11) 'facial image' means a digital image of the face;

(12) 'facial image reference data' means a facial image and the reference number referred to in Article 21;

(13) 'unidentified facial image' means a facial image collected during the investigation of a criminal offence and belonging to a person not yet identified, including a facial image obtained from traces;

(14) 'identified facial image' means the facial image of an identified person;

(15) 'biometric data' means DNA profiles, dactyloscopic data or facial images;

(16) 'alphanumeric data' means data represented by letters, digits, special characters, spaces and punctuation marks;

(17) 'match' means the existence of a correspondence as a result of an automated comparison between personal data held in a database;

(18) 'candidate' means data with which a match has occurred;

(19) 'requesting Member State' means a Member State conducting a search via the Prüm II framework;

(20) 'requested Member State' means a Member State in whose databases a requesting Member State conducts a search via the Prüm II framework;

(21) ‘police records’ means biographical data of suspects and convicted persons available in national databases established for the prevention, detection and investigation of criminal offences;

(22) ‘pseudonymisation’ means pseudonymisation as defined in Article 3, point (5), of Directive (EU) 2016/680;

(23) ‘suspect’ means a person as referred to in Article 6, point (a), of Directive (EU) 2016/680;

(24) ‘personal data’ means personal data as defined in Article 3, point (1), of Directive (EU) 2016/680;

(25) ‘Europol data’ means any operational personal data processed by Europol in accordance with Regulation (EU) 2016/794;

(26) ‘competent authority’ means any public authority competent for the prevention, detection or investigation of criminal offences, or any other body or entity entrusted by Member State law with the exercise of public authority and public powers for the purposes of the prevention, detection or investigation of criminal offences;

(27) ‘supervisory authority’ means an independent public authority established by a Member State pursuant to Article 41 of Directive (EU) 2016/680;

(28) ‘SIENA’ means the secure information exchange network application managed and developed by Europol in accordance with Regulation (EU) 2016/794;

(29) ‘incident’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555 of the European Parliament and of the Council ([17]).

(30) ‘significant incident’ means an incident unless that incident has a limited impact and is likely to be already well understood in terms of method or technology;

(31) ‘significant cyber threat’ means a cyber threat with the opportunity and capability, and the purpose of which is, to cause a significant incident;

(32) ‘significant vulnerability’ means a vulnerability that will likely lead to a significant incident if it is exploited.

*CHAPTER 2*

***Exchange of data***

Section 1

**DNA profiles**

*Article 5*

**DNA reference data**

1. Member States shall ensure the availability of DNA reference data from their national DNA databases for the purposes of automated searches by other Member States and Europol pursuant to this Regulation.

DNA reference data shall not contain any additional data from which an individual can be directly identified.

Unidentified DNA profiles shall be recognisable as such.

2. DNA reference data shall be processed in accordance with this Regulation and in compliance with the national law applicable to the processing of those data.

([17]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

3. The Commission shall adopt an implementing act to specify the identification characteristics of a DNA profile which is to be exchanged. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 6*

**Automated searching of DNA profiles**

1. For the investigation of criminal offences, Member States shall, at the time of initial connection to the router via their national contact points, conduct an automated search by comparing all the DNA profiles stored in their DNA databases with all the DNA profiles stored in all other Member States' DNA databases and Europol data. Each Member State shall agree bilaterally with each other Member State and with Europol on the arrangements for those automated searches in accordance with the rules and procedures laid down in this Regulation.

2. For the investigation of criminal offences, Member States shall, via their national contact points, conduct automated searches by comparing all the new DNA profiles added to their DNA databases with all the DNA profiles stored in all other Member States' DNA databases and Europol data.

3. Where searches as referred to in paragraph 2 could not take place, the Member State concerned may agree bilaterally with each other Member State and with Europol to conduct them at a later stage by comparing DNA profiles with all DNA profiles stored in all other Member States' DNA databases and Europol data. The Member State concerned shall agree bilaterally with each other Member State and with Europol on the arrangements for those automated searches in accordance with the rules and procedures laid down in this Regulation.

4. Searches as referred to in paragraphs 1, 2 and 3 shall only be conducted in the framework of individual cases and in compliance with the national law of the requesting Member State.

5. Where an automated search shows that a supplied DNA profile matches DNA profiles stored in the requested Member State's searched database or databases, the national contact point of the requesting Member State shall receive in an automated manner the DNA reference data with which a match has been found.

6. The national contact point of the requesting Member State may decide to confirm a match between two DNA profiles. Where it decides to confirm a match between two DNA profiles, it shall inform the requested Member State and shall ensure that at least one qualified member of staff conducts a manual review in order to confirm that match with DNA reference data received from the requested Member State.

7. Where relevant for the investigation of criminal offences, the national contact point of the requested Member State may decide to confirm a match between two DNA profiles. Where it decides to confirm a match between two DNA profiles, it shall inform the requesting Member State and shall ensure that at least one qualified member of staff conducts a manual review in order to confirm that match with DNA reference data received from the requesting Member State.

*Article 7*

**Reference numbers for DNA profiles**

The reference numbers for DNA profiles shall be the combination of the following:

(a) a reference number allowing Member States, in the event of a match, to retrieve further data and other information in their national DNA databases in order to supply them or it to one, several or all of the other Member States in accordance with Article 47 or to Europol in accordance with Article 49(6);

(b) a reference number allowing Europol, in the event of a match, to retrieve further data and other information for the purposes of Article 48(1) of this Regulation in order to supply them or it to one, several or all Member States in accordance with Regulation (EU) 2016/794;

(c) a code to indicate the Member State which holds the DNA profile;

(d) a code to indicate whether the DNA profile is an identified DNA profile or an unidentified DNA profile.

*Article 8*

**Principles for the exchange of DNA profiles**

1. Member States shall take appropriate measures to ensure the confidentiality and integrity of DNA reference data sent to other Member States or Europol, including their encryption. Europol shall take appropriate measures to ensure the confidentiality and integrity of DNA reference data sent to Member States, including their encryption.

2. Each Member State and Europol shall ensure that the DNA profiles it transmits are of sufficient quality for automated comparison. The Commission shall establish, by means of implementing acts, a minimum quality standard to allow for the comparison of DNA profiles.

3. The Commission shall adopt implementing acts specifying the relevant European or international standards to be used by Member States and Europol for the exchange of DNA reference data.

4. The implementing acts referred to in paragraphs 2 and 3 of this Article shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 9*

**Rules for requests and replies regarding DNA profiles**

1. A request for an automated search of DNA profiles shall include only the following information:

(a) the code of the requesting Member State;

(b) the date and time of the request and the request number;

(c) DNA reference data;

(d) whether the DNA profiles transmitted are unidentified DNA profiles or identified DNA profiles.

2. A reply to a request as referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches or no matches;

(b) the date and time of the request and the request number;

(c) the date and time of the reply and the reply number;

(d) the codes of the requesting and requested Member States;

(e) the reference numbers of the DNA profiles from the requesting and requested Member States;

(f) whether the DNA profiles transmitted are unidentified DNA profiles or identified DNA profiles;

(g) the matching DNA profiles.

3. A match shall be automatically notified only where the automated search has resulted in a match of a minimum number of loci. The Commission shall adopt implementing acts specifying the minimum number of loci for that purpose in accordance with the examination procedure referred to in Article 77(2).

4. Where a search with unidentified DNA profiles results in a match, each requested Member State with matching data may insert a marking in its national database indicating that there has been a match for that DNA profile following another Member State's search. The marking shall include the reference number of the DNA profile used by the requesting Member State.

5. Member States shall ensure that requests as referred to in paragraph 1 of this Article are consistent with notifications sent pursuant to Article 74. Those notifications shall be reproduced in the practical handbook referred to in Article 79.

Section 2

**Dactyloscopic data**

*Article 10*

**Dactyloscopic reference data**

1. Member States shall ensure the availability of dactyloscopic reference data from their national databases established for the prevention, detection and investigation of criminal offences.

2. Dactyloscopic reference data shall not contain any additional data from which an individual can be directly identified.

3. Unidentified dactyloscopic data shall be recognisable as such.

*Article 11*

**Automated searching of dactyloscopic data**

1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to the dactyloscopic reference data in their national databases established for that purpose to conduct automated searches by comparing dactyloscopic reference data.

Searches as referred to in the first subparagraph shall only be conducted in the framework of individual cases and in compliance with the national law of the requesting Member State.

2. The national contact point of the requesting Member State may decide to confirm a match between two sets of dactyloscopic data. Where it decides to confirm a match between two sets of dactyloscopic data, it shall inform the requested Member State and shall ensure that at least one qualified member of staff conducts a manual review in order to confirm that match with dactyloscopic reference data received from the requested Member State.

*Article 12*

**Reference numbers for dactyloscopic data**

The reference numbers for dactyloscopic data shall be the combination of the following:

(a) a reference number allowing Member States, in the event of a match, to retrieve further data and other information in their databases referred to in Article 10 in order to supply them or it to one, several or all of the other Member States in accordance with Article 47 or to Europol in accordance with Article 49(6);

(b) a reference number allowing Europol, in the event of a match, to retrieve further data and other information for the purposes of Article 48(1) of this Regulation in order to supply them or it to one, several or all Member States in accordance with Regulation (EU) 2016/794;

(c) a code to indicate the Member State which holds the dactyloscopic data.

*Article 13*

**Principles for the exchange of dactyloscopic data**

1. Member States shall take appropriate measures to ensure the confidentiality and integrity of dactyloscopic data sent to other Member States or Europol, including their encryption. Europol shall take appropriate measures to ensure the confidentiality and integrity of dactyloscopic data sent to Member States, including their encryption.

2. Each Member State and Europol shall ensure that the dactyloscopic data it transmits are of sufficient quality for automated comparison. The Commission shall establish, by means of implementing acts, a minimum quality standard to allow for the comparison of dactyloscopic data.

3. Dactyloscopic data shall be digitalised and transmitted to the other Member States or Europol in accordance with European or international standards. The Commission shall adopt implementing acts specifying the relevant European or international standards to be used by Member States and Europol for the exchange of dactyloscopic data.

4. The implementing acts referred to in paragraphs 2 and 3 of this Article shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 14*

**Search capacities for dactyloscopic data**

1. Each Member State shall ensure that its search requests do not exceed the search capacities specified by the requested Member State or Europol to ensure system readiness and to avoid overloading the system. For the same purpose, Europol shall ensure that its search requests do not exceed the search capacities specified by the requested Member State.

Member States shall inform the other Member States, the Commission, eu-LISA and Europol about their maximum search capacities per day for identified and unidentified dactyloscopic data. Europol shall inform Member States, the Commission and eu-LISA about its maximum search capacities per day for identified and unidentified dactyloscopic data. Member States or Europol may temporarily or permanently raise those search capacities at any time, including in a case of urgency. Where a Member State raises those maximum search capacities, it shall notify the other Member States, the Commission, eu-LISA and Europol of the new maximum search capacities. Where Europol raises those maximum search capacities, it shall notify the Member States, the Commission and eu-LISA of the new maximum search capacities.

2. The Commission shall adopt implementing acts specifying the maximum numbers of candidates accepted for comparison per transmission and the distribution of unused search capacities between Member States in accordance with the examination procedure referred to in Article 77(2).

*Article 15*

**Rules for requests and replies regarding dactyloscopic data**

1. A request for an automated search of dactyloscopic data shall include only the following information:

(a) the code of the requesting Member State;

(b) the date and time of the request and the request number;

(c) dactyloscopic reference data.

2. A reply to a request as referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches or no matches;

(b) the date and time of the request and the request number;

(c) the date and time of the reply and the reply number;

(d) the codes of the requesting and requested Member States;

(e) the reference numbers of the dactyloscopic data from the requesting and requested Member States;

(f) the matching dactyloscopic data.

3. Member States shall ensure that requests as referred to in paragraph 1 of this Article are consistent with notifications sent pursuant to Article 74. Those notifications shall be reproduced in the practical handbook referred to in Article 79.

Section 3

**Vehicle registration data**

*Article 16*

**Automated searching of vehicle registration data**

1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to the following national vehicle registration data to conduct automated searches in individual cases:

(a) data relating to the owner or holder of the vehicle;

(b) data relating to the vehicle.

2. Searches as referred to in paragraph 1 shall be conducted only with the following data:

(a) a complete chassis number;

(b) a complete registration number; or

(c) where authorised by the national law of the requested Member State, data relating to the owner or holder of the vehicle.

3. Searches as referred to in paragraph 1 conducted with data related to the owner or holder of the vehicle shall only be conducted in the case of suspects or convicted persons. All of the following identification data shall be used for the purposes of such searches:

(a) where the owner or holder of the vehicle is a natural person:

(i) the first name or names of the natural person;

(ii) the family name or names of the natural person; and

(iii) the date of birth of the natural person;

(b) where the owner or holder of the vehicle is a legal person, that legal person's name.

4. Searches as referred to in paragraph 1 shall be conducted only in compliance with the national law of the requesting Member State.

*Article 17*

**Principles of automated searching of vehicle registration data**

1. For automated searching of vehicle registration data, Member States shall use the European Vehicle and Driving Licence Information System (Eucaris).

2. Information exchanged via Eucaris shall be transmitted in encrypted form.

3. The Commission shall adopt implementing acts specifying the data elements of the vehicle registration data which can be exchanged and the technical procedure for Eucaris to query Member States' databases. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 18*

**Keeping of logs**

1. Each Member State shall keep logs of queries that the staff of its competent authorities duly authorised to exchange vehicle registration data make and logs of queries requested by other Member States. Europol shall keep logs of queries that its duly authorised staff make.

Each Member State and Europol shall keep logs of all data processing operations concerning vehicle registration data. Those logs shall include the following:

(a) whether it was a Member State or Europol that launched the request for a query; where it was a Member State that launched the request for a query, the Member State in question;

(b) the date and time of the request;

(c) the date and time of the reply;

(d) the national databases to which a request for a query was sent;

(e) the national databases that provided a positive reply.

2. The logs referred to in paragraph 1 shall be used only for the collection of statistics, for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and shall be erased three years after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

3. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 55.

Section 4

**Facial images**

*Article 19*

**Facial image reference data**

1. Member States shall ensure the availability of facial image reference data of suspects, convicted persons and, where permitted under national law, victims from their national databases established for the prevention, detection and investigation of criminal offences.

2. Facial image reference data shall not contain any additional data from which an individual can be directly identified.

3. Unidentified facial images shall be recognisable as such.

*Article 20*

**Automated searching of facial images**

1. For the prevention, detection and investigation of criminal offences punishable by a maximum term of imprisonment of at least one year under the law of the requesting Member State, Member States shall allow national contact points of other Member States and Europol access to the facial image reference data in their national databases to conduct automated searches.

Searches as referred to in the first subparagraph shall only be conducted in the framework of individual cases and in compliance with the national law of the requesting Member State.

Profiling as referred to in Article 11(3) of Directive (EU) 2016/680 shall be prohibited.

2. The national contact point of the requesting Member State may decide to confirm a match between two facial images. Where it decides to confirm a match between two facial images, it shall inform the requested Member State and shall ensure that at least one qualified member of staff conducts a manual review in order to confirm that match with facial image reference data received from the requested Member State.

*Article 21*

**Reference numbers for facial images**

The reference numbers for facial images shall be the combination of the following:

(a) a reference number allowing Member States, in the event of a match, to retrieve further data and other information in their databases referred to in Article 19 in order to supply them or it to one, several or all of the other Member States in accordance with Article 47 or to Europol in accordance with Article 49(6);

(b) a reference number allowing Europol, in the event of a match, to retrieve further data and other information for the purposes of Article 48(1) of this Regulation in order to supply them or it to one, several or all Member States in accordance with Regulation (EU) 2016/794;

(c) a code to indicate the Member State which holds the facial images.

*Article 22*

**Principles for the exchange of facial images**

1. Member States shall take appropriate measures to ensure the confidentiality and integrity of facial images sent to other Member States or Europol, including their encryption. Europol shall take appropriate measures to ensure the confidentiality and integrity of facial images sent to Member States, including their encryption.

2. Each Member State and Europol shall ensure that the facial images it transmits are of sufficient quality for automated comparison. The Commission shall establish, by means of implementing acts, a minimum quality standard to allow for the comparison of facial images. Where the report referred to in Article 80(7) shows a high risk of false matches, the Commission shall review those implementing acts.

3. The Commission shall adopt implementing acts specifying the relevant European or international standards to be used by Member States and Europol for the exchange of facial images.

4. The implementing acts referred to in paragraphs 2 and 3 of this Article shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 23*

**Search capacities for facial images**

1. Each Member State shall ensure that its search requests do not exceed the search capacities specified by the requested Member State or Europol to ensure system readiness and to avoid overloading the system. For the same purpose, Europol shall ensure that its search requests do not exceed the search capacities specified by the requested Member State.

Member States shall inform the other Member States, the Commission, eu-LISA and Europol about their maximum search capacities per day for identified and unidentified facial images. Europol shall inform the Member States, the Commission and eu-Lisa about its maximum search capacities per day for identified and unidentified facial images. Member States or Europol may temporarily or permanently raise those search capacities at any time, including in a case of urgency. Where a Member State raises those maximum search capacities, it shall notify the other Member States, the Commission, eu-LISA and Europol of the new maximum search capacities. Where Europol raises those maximum search capacities, it shall notify the Member States, the Commission and eu-LISA of the new maximum search capacities.

2. The Commission shall adopt implementing acts specifying the maximum numbers of candidates accepted for comparison per transmission and the distribution of unused search capacities between Member States in accordance with the examination procedure referred to in Article 77(2).

*Article 24*

**Rules for requests and replies regarding facial images**

1. A request for an automated search of facial images shall include only the following information:

(a) the code of the requesting Member State;

(b) the date and time of the request and the request number;

(c) facial image reference data.

2. A reply to a request as referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches or no matches;

(b) the date and time of the request and the request number;

(c) the date and time of the reply and the reply number;

(d) the codes of the requesting and requested Member States;

(e) the reference numbers of the facial images from the requesting and requested Member States;

(f) the matching facial images.

3. Member States shall ensure that requests as referred to in paragraph 1 of this Article are consistent with notifications sent pursuant to Article 74. Those notifications shall be reproduced in the practical handbook referred to in Article 79.

Section 5

## Police records

*Article 25*

### Police records

1. Member States may participate in the automated exchange of police records. For the purposes of such exchanges, participating Member States shall ensure the availability of national police record indexes which contain sets of biographical data of suspects and convicted persons from their national databases established for the prevention, detection and investigation of criminal offences. Those sets of data shall contain only the following data to the extent that they are available:

(a) first name or names;

(b) family name or names;

(c) alias or aliases and previously used name or names;

(d) date of birth;

(e) nationality or nationalities;

(f) country of birth;

(g) gender.

2. The data referred to in paragraph 1, points (a), (b) and (c), shall be pseudonymised.

*Article 26*

### Automated searching of national police record indexes

For the prevention, detection and investigation of criminal offences punishable by a maximum term of imprisonment of at least one year under the law of the requesting Member State, Member States participating in the automated exchange of police records shall allow national contact points of other participating Member States and Europol access to data from their national police record indexes to conduct automated searches.

Searches as referred to in the first paragraph shall only be conducted in the framework of individual cases and in compliance with the national law of the requesting Member State.

*Article 27*

### Reference numbers for police records

The reference numbers for police records shall be the combination of the following:

(a) a reference number allowing Member States, in the event of a match, to retrieve biographical data and other information in their national police record indexes referred to in Article 25 in order to supply them or it to one, several or all of the other Member States in accordance with Article 44;

(b) a code to indicate the Member State which holds the police records.

*Article 28*

### Rules for requests and replies regarding police records

1. A request for an automated search of national police record indexes shall include only the following information:

(a) the code of the requesting Member State;

(b) the date and time of the request and the request number;

(c) the data referred to in Article 25, in so far as they are available.

2. A reply to a request as referred to in paragraph 1 shall contain only the following information:

(a) an indication as to the number of matches;

(b) the date and time of the request and the request number;

(c) the date and time of the reply and the reply number;

(d) the codes of the requesting and requested Member States;

(e) the reference numbers of the police records from the requested Member States.

3. Member States shall ensure that requests as referred to in paragraph 1 of this Article are consistent with notifications sent pursuant to Article 74. Those notifications shall be reproduced in the practical handbook referred to in Article 79.

Section 6

**Common provisions**

*Article 29*

**Missing persons and unidentified human remains**

1. Where a national authority has been so empowered by national legislative measures as referred to in paragraph 2, it may conduct automated searches using the Prüm II framework for the following purposes only:

(a) searching for missing persons in the context of criminal investigations or on humanitarian grounds;

(b) identifying human remains.

2. Member States wishing to avail themselves of the possibility provided for in paragraph 1 shall, by means of national legislative measures, designate the national authorities competent for the purposes laid down therein and lay down the procedures, conditions and criteria, including the humanitarian grounds on which it is permitted to conduct automated searches for missing persons as referred to in paragraph 1, point (a).

*Article 30*

**National contact points**

Each Member State shall designate one or more national contact points for the purposes of Articles 6, 11, 16, 20 and 26.

*Article 31*

**Implementing measures**

The Commission shall adopt implementing acts specifying the technical arrangements for the Member States with respect to the procedures set out in Articles 6, 11, 16, 20 and 26. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 32*

**Availability of the automated exchange of data at national level**

1. Member States shall take all necessary measures to ensure that automated searching of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records is possible 24 hours a day, 7 days a week.

2. National contact points shall immediately inform each other, the Commission, eu-LISA and Europol of any unavailability of the automated exchange of data, including, where applicable, of any technical faults causing that unavailability.

National contact points shall agree, in accordance with the applicable Union and national law, on temporary alternative information exchange arrangements to be used where the automated exchange of data is unavailable.

3. Where the automated exchange of data is unavailable, national contact points shall ensure that it is re-established by any means necessary and without delay.

*Article 33*

**Justification for the processing of data**

1. Each Member State shall keep a record of the justifications for the queries that its competent authorities make.

Europol shall keep a record of the justifications for the queries it makes.

2. The justifications referred to in paragraph 1 shall include:

(a) the purpose of the query, including a reference to the specific case or investigation and, where applicable, the criminal offence;

(b) an indication as to whether the query concerns a suspect or a person convicted of a criminal offence, a victim of a criminal offence, a missing person or unidentified human remains;

(c) an indication as to whether the query aims to identify a person or obtain more data on a known person.

3. The justifications referred to in paragraph 1 of this Article shall be traceable to the logs referred to in Articles 18, 40 and 45. Those justifications shall only be used for assessing whether the searches are proportionate and necessary for the purpose of preventing, detecting or investigating a criminal offence, for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those justifications shall be protected by appropriate measures against unauthorised access and shall be erased three years after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the justification.

4. In order to assess the proportionality and necessity of searches for the purpose of preventing, detecting or investigating a criminal offence or for the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to those justifications for self-monitoring as referred to in Article 55.

*Article 34*

**Use of the universal message format**

1. The universal message format (UMF) standard established by Article 38 of Regulation (EU) 2019/818 shall be used in the development of the router referred to in Article 35 of this Regulation and the European Police Record Index System (EPRIS) in so far as possible.

2. Any automated exchange of data in accordance with this Regulation shall use the UMF standard in so far as possible.

*CHAPTER 3*

***Architecture***

Section 1

**Router**

*Article 35*

**Router**

1. A router is established for the purpose of facilitating the establishment of connections between Member States, and between Member States and Europol, for querying with, retrieving and scoring biometric data and for retrieving alphanumeric data in accordance with this Regulation.

2. The router shall be composed of:

(a) a central infrastructure, including a search tool enabling the simultaneous querying of the national databases referred to in Articles 5, 10 and 19 and of Europol data;

(b) a secure communication channel between the central infrastructure, the competent authorities authorised to use the router pursuant to Article 36 and Europol;

(c) a secure communication infrastructure between the central infrastructure and the European Search Portal, established by Article 6 of Regulation (EU) 2019/817 and Article 6 of Regulation (EU) 2019/818, for the purposes of Article 39.

*Article 36*

**Use of the router**

The use of the router shall be reserved to the Member States' competent authorities that are authorised to access and exchange DNA profiles, dactyloscopic data and facial images in accordance with this Regulation and to Europol in accordance with this Regulation and Regulation (EU) 2016/794.

*Article 37*

**Processes**

1. The competent authorities authorised to use the router pursuant to Article 36 or Europol shall request a query by submitting biometric data to the router. The router shall dispatch the request for a query to databases of all or specific Member States and Europol data simultaneously with the data submitted by the user in accordance with his or her access rights.

2. Upon receipt of a request for a query from the router, each requested Member State shall launch a query of their databases in an automated manner and without delay. Upon receipt of a request for a query from the router, Europol shall launch a query of Europol data in an automated manner and without delay.

3. Any matches resulting from queries as referred to in paragraph 2 shall be sent back in an automated manner to the router. The requesting Member State shall be notified in an automated manner where there is no match.

4. The router shall rank, where the requesting Member State so decides and where applicable, the replies by comparing the biometric data used for querying and the biometric data supplied in the replies from the requested Member State or Member States or Europol.

5. The router shall return the list of matching biometric data and their ranking to the router user.

6. The Commission shall adopt implementing acts specifying the technical procedure for the router to query Member States' databases and Europol data, the format in which the router answers such queries and the technical rules for comparing and ranking the correspondence between biometric data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 38*

**Quality check**

The requested Member State shall check the quality of the transmitted data by means of an automated procedure.

The requested Member State shall, without delay, inform the requesting Member State via the router where the data are unsuitable for automated comparison.

*Article 39*

**Interoperability between the router and the Common Identity Repository for the purposes of law enforcement access**

1. Where designated authorities as defined in Article 4, point (20), of Regulation (EU) 2019/817 and Article 4, point (20), of Regulation (EU) 2019/818 are authorised to use the router pursuant to Article 36 of this Regulation, they may launch a query to Member States' databases and Europol data simultaneously with a query to the Common Identity Repository, established by Article 17 of Regulation (EU) 2019/817 and Article 17 of Regulation (EU) 2019/818, provided that the relevant conditions under Union law have been fulfilled and that the query is launched in accordance with their access rights. For that purpose, the router shall query the Common Identity Repository via the European Search Portal.

2. Queries to the Common Identity Repository for law enforcement purposes shall be carried out in accordance with Article 22 of Regulation (EU) 2019/817 and Article 22 of Regulation (EU) 2019/818. Any result from such queries shall be transmitted via the European Search Portal.

Simultaneous queries of the Member States' databases and Europol data and the Common Identity Repository shall be launched only where there are reasonable grounds to believe that data on a suspect, perpetrator or victim of a terrorist offence or other serious criminal offence as defined in Article 4, points (21) and (22), respectively, of Regulation (EU) 2019/817 and Article 4, points (21) and (22), respectively, of Regulation (EU) 2019/818 are stored in the Common Identity Repository.

*Article 40*

**Keeping of logs**

1. eu-LISA shall keep logs of all data processing operations in the router. Those logs shall include the following:

(a) whether it was a Member State or Europol that launched the request for a query; where it was a Member State that launched the request for a query, the Member State in question;

(b) the date and time of the request;

(c) the date and time of the reply;

(d) the national databases or Europol data to which a request for a query was sent;

(e) the national databases or Europol data that provided a reply;

(f) where applicable, the fact that there was a simultaneous query to the Common Identity Repository.

2. Each Member State shall keep logs of queries that the staff of its competent authorities duly authorised to use the router make and logs of queries requested by other Member States.

Europol shall keep logs of queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 shall be used only for the collection of statistics, for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and erased three years after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 55.

*Article 41*

**Notification procedures where it is technically impossible to use the router**

1. Where it is technically impossible to use the router to query one or several national databases or Europol data because of a failure of the router, eu-LISA shall notify the router users referred to Article 36 in an automated manner. eu-LISA shall take appropriate measures to address the technical impossibility to use the router without delay.

2. Where it is technically impossible to use the router to query one or several national databases because of a failure of the national infrastructure in a Member State, that Member State shall notify the other Member States, the Commission, eu-LISA and Europol in an automated manner. The Member State concerned shall take appropriate measures to address the technical impossibility to use the router without delay.

3. Where it is technically impossible to use the router to query Europol data because of a failure of Europol's infrastructure, Europol shall notify the Member States, the Commission and eu-LISA in an automated manner. Europol shall take appropriate measures to address the technical impossibility to use the router without delay.

Section 2

**EPRIS**

*Article 42*

**EPRIS**

1. The European Police Record Index System (EPRIS) is hereby established. For the automated searching of national police record indexes referred to in Article 26, Member States and Europol shall use EPRIS.

2. EPRIS shall be composed of:

(a) a decentralised infrastructure in the Member States, including a search tool enabling the simultaneous querying of national police record indexes, based on national databases;

(b) a central infrastructure, supporting the search tool, enabling the simultaneous querying of national police record indexes;

(c) a secure communication channel between the central infrastructure, Member States and Europol.

*Article 43*

**Use of EPRIS**

1. For the purpose of searching national police record indexes via EPRIS, at least two of the following sets of data shall be used:

(a) first name or names;

(b) family name or names;

(c) date of birth.

2. Where available, the following sets of data may also be used:

(a) alias or aliases and previously used name or names;

(b) nationality or nationalities;

(c) country of birth;

(d) gender.

3. The data referred to in paragraph 1, points (a) and (b), and paragraph 2, point (a), shall be pseudonymised.

*Article 44*

**Processes**

1. Where a Member State or Europol requests a query, it shall submit the data referred to in Article 43.

EPRIS shall dispatch the request for a query to the Member States' national police record indexes with the data submitted by the requesting Member State or Europol and in accordance with this Regulation.

2. Upon receipt of a request for a query from EPRIS, each requested Member State shall launch a query of their national police record index in an automated manner and without delay.

3. Any matches resulting from queries as referred to in paragraph 1 in each requested Member State's police records indexes shall be sent back in an automated manner to EPRIS.

4. The list of matches shall be returned to the requesting Member State or Europol by EPRIS in an automated manner. The list of matches shall indicate the quality of the match and the Member State or Member States whose police record indexes contain data that resulted in the match or matches.

5. Upon receipt of the list of matches, the requesting Member State shall decide the matches for which a follow-up is necessary and send a reasoned follow-up request containing the data referred to in Articles 25 and 27 and any additional relevant information to the requested Member State or Member States via SIENA. The requested Member State or Member States shall process such requests without delay in order to decide whether to share the data stored in its or their database.

6. The Commission shall adopt implementing acts specifying the technical procedure for EPRIS to query Member States' police record indexes and the format and maximum number of replies. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 45*

**Keeping of logs**

1. Each participating Member State and Europol shall keep logs of all data processing operations in EPRIS. Those logs shall include the following:

(a) whether it was a Member State or Europol that launched the request for a query; where it was a Member State that launched the request for a query, the Member State in question;

(b) the date and time of the request;

(c) the date and time of the reply;

(d) the national databases to which a request for a query was sent;

(e) the national databases that provided a reply.

2. Each participating Member State shall keep logs of the requests for queries that the staff of its competent authorities duly authorised to use EPRIS make. Europol shall keep logs of requests for queries that its duly authorised staff make.

3. The logs referred to in paragraphs 1 and 2 shall be used only for the collection of statistics, for data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, and for ensuring data security and integrity. Those logs shall be protected by appropriate measures against unauthorised access and shall be erased three years after their creation. If, however, they are required for monitoring procedures that have already begun, they shall be erased once the monitoring procedures no longer require the logs.

4. For the purposes of data protection monitoring, including checking the admissibility of a query and the lawfulness of data processing, the data controllers shall have access to the logs for self-monitoring as referred to in Article 55.

*Article 46*

**Notification procedures where it is technically impossible to use EPRIS**

1. Where it is technically impossible to use EPRIS to query one or several national police record indexes because of a failure of Europol's infrastructure, Europol shall notify Member States in an automated manner. Europol shall take measures to address the technical impossibility of using EPRIS without delay.

2. Where it is technically impossible to use EPRIS to query one or several national police record indexes because of a failure of the national infrastructure in a Member State, that Member State shall notify the other Member States, the Commission and Europol in an automated manner. Member States shall take measures to address the technical impossibility of using EPRIS without delay.

*CHAPTER 4*

***Exchange of data following a match***

*Article 47*

**Exchange of core data**

1. A set of core data shall be returned via the router within 48 hours of all of the following conditions being met:

(a) the procedures referred to in Article 6, 11 or 20 show a match between the data used for the search and data stored in the database of the requested Member State or Member States;

(b) the match referred to in point (a) of this paragraph has been manually confirmed by a qualified member of staff of the requesting Member State as referred to in Article 6(6), Article 11(2) and Article 20(2), or, in the case of DNA profiles referred to in Article 6(7), of the requested Member State;

(c) a description of the facts and an indication of the underlying offence have been transmitted, using the common table of offence categories set out in an implementing act to be adopted pursuant to Article 11b(1), point (a), of Framework Decision 2009/315/JHA, by the requesting Member State or, in the case of DNA profiles referred to in Article 6(7), by the requested Member State in order to assess the proportionality of the request, including the seriousness of the offence for which a search was conducted, in accordance with the national law of the Member State which provides the set of core data.

2. Where, under its national law, a Member State can provide a particular set of core data only after having obtained a judicial authorisation, that Member State may deviate from the time limit set out in paragraph 1 in so far as necessary for the purpose of obtaining such an authorisation.

3. The set of core data referred to in paragraph 1 of this Article shall be returned by the requested Member State or, in the case of DNA profiles referred to in Article 6(7), by the requesting Member State.

4. Where the confirmed match concerns identified data of a person, the set of core data referred to in paragraph 1 shall contain the following data to the extent that they are available:

(a) first name or names;

(b) family name or names;

(c) alias or aliases and previously used name or names;

(d) date of birth;

(e) nationality or nationalities;

(f) place and country of birth;

(g) gender;

(h) the date on which and the place where the biometric data were acquired;

(i) the criminal offence for which the biometric data were acquired;

(j) the criminal case number;

(k) the competent authority responsible for the criminal case.

5. Where the confirmed match concerns unidentified data or traces, the set of core data referred to in paragraph 1 shall contain the following data to the extent that they are available:

(a) the date on which and the place where the biometric data were acquired;

(b) the criminal offence for which the biometric data were acquired;

(c) the criminal case number;

(d) the competent authority responsible for the criminal case.

6. The return of core data by the requested Member State or, in the case of DNA profiles referred to in Article 6(7), by the requesting Member State shall be subject to the decision of a human.

*CHAPTER 5*

***Europol***

*Article 48*

**Access by Member States to biometric data provided by third countries and stored by Europol**

1. Member States shall, in accordance with Regulation (EU) 2016/794, have access to, and be able to search via the router, biometric data which have been provided to Europol by third countries for the purposes of Article 18(2), points (a), (b) and (c), of Regulation (EU) 2016/794.

2. Where a search as referred to in paragraph 1 results in a match between the data used for the search and data provided by a third country and stored by Europol, the follow-up shall take place in accordance with Regulation (EU) 2016/794.

*Article 49*

**Access by Europol to data stored in Member States' databases, using data provided by third countries**

1. Where necessary to achieve the objectives set out in Article 3 of Regulation (EU) 2016/794, Europol shall, in accordance with that Regulation and this Regulation, have access to data which are stored by Member States in their national databases and police record indexes.

2. Europol queries performed with biometric data as a search criterion shall be carried out using the router.

3. Europol queries performed with vehicle registration data as a search criterion shall be carried out using Eucaris.

4. Europol queries performed with biographical data of suspects and convicted persons as referred to in Article 25 as a search criterion shall be carried out using EPRIS.

5. Europol shall conduct searches with data provided by third countries in accordance with paragraphs 1 to 4 of this Article only where necessary for carrying out its tasks for the purposes of Article 18(2), points (a) and (c), of Regulation (EU) 2016/794.

6. Where the procedures referred to in Article 6, 11 or 20 show a match between the data used for the search and data held in the national database of the requested Member State or Member States, Europol shall inform only the Member State or Member States involved.

The requested Member State shall decide whether to return a set of core data via the router within 48 hours of all of the following conditions being met:

(a) a match as referred to in the first subparagraph has been manually confirmed by a qualified member of staff of Europol;

(b) a description of the facts and an indication of the underlying offence have been transmitted, using the common table of offence categories set out in an implementing act to be adopted pursuant to Article 11b(1), point (a), of Framework Decision 2009/315/JHA, by Europol in order to assess the proportionality of the request, including the seriousness of the offence for which a search was conducted, in accordance with the national law of the Member State which provides the set of core data;

(c) the name of the third country which provided the data has been transmitted.

Where, under its national law, a Member State can provide a particular set of core data only after having obtained a judicial authorisation, that Member State may deviate from the time limit set out in the second subparagraph in so far as necessary for the purpose of obtaining such an authorisation.

Where the confirmed match concerns identified data of a person, the set of core data referred to in the second subparagraph shall contain the following data to the extent that they are available:

(a) first name or names;

(b) family name or names;

(c) alias or aliases and previously used name or names;

(d) date of birth;

(e) nationality or nationalities;

(f) place and country of birth;

(g) gender;

(h) the date on which and the place where the biometric data were acquired;

(i) the criminal offence for which the biometric data were acquired;

(j) the criminal case number;

(k) the competent authority responsible for the criminal case.

Where the confirmed match concerns unidentified data or traces, the set of core data referred to in the second subparagraph shall contain the following data to the extent that they are available:

(a) the date on which and the place where the biometric data were acquired;

(b) the criminal offence for which the biometric data were acquired;

(c) the criminal case number;

(d) the competent authority responsible for the criminal case.

The return of core data by the requested Member State shall be subject to the decision of a human.

7. Europol's use of information obtained from a query made in accordance with this Article, and from the exchange of a set of core data in accordance with paragraph 6, shall be subject to the consent of the Member State in whose database the match occurred. Where the Member State allows such information to be used, its handling by Europol shall be governed by Regulation (EU) 2016/794.

*CHAPTER 6*

***Data protection***

*Article 50*

**Purpose of the data processing**

1. Processing of personal data received by a Member State or Europol shall be permitted solely for the purposes for which the data were supplied by the Member State which provided the data in accordance with this Regulation. Processing for other purposes shall be permitted solely with the prior authorisation of the Member State which provided the data.

2. Processing of data supplied by a Member State or Europol pursuant to Article 6, 11, 16, 20 or 26 shall be permitted solely where necessary for the purpose of:

(a) establishing whether the compared DNA profiles, dactyloscopic data, vehicle registration data, facial images or police records match;

(b) exchanging a set of core data in accordance with Article 47;

(c) preparing and submitting a police or judicial request for legal assistance where those data match;

(d) keeping logs as provided for in Articles 18, 40 and 45.

3. The data received by a Member State or Europol shall be deleted immediately following automated replies to searches unless further processing is necessary for the purposes referred to in paragraph 2 or is authorised in accordance with paragraph 1.

4. Prior to connecting their national databases to the router or EPRIS, Member States shall conduct a data protection impact assessment as referred to in Article 27 of Directive (EU) 2016/680 and, where appropriate, consult the supervisory authority as provided for in Article 28 of that Directive. The supervisory authority may use any of the powers it has under Article 47 of that Directive, in accordance with Article 28(5) of that Directive.

*Article 51*

**Accuracy, relevance and data retention**

1. Member States and Europol shall ensure the accuracy and relevance of personal data which are processed pursuant to this Regulation. Where a Member State or Europol become aware that data which are incorrect or no longer up to date or data which should not have been supplied have been supplied, it shall notify the Member State which received the data or Europol of that fact without undue delay. All Member States concerned or Europol shall correct or delete the data accordingly without undue delay. Where the Member State which received the data or Europol has reason to believe that the data supplied are incorrect or should be deleted, it shall inform the Member State which provided the data without undue delay.

2. Member States and Europol shall put in place appropriate measures for updating data relevant for the purposes of this Regulation.

3. Where a data subject contests the accuracy of data in the possession of a Member State or Europol, where the accuracy cannot be reliably established by the Member State concerned or Europol and where requested by the data subject, the data concerned shall be marked with a flag. Where such a flag exists, Member States or Europol may remove it only with the permission of the data subject or based on a decision of the competent court, of the supervisory authority or of the European Data Protection Supervisor, as relevant.

4. Data which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) where they are not or no longer necessary for the purpose for which they were supplied;

(b) upon the expiry of the maximum period for keeping data laid down by the national law of the Member State which provided the data where that Member State informed the Member State which received the data or Europol of that maximum period at the time of supplying the data; or

(c) upon the expiry of the maximum period for keeping data laid down in Regulation (EU) 2016/794.

Where there is reason to believe that the deletion of data would prejudice the interests of the data subject, the processing of those data shall be restricted instead of being deleted. Where the processing of data has been restricted, they shall be processed solely for the purpose which prevented their deletion.

*Article 52*

**Data processor**

1. eu-LISA shall be the processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the processing of personal data via the router.

2. Europol shall be the processor within the meaning of Article 3, point (12), of Regulation (EU) 2018/1725 for the processing of personal data via EPRIS.

*Article 53*

**Security of processing**

1. The Member States' competent authorities, eu-LISA and Europol shall ensure the security of the processing of personal data under this Regulation. The Member States' competent authorities, eu-LISA and Europol shall cooperate on security-related tasks.

2. Without prejudice to Article 33 of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/794, eu-LISA and Europol shall take the necessary measures to ensure the security of the router and EPRIS, respectively, and of their related communication infrastructure.

3. eu-LISA shall adopt the necessary measures concerning the router, and Europol shall adopt the necessary measures concerning EPRIS, in order to:

(a) physically protect data, including by making contingency plans for the protection of critical infrastructure;

(b) deny unauthorised persons access to data-processing equipment and installations;

(c) prevent the unauthorised reading, copying, modification or removal of data media;

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of recorded personal data;

(e) prevent the unauthorised processing of data and any unauthorised copying, modification or deletion of data;

(f) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment;

(g) ensure, by means of individual user identities and confidential access modes only, that persons authorised to access the router or EPRIS, as applicable, have access only to the data covered by their access authorisation;

(h) ensure that it is possible to verify and establish to which bodies personal data can be supplied using data communication equipment;

(i) ensure that it is possible to verify and establish which data have been processed in the router or EPRIS, as applicable, and when, by whom and for what purpose they have been processed;

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the router or EPRIS, as applicable, or during the transport of data media, in particular by means of appropriate encryption techniques;

(k) ensure that, in the event of interruption, installed systems can be restored to normal operation;

(l) ensure reliability by making sure that any faults in the functioning of the router or EPRIS, as applicable, are properly reported;

(m) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation and to assess those security measures in the light of new technological developments.

The necessary measures referred to in the first subparagraph shall include a security plan, a business continuity plan and a disaster recovery plan.

*Article 54*

**Security incidents**

1. Any event that has or may have an impact on the security of the router or EPRIS and may cause damage to or loss of data stored in the router or EPRIS shall be considered to be a security incident, in particular where unauthorised access to data may have occurred or where the availability, integrity and confidentiality of data has or may have been compromised.

2. In the event of a security incident concerning the router, eu-LISA and the Member States concerned or, where applicable, Europol shall cooperate with one another in order to ensure a swift, effective and proper response.

3. In the event of a security incident concerning EPRIS, the Member States concerned and Europol shall cooperate with one another in order to ensure a swift, effective and proper response.

4. Member States shall notify their competent authorities of any security incidents without undue delay.

Without prejudice to Article 92 of Regulation (EU) 2018/1725, in the event of a security incident in relation to the central infrastructure of the router, eu-LISA shall notify the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and, in any event, no later than 24 hours after becoming aware of them. Actionable and appropriate technical details of cyber threats, vulnerabilities and incidents that enable proactive detection, incident response or mitigating measures shall be disclosed to CERT-EU without undue delay.

Without prejudice to Article 34 of Regulation (EU) 2016/794 and Article 92 of Regulation (EU) 2018/1725, in the event of a security incident in relation to the EPRIS central infrastructure, Europol shall notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and, in any event, no later than 24 hours after becoming aware of them. Actionable and appropriate technical details of cyber threats, vulnerabilities and incidents that enable proactive detection, incident response or mitigating measures shall be disclosed to CERT-EU without undue delay.

5. Information regarding a security incident that has or may have an impact on the operation of the router or on the availability, integrity and confidentiality of the data shall be provided by the Member States and Union agencies concerned to the Member States and Europol without delay and reported in compliance with the incident management plan to be provided by eu-LISA.

6. Information regarding a security incident that has or may have an impact on the operation of EPRIS or on the availability, integrity and confidentiality of the data shall be provided by the Member States and Union agencies concerned to the Member States without delay and reported in compliance with the incident management plan to be provided by Europol.

*Article 55*

**Self-monitoring**

1. Member States shall ensure that each authority entitled to use the Prüm II framework takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority. Europol shall take the measures necessary to monitor its compliance with this Regulation and shall cooperate, where necessary, with the European Data Protection Supervisor.

2. Data controllers shall implement the necessary measures to effectively monitor the compliance of data processing with this Regulation, including by frequently verifying the logs referred to in Articles 18, 40 and 45. They shall cooperate, where necessary and as appropriate, with the supervisory authorities or with the European Data Protection Supervisor.

*Article 56*

**Penalties**

Member States shall ensure that any misuse of data, processing of data or exchange of data contrary to this Regulation is punishable in accordance with national law. The penalties provided shall be effective, proportionate and dissuasive.

*Article 57*

**Liability**

If any failure of a Member State or, when performing queries in accordance with Article 49, Europol to comply with its obligations under this Regulation causes damage to the router or EPRIS, that Member State or Europol shall be liable for such damage, unless and in so far as eu-LISA, Europol or another Member State bound by this Regulation failed to take reasonable measures to prevent the damage from occurring or to minimise its impact.

*Article 58*

**Audits by the European Data Protection Supervisor**

1. The European Data Protection Supervisor shall ensure that an audit of personal data processing operations by eu-LISA and Europol for the purposes of this Regulation is carried out in accordance with relevant international auditing standards at least every four years. A report of that audit shall be sent to the European Parliament, to the Council, to the Commission, to the Member States and to the Union agency concerned. eu-LISA and Europol shall be given an opportunity to make comments before the reports are adopted.

2. eu-LISA and Europol shall supply information requested by the European Data Protection Supervisor to it, grant the European Data Protection Supervisor access to all the documents it requests and to their logs referred to in Articles 40 and 45 and allow the European Data Protection Supervisor access to all their premises at any time. This paragraph is without prejudice to the powers of the European Data Protection Supervisor under Article 58 of Regulation (EU) 2018/1725 and, with regard to Europol, under Article 43(3) of Regulation (EU) 2016/794.

*Article 59*

**Cooperation between supervisory authorities and the European Data Protection Supervisor**

1. The supervisory authorities and the European Data Protection Supervisor shall, each acting within the scope of their respective competences, cooperate actively within the framework of their respective responsibilities to ensure a coordinated supervision of the application of this Regulation, in particular if the European Data Protection Supervisor or a supervisory authority finds major discrepancies between practices of Member States or finds potentially unlawful transfers using the communication channels of the Prüm II framework.

2. In the cases referred to in paragraph 1 of this Article, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725.

3. Two years after the start of operations of the router and EPRIS and every two years thereafter, the European Data Protection Board shall send a report of its activities under this Article to the European Parliament, to the Council, to the Commission, to eu-LISA and to Europol. That report shall include a chapter on each Member State prepared by the supervisory authority of the Member State concerned.

*Article 60*

**Transfer of personal data to third countries and international organisations**

A Member State shall only transfer personal data obtained under this Regulation to a third country or an international organisation in accordance with Chapter V of Directive (EU) 2016/680 and where the requested Member State has granted its authorisation prior to the transfer.

Europol shall only transfer personal data obtained under this Regulation to a third country or an international organisation where the conditions laid down in Article 25 of Regulation (EU) 2016/794 have been fulfilled and where the requested Member State has granted its authorisation prior to the transfer.

*Article 61*

**Relation to other legal acts on data protection**

Any processing of personal data for the purposes of this Regulation shall be carried out in accordance with this Chapter and with Directive (EU) 2016/680 or Regulation (EU) 2018/1725, (EU) No 2016/794 or (EU) 2016/679, as applicable.

*CHAPTER 7*

***Responsibilities***

*Article 62*

**Responsibility of due diligence**

Member States and Europol shall exercise due diligence in assessing whether the automated exchange of data falls under the purpose of the Prüm II framework set out in Article 2 and whether it complies with the conditions set out therein, in particular with regard to respect for fundamental rights.

*Article 63*

**Training**

Authorised staff of Member States' competent authorities, of supervisory authorities and of Europol shall be provided, as relevant, with adequate resources and training, including on data protection and the accurate review of matches, to perform the tasks under this Regulation.

*Article 64*

**Responsibilities of the Member States**

1. Each Member State shall be responsible for:

(a) the connection to the infrastructure of the router;

(b) the integration of its existing national systems and infrastructure with the router;

(c) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to the router;

(d) the connection to the infrastructure of EPRIS;

(e) the integration of its existing national systems and infrastructure with EPRIS;

(f) the organisation, management, operation and maintenance of its existing national infrastructure and of its connection to EPRIS;

(g) the management of, and arrangements for, access by the duly authorised staff of its competent authorities to the router in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

(h) the management of, and arrangements for, access by the duly authorised staff of its competent authorities to EPRIS in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

(i) the management of, and arrangements for, access by the duly authorised staff of its competent authorities to Eucaris in accordance with this Regulation and the creation and regular update of a list of those staff and their profiles;

(j) the manual confirmation by qualified staff of a match as referred to in Article 6(6), Article 6(7), Article 11(2) and Article 20(2);

(k) ensuring the availability of the data necessary for the exchange of data in accordance with Articles 5, 10, 16, 19 and 25;

(l) the exchange of information in accordance with Articles 6, 11, 16, 20 and 26;

(m) correcting, updating or deleting any data received from a requested Member State within 48 hours of the notification from the requested Member State that the data submitted were incorrect, are no longer up to date or were unlawfully transmitted;

(n) compliance with the data quality requirements set out in this Regulation.

2. Each Member State shall be responsible for connecting its competent authorities to the router, EPRIS and Eucaris.

*Article 65*

**Responsibilities of Europol**

1. Europol shall be responsible for the management of, and arrangements for the access by its duly authorised staff to, the router, EPRIS and Eucaris in accordance with this Regulation.

2. Europol shall be responsible for processing the queries of Europol data by the router. Europol shall adapt its information systems accordingly.

3. Europol shall be responsible for any technical adaptations in Europol infrastructure required for establishing the connection to the router and to Eucaris.

4. Without prejudice to searches by Europol pursuant to Article 49, Europol shall not have access to any of the personal data processed through EPRIS.

5. Europol shall be responsible for the development of EPRIS in cooperation with the Member States. EPRIS shall provide the functionalities laid down in Articles 42 to 46.

Europol shall be responsible for the technical management of EPRIS. Technical management of EPRIS shall consist of all the tasks and technical solutions necessary to keep the EPRIS central infrastructure functioning and providing uninterrupted services to Member States 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that EPRIS functions are at a satisfactory level of technical quality, in particular as regards the response time for submitting requests to the national databases in accordance with the technical specifications.

6. Europol shall provide training on the technical use of EPRIS.

7. Europol shall be responsible for the procedures provided for in Articles 48 and 49.

*Article 66*

**Responsibilities of eu-LISA during the design and development phase of the router**

1. eu-LISA shall ensure that the central infrastructure of the router is operated in accordance with this Regulation.

2. The router shall be hosted by eu-LISA in its technical sites and shall provide the functionalities laid down in this Regulation in accordance with the conditions of security, availability, quality and performance referred to in Article 67(1).

3. eu-LISA shall be responsible for the development of the router and for any technical adaptations necessary for the operations of the router.

4. eu-LISA shall not have access to any of the personal data processed through the router.

5. eu-LISA shall determine the design of the physical architecture of the router, including its secure communication infrastructure and the technical specifications, and its evolution as regards the central infrastructure and the secure communication infrastructure. eu-LISA's Management Board shall approve the design, subject to a favourable opinion of the Commission. eu-LISA shall also implement any necessary adaptations to the interoperability components deriving from the establishment of the router as provided for by this Regulation.

6. eu-LISA shall develop and implement the router as soon as possible after the adoption by the Commission of the measures provided for in Article 37(6). That development shall consist of the elaboration and implementation of the technical specifications, testing and overall project management and coordination.

7. During the design and development phase, the Programme Management Board referred to in Article 54 of Regulation (EU) 2019/817 and in Article 54 of Regulation (EU) 2019/818 shall meet regularly. It shall ensure the adequate management of the design and development phase of the router.

Every month, the Programme Management Board shall submit written reports on the progress of the project to eu-LISA's Management Board. The Programme Management Board shall not have decision-making powers or any mandate to represent the members of eu-LISA's Management Board.

The Interoperability Advisory Group referred to in Article 78 shall meet regularly until the start of operations of the router. It shall report after each meeting to the Programme Management Board. It shall provide technical expertise to support the tasks of the Programme Management Board and shall follow up on the state of preparation of the Member States.

*Article 67*

**Responsibilities of eu-LISA following the start of operations of the router**

1. Following the start of operations of the router, eu-LISA shall be responsible for the technical management of the central infrastructure of the router, including its maintenance and technological developments. In cooperation with Member States, it shall ensure that the best available technology is used, subject to a cost-benefit analysis. eu-LISA shall also be responsible for the technical management of the necessary communication infrastructure.

Technical management of the router shall consist of all the tasks and technical solutions necessary to keep the router functioning and providing uninterrupted services to Member States and to Europol 24 hours a day, 7 days a week in accordance with this Regulation. It shall include the maintenance work and technical developments necessary to ensure that the router functions at a satisfactory level of technical quality, in particular as regards availability and the response time for submitting requests to the national databases and Europol data in accordance with the technical specifications.

The router shall be developed and managed in such a way as to ensure swift, efficient and controlled access, full and uninterrupted availability, and a response time in line with the operational needs of the Member States' competent authorities and Europol.

2. Without prejudice to Article 17 of the Staff Regulations of Officials of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([18]), eu-LISA shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to its staff required to work with data stored in the router. That obligation shall also apply after such staff leave office or employment or after the termination of their activities.

eu-LISA shall not have access to any of the personal data processed through the router.

3. eu-LISA shall perform tasks related to the provision of training on the technical use of the router.

*CHAPTER 8*

***Amendments to other existing instruments***

*Article 68*

**Amendments to Decisions 2008/615/JHA and 2008/616/JHA**

1. In Decision 2008/615/JHA, Article 1, point (a), Articles 2 to 6 and Sections 2 and 3 of Chapter 2 are replaced with regard to the Member States bound by this Regulation from the date of application of the provisions of this Regulation related to the router set out in Article 75(1). Therefore, Article 1, point (a), Articles 2 to 6 and Sections 2 and 3 of Chapter 2 of Decision 2008/615/JHA are deleted from the date of application of the provisions of this Regulation related to the router set out in Article 75(1).

2. In Decision 2008/616/JHA, Chapters 2 to 5 and Articles 18, 20 and 21 are replaced with regard to the Member States bound by this Regulation from the date of application of the provisions of this Regulation related to the router set out in Article 75(1). Therefore, Chapters 2 to 5 and Articles 18, 20 and 21 of Decision 2008/616/JHA are deleted from the date of application of the provisions of this Regulation related to the router set out in Article 75(1).

*Article 69*

**Amendments to Regulation (EU) 2018/1726**

Regulation (EU) 2018/1726 is amended as follows:

(1) the following article is inserted:

'*Article 8d*

**Tasks related to the Prüm II router**

([18]) OJ L 56, 4.3.1968, p. 1.

In relation to the Prüm II router, the Agency shall perform the tasks conferred on it by Regulation (EU) 2024/982 of the European Parliament and of the Council (*).

_____

(*) Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) (OJ L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj).';

(2) in Article 17(3), the second subparagraph is replaced by the following:

'The tasks relating to development and operational management referred to in Article 1(4) and (5), Articles 3 to 8 and Articles 8d, 9 and 11 shall be carried out at the technical site in Strasbourg, France.';

(3) Article 19(1) is amended as follows:

(a) the following point is inserted:

'(eeb) adopt reports on the state of play of the development of the Prüm II router pursuant to Article 80(2) of Regulation (EU) 2024/982;';

(b) point (ff) is replaced by the following:

'(ff) adopt reports on the technical functioning of the following:

(i) SIS pursuant to Article 60(7) of Regulation (EU) 2018/1861 of the European Parliament and of the Council (*) and Article 74(8) of Regulation (EU) 2018/1862 of the European Parliament and of the Council (**);

(ii) VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA;

(iii) the EES pursuant to Article 72(4) of Regulation (EU) 2017/2226;

(iv) ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240;

(v) ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816;

(vi) the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818;

(vii) the e-CODEX system pursuant to Article 16(1) of Regulation (EU) 2022/850;

(viii) the JITs collaboration platform pursuant to Article 26(6) of Regulation (EU) 2023/969;

(ix) the Prüm II router pursuant to Article 80(5) of Regulation (EU) 2024/982;

_____

(*) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

(**) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).';

(c) point (hh) is replaced by the following:

'(hh) adopt formal comments on the European Data Protection Supervisor's reports on its audits pursuant to Article 56(2) of Regulation (EU) 2018/1861, Article 42(2) of Regulation (EC) No 767/2008, Article 31(2) of Regulation (EU) No 603/2013, Article 56(2) of Regulation (EU) 2017/2226, Article 67 of Regulation (EU) 2018/1240, Article 29(2) of Regulation (EU) 2019/816, Article 52 of Regulations (EU) 2019/817 and (EU) No 2019/818 and Article 58(1) of Regulation (EU) 2024/982 and ensure appropriate follow-up of those audits;'.

*Article 70*

**Amendment to Regulation (EU) 2019/817**

In Article 6(2) of Regulation (EU) 2019/817 the following point is added:

'(d) a secure communication infrastructure between the ESP and the router established by Regulation (EU) 2024/982 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) (OJ L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj).'.

*Article 71*

**Amendments to Regulation (EU) 2019/818**

Regulation (EU) 2019/818 is amended as follows:

(1) in Article 6(2), the following point is added:

'(d) a secure communication infrastructure between the ESP and the router established by Regulation (EU) 2024/982 of the European Parliament and of the Council (*).

(*) Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) (OJ L, 2024/982, 5.4.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj).';

(2) in Article 39, paragraphs 1 and 2 are replaced by the following:

'1. A central repository for reporting and statistics (CRRS) is established for the purposes of supporting the objectives of the SIS, Eurodac and ECRIS-TCN, in accordance with the respective legal instruments governing those systems, and to provide cross-system statistical data and analytical reporting for policy, operational and data quality purposes. The CRRS shall also support the objectives of Regulation (EU) 2024/982.

2. eu-LISA shall establish, implement and host in its technical sites the CRRS containing the data and statistics referred to in Article 74 of Regulation (EU) 2018/1862 and Article 32 of Regulation (EU) 2019/816 logically separated by EU information system. eu-LISA shall also collect the data and statistics from the router referred to in Article 72(1) of Regulation (EU) 2024/982. Access to the CRRS shall be granted by means of controlled, secured access and specific user profiles, solely for the purpose of reporting and statistics, to the authorities referred to in Article 74 of Regulation (EU) 2018/1862, Article 32 of Regulation (EU) 2019/816 and Article 72(1) of Regulation (EU) 2024/982'.

*CHAPTER 9*

***Final provisions***

*Article 72*

**Reporting and statistics**

1. Where needed, the duly authorised staff of the Member States' competent authorities, the Commission, eu-LISA and Europol shall have access to the following data related to the router, solely for the purposes of reporting and statistics:

(a) the number of queries per Member State and the number of queries by Europol per category of data;

(b) the number of queries to each of the connected databases;

(c) the number of matches against each Member State's database per category of data;

(d) the number of matches against Europol data per category of data;

(e) the number of confirmed matches where there were exchanges of core data;

(f) the number of confirmed matches where there were no exchanges of core data;

(g) the number of queries to the Common Identity Repository via the router; and

(h) the number of matches per type as follows:

(i) identified data (person) – unidentified data (trace);

(ii) unidentified data (trace) – identified data (person);

(iii) unidentified data (trace) – unidentified data (trace);

(iv) identified data (person) – identified data (person).

It shall not be possible to identify individuals from the data set out in the first subparagraph.

2. The duly authorised staff of the Member States' competent authorities, the Commission and Europol shall have access to the following data related to Eucaris, solely for the purposes of reporting and statistics:

(a) the number of queries per Member State and the number of queries by Europol;

(b) the number of queries to each of the connected databases; and

(c) the number of matches against each Member State's database.

It shall not be possible to identify individuals from the data set out in the first subparagraph.

3. The duly authorised staff of the Member States' competent authorities, the Commission and Europol shall have access to the following data related to EPRIS, solely for the purposes of reporting and statistics:

(a) the number of queries per Member State and the number of queries by Europol;

(b) the number of queries to each of the connected indexes; and

(c) the number of matches against each Member State's database.

It shall not be possible to identify individuals from the data set out in the first subparagraph.

4. eu-LISA shall store the data set out in paragraph 1 of this Article in the central repository for reporting and statistics established by Article 39 of Regulation (EU) 2019/818. Europol shall store the data set out in paragraph 3. Those data shall allow the Member States' competent authorities, the Commission, eu-LISA and Europol to obtain customisable reports and statistics to enhance the efficiency of law enforcement cooperation.

*Article 73*

**Costs**

1. Costs incurred in connection with the establishment and operation of the router and EPRIS shall be borne by the general budget of the Union.

2. Costs incurred in connection with the integration of existing national infrastructure and its connection to the router and EPRIS and costs incurred in connection with the establishment of national facial image databases and national police record indexes for the prevention, detection and investigation of criminal offences shall be borne by the general budget of the Union.

The following costs shall be excluded:

(a) Member States' project management office (meetings, missions, offices);

(b) hosting of national IT systems (space, implementation, electricity, cooling);

(c) operation of national IT systems (operators and support contracts);

(d) design, development, implementation, operation and maintenance of national communication networks.

3. Each Member State shall bear the costs arising from the administration, use and maintenance of Eucaris.

4. Each Member State shall bear the costs arising from the administration, use and maintenance of their connections to the router and EPRIS.

*Article 74*

**Notifications**

1. Member States shall notify eu-LISA of the competent authorities referred to in Article 36. Those authorities may use or have access to the router.

2. eu-LISA shall notify the Commission of the successful completion of the test referred to in Article 75(1), point (b).

3. Europol shall notify the Commission of the successful completion of the test referred to in Article 75(3), point (b).

4. Each Member State shall notify the other Member States, the Commission, eu-LISA and Europol of the content of its national DNA databases and the conditions for automated searches to which Articles 5 and 6 apply.

5. Each Member State shall inform the other Member States, the Commission, eu-LISA and Europol of the content of its national dactyloscopic databases and the conditions for automated searches to which Articles 10 and 11 apply.

6. Each Member State shall inform the other Member States, the Commission, eu-LISA and Europol of the content of its national facial image databases and the conditions for automated searches to which Articles 19 and 20 apply.

7. Member States participating in automated exchanges of police records pursuant to Articles 25 and 26 shall notify the other Member States, the Commission and Europol of the content of their national police record indexes and of the national databases used for the establishment of those indexes and the conditions for automated searches.

8. Member States shall notify the Commission, eu-LISA and Europol of their national contact point designated pursuant to Article 30. The Commission shall compile a list of the national contact points notified to it and make it available to all Member States.

*Article 75*

**Start of operations**

1. The Commission shall determine the date from which the Member States and Europol can start using the router by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Article 5(3), Article 8(2) and (3), Article 13(2) and (3), Article 17(3), Article 22(2) and (3), Article 31 and Article 37(6) have been adopted;

(b) eu-LISA has declared the successful completion of a comprehensive test of the router, which it has conducted in cooperation with the Member States' competent authorities and Europol.

The Commission shall determine, by means of the implementing act referred to in the first subparagraph, the date from which the Member States and Europol are to start using the router. That date shall be one year after the date determined in accordance with the first subparagraph.

The Commission may postpone the date from which the Member States and Europol are to start using the router by one year at most where an assessment of the implementation of the router has shown that such a postponement is necessary.

2. Member States shall ensure, two years after the start of operations of the router, the availability of facial images as referred to in Article 19 for the purposes of automated searching of facial images as referred to in Article 20.

3. The Commission shall determine the date from which the Member States and Europol are to start using EPRIS by means of an implementing act once the following conditions have been met:

(a) the measures referred to in Article 44(6) have been adopted;

(b) Europol has declared the successful completion of a comprehensive test of EPRIS, which it has conducted in cooperation with the Member States' competent authorities.

4. The Commission shall determine the date from which Europol is to make available third country-sourced biometric data to Member States in accordance with Article 48 by means of an implementing act once the following conditions have been met:

(a) the router is in operation;

(b) Europol has declared the successful completion of a comprehensive test of its connection to the router, which it has conducted in cooperation with the Member States' competent authorities and eu-LISA.

5. The Commission shall determine the date from which Europol is to have access to data stored in Member States' databases in accordance with Article 49 by means of an implementing act once the following conditions have been met:

(a) the router is in operation;

(b) Europol has declared the successful completion of a comprehensive test of its connection to the router, which it has conducted in cooperation with the Member States' competent authorities and eu-LISA.

6. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure referred to in Article 77(2).

*Article 76*

**Transitional provisions and derogations**

1. Member States and the Union agencies shall start applying Articles 19 to 22, Article 47 and Article 49(6) from the date determined in accordance with Article 75(1), first subparagraph, with the exception of Member States which have not started using the router.

2. Member States and the Union agencies shall start applying Articles 25 to 28 and Article 49(4) from the date determined in accordance with Article 75(3).

3. Member States and the Union agencies shall start applying Article 48 from the date determined in accordance with Article 75(4).

4. Member States and the Union agencies shall start applying Article 49(1), (2), (3), (5) and (7) from the date determined in accordance with Article 75(5).

*Article 77*

**Committee procedure**

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), the third subparagraph, of Regulation (EU) No 182/2011 shall apply.

*Article 78*

**Interoperability Advisory group**

The responsibilities of the Interoperability Advisory Group, established by Article 75 of Regulation (EU) 2019/817 and Article 71 of Regulation (EU) 2019/818, shall be extended to cover the router. That Interoperability Advisory Group shall provide eu-LISA with expertise related to the router, in particular in the context of the preparation of its annual work programme and its annual activity report.

*Article 79*

**Practical handbook**

The Commission shall, in close cooperation with the Member States, eu-LISA, Europol and the European Union Agency for Fundamental Rights, make available a practical handbook for the implementation and management of this Regulation. The practical handbook shall provide technical and operational guidelines, recommendations and best practices. The Commission shall adopt the practical handbook in the form of a recommendation before the start of operations of both the router and EPRIS. The Commission shall update the practical handbook regularly and where necessary.

*Article 80*

**Monitoring and evaluation**

1. eu-LISA shall ensure that procedures are in place to monitor the development of the router in light of objectives relating to planning and costs and to monitor its functioning in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

Europol shall ensure that procedures are in place to monitor the development of EPRIS in light of objectives relating to planning and costs and to monitor its functioning in light of objectives relating to the technical output, cost-effectiveness, security and quality of service.

2. By 26 April 2025 and every year thereafter during the development phase of the router, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the development of the router. Those reports shall contain detailed information about the costs incurred and information as to any risks which could impact the overall costs to be borne by the general budget of the Union pursuant to Article 73.

Once the development of the router is finalised, eu-LISA shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved and justifying any divergences.

3. By 26 April 2025 and every year thereafter during the development phase of EPRIS, Europol shall submit a report to the European Parliament and to the Council on the state of play of the development of EPRIS. Those reports shall contain detailed information about the costs incurred and information as to any risks which could impact the overall costs to be borne by the general budget of the Union pursuant to Article 73.

Once the development of EPRIS is finalised, Europol shall submit a report to the European Parliament and to the Council explaining in detail how the objectives, in particular relating to planning and costs, were achieved and justifying any divergences.

4. For the purposes of technical maintenance, eu-LISA shall have access to the necessary information relating to the data processing operations performed in the router. For the purposes of technical maintenance, Europol shall have access to the necessary information relating to the data processing operations performed in EPRIS.

5. Two years after the start of operations of the router and every two years thereafter, eu-LISA shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning, including the security, of the router.

6. Two years after the start of operations of EPRIS and every two years thereafter, Europol shall submit to the European Parliament, to the Council and to the Commission a report on the technical functioning, including the security, of EPRIS.

7. Three years after the start of operations of the router and EPRIS as referred to in Article 75 and every four years thereafter, the Commission shall produce a report on the overall evaluation of the Prüm II framework.

One year after the start of operations of the router and every two years thereafter, the Commission shall produce a report evaluating the use of facial images under this Regulation.

The reports referred to in the first and second subparagraphs shall include the following:

(a) an assessment of the application of this Regulation, including its use by each Member State and Europol;

(b) an examination of the results achieved against the objectives of this Regulation and its impact on fundamental rights;

(c) the impact, effectiveness and efficiency of the performance of the Prüm II framework and its working practices in light of its objectives, mandate and tasks;

(d) an assessment of the security of the Prüm II framework.

The Commission shall transmit those reports to the European Parliament, to the Council, to the European Data Protection Supervisor and to the European Union Agency for Fundamental Rights.

8. In the reports referred to in the first subparagraph of paragraph 7, the Commission shall pay special attention to the following new categories of data: facial images and police records. The Commission shall include in such reports the use made by each Member State and Europol of those new categories of data and their impact, effectiveness and efficiency. In the reports referred to in the second subparagraph of paragraph 7, the Commission shall pay special attention to the risk of false matches and to data quality.

9. The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the reports referred to in paragraphs 2 and 5. That information shall not jeopardise working methods or reveal the sources, staff members or investigations of the Member States' competent authorities.

10. The Member States shall provide the Commission and Europol with the information necessary to draft the reports referred to in paragraphs 3 and 6. That information shall not jeopardise working methods or reveals the sources, staff members or investigations of the Member States' competent authorities.

11. Without prejudice to confidentiality requirements, Member States, eu-LISA and Europol shall provide the Commission with the information necessary to produce the reports referred to in paragraph 7. Member States shall also provide the Commission with the number of confirmed matches against each Member State's database per category and per type of data. That information shall not jeopardise working methods or reveal the sources, staff members or investigations of the Member States' competent authorities.

*Article 81*

**Entry into force and applicability**

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 13 March 2024.

| *For the European Parliament* | *For the Council* |
|---|---|
| *The President* | *The President* |
| R. METSOLA | H. LAHBIB |