Council of the European Union

Brussels, 16 June 2022
(OR. en)

10350/22

Interinstitutional File: 2021/0410(COD)

IXIM 168
ENFOPOL 356
JAI 910
CODEC 940

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	9544/22
No. Cion doc.:	14204/21
Subject:	Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council – General approach

At its meeting on 10 June 2022, the Council reached a general approach on the proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

ANNEXE

2021/0410 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council

THE 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 82(1), point (d),*** 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],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

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 should be achieved by means of, among others, appropriate measures to prevent and combat crime, including organised crime and terrorism.

---

1 OJ C , , p. .
2 OJ C , , p. .

(2) That objective requires that law enforcement authorities exchange data, in an efficient and timely manner, in order to effectively fight crime.

(3) The objective of this Regulation is therefore to improve, streamline and facilitate the exchange of criminal information between Member States' law enforcement authorities, but also with the European Union Agency for Law Enforcement Cooperation established by Regulation (EU) No 2016/794 of the European Parliament and of the Council[3] (Europol) as the Union criminal information hub.

(4) Council Decisions 2008/615/JHA[4] and 2008/616/JHA[5] laying 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.

(5) ***Building upon existing procedures for the automated search of data,*** ~~T~~*t*his Regulation should lay down the conditions and procedures for the automated transfer of DNA profiles, dactyloscopic data, vehicle registration data, ***driving licence data,*** facial images and police records. This should be without prejudice to the processing of any of these data in the Schengen Information System (SIS) or the exchange of supplementary information related to them via the SIRENE bureaux or to the rights of individuals whose data is processed therein.

---

[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).

(6) The processing of personal data and the 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.

(6a) Any processing or exchange of personal data should be subject to the provisions on data protection of Chapter VI of this Regulation and as applicable, Directive (EU) 2016/680 of the European Parliament and of the Council[5a] or Regulation (EU) 2018/1725 of the European Parliament and of the Council[5b].

(7) By providing for the automated search ~~or comparison~~ of DNA profiles, dactyloscopic data, vehicle registration data, ***driving licence data,*** facial images and police records, the purpose of this Regulation is also to allow for the search of missing persons and ***the identification of*** unidentified human remains. ***These automated searches should follow the same rules and procedures.*** This should be without prejudice to the entry of SIS alerts on missing persons and the exchange of supplementary information on such alerts under Regulation (EU) 2018/1862 of the European Parliament and of the Council.[6]

[5a] 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 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).

[5b] 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).

[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).

(7a) This Regulation lays down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data, facial images, police records, certain vehicle registration data and driving licence data (step one), and the rules regarding the exchange of core data following a confirmed match on biometric data (step two). It does not apply to the exchange of supplementary information beyond what is provided for in this Regulation (step three), which should be regulated by Directive (EU) …/… [on information exchange between law enforcement authorities of Member States].

(8) The Directive (EU) …/… [*on information exchange between law enforcement authorities of Member States*] provides a coherent Union legal framework to ensure that law enforcement authorities have equivalent access to information held by other Member States when they need it to fight crime and terrorism. To enhance information exchange, that Directive formalises and clarifies the procedures for information sharing between Member States, in particular for investigative purposes, including the role of the 'Single Point of Contact' for such exchanges~~, and making full use of Europol's information exchange channel SIENA. Any exchange of information beyond what is provided for in this Regulation should be regulated by Directive (EU) …/… [*on information exchange between law enforcement authorities of Member States*]~~.

(8a) For the automated searching of DNA profiles, Member States should, at the initial connection to the router, send all their DNA profiles for comparison to all other Member States and Europol. This initial automated search by comparing all DNA profiles held by a Member State should seek to avoid any gaps in matches between DNA profiles stored in a Member State's database and DNA profiles stored in all other Member States' databases and Europol. It should be done bilaterally and should not necessarily be performed with all Member States and Europol at the same time. The modalities, including the timing and the quantity by batch, should be agreed bilaterally. Once this initial automated search of all DNA profiles has been performed, Member States should have the possibility to repeat automated searches by comparing all DNA profiles at a later stage, to ensure that matches have not been missed since the initial automated search. The modalities of these new searches should be agreed bilaterally.

(8b) For the automated searching of DNA profiles, Member States should also send all their new DNA profiles added to their databases for comparison to all other Member States and Europol. This automated searching of new DNA profiles should take place regularly.

(9) For the automated searching of vehicle registration data ***and driving licence data***, Member States 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) designed for this purpose. Eucaris should connect all participating Member States in a network. There is no central component needed for the communication to be established as each Member State communicates directly to the other connected Member States.

(9a) For the automated searching of driving licence data, Member States should use the EU driving licence network (RESPER) set up by the Directive 2006/126/EC[6a] on driving licences.

(10) The identification of a criminal is essential for a successful criminal investigation and prosecution. The automated searching of facial images of suspects and convicted criminals should provide for additional information for successfully identifying criminals and fighting crime.

(11) The automated search ~~or comparison~~ of biometric data (DNA profiles, dactyloscopic data and facial images) between 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.

(12) Participation in the exchange of police records should remain voluntary. Where Member States decide to participate, in the spirit of reciprocity, it should not be possible for them to query other Member States' databases if they do not make their own data available for queries by other Member States. ***Participating Member States should establish indexes of national police record databases. They may decide which national databases established for the prevention, detection and investigation of criminal offences, they will use to create their national police records indexes. These indexes include data from national databases that the police normally checks when receiving information requests from other law enforcement authorities. The European Police Records Index System (EPRIS) is established in accordance with the privacy-by-design principle. Data protection safeguards include pseudonymisation, as indexes and queries do not contain clear personal data, but alphanumerical strings. EPRIS should inhibit Member States or Europol to reverse the pseudonymisation and reveal the personal data which resulted in the match.***

[6a] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (OJ L 403, 30.12.2006, p. 18).

(12a) As referred to in Annex II of Regulation (EU) 2016/794, a suspect may be understood as a person who, in accordance with the national law of the Member State concerned, is suspected of having committed or having taken part in a criminal offence, or a person regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that this person will commit criminal offences.

(12b) Exchange of police records does not concern criminal records, which can be subject of exchange of information through the existing ECRIS framework in accordance with Decision 2009/316/JHA[6b].

(13) In recent years, Europol has received a large amount of biometric data of suspected and convicted terrorists and criminals from several third countries. Including third country-sourced data stored at Europol in the Prüm framework and thus making this data available to law enforcement authorities ***of Member States*** is necessary for better prevention***, detection*** and investigation of criminal offences. It also contributes to building synergies between different law enforcement tools.

(14) ***For supporting Member States' action in preventing, detecting, and investigating criminal offences in accordance with Article 3 of Regulation (EU) 2016/794,*** Europol should be able to search Member States' databases under the Prüm framework with data received from third countries in order to establish cross-border links between criminal cases***, according to guidelines adopted by the Management Board of Europol***.

(14a) Being able to use Prüm data, next to other databases available to Europol, should allow establishing more complete and informed analysis on the criminal investigations and should allow Europol to provide better support to Member States' law enforcement authorities.

[6b] Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33).

(14b) 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 case of a match between data used for the search and data ~~held~~ ***stored*** in Member States' databases, Member States may ***decide whether to*** supply Europol with the information necessary for it to fulfil its tasks.

(14c) All provisions of Regulation (EU) 2016/794 apply to the participation of Europol in the Prüm 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 framework should be subject to the consent of the Member State which provided the data, and governed by Article 25 of Regulation (EU) 2016/794 if the data is transferred to third countries.

(15) 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 this technical architecture, each Member State should establish at least 26 connections, that means a connection with each Member State, per data category. The router and the European Police Records Index System (EPRIS) established by this Regulation should 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 and EPRIS should require a single connection per Member State in relation to police records.

(16) The router should be connected to the European Search Portal established by Article 6 of Regulation (EU) 2019/817 of the European Parliament and of the Council[7] and Article 6 of Regulation (EU) 2019/818 of the European Parliament and of the Council[8] to allow Member States' authorities and Europol to launch queries to national databases under this Regulation simultaneously to queries to the Common Identity Repository established by Article 17 of Regulation (EU) 2019/817 and Article 17 of Regulation (EU) 2019/818 for law enforcement purposes.

(16a) The reference numbers of biometric data (DNA profiles, dactyloscopic data and facial images) may be a provisional reference number or a transaction control number.

(16b) 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.

(16c) The router should rank, if decided by the requesting Member State and where applicable according to the type of biometric data, the replies from requested Member State(s) or Europol, by comparing the biometric data used for querying and the biometric data supplied in the answers by the requested Member State(s) or Europol.

---

7 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

8 Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

(17) In case of a match between the data used for the search ~~or comparison~~ and data held in the national database of the requested Member State(s), ~~and~~ upon confirmation of this match by the requesting Member State ***and upon transmission of a description of the facts and indication of the underlying offence using the common table of offences categories referred to in Annex A of Decision 2009/316/JHA***, the requested Member State should return a limited set of core data via the router within ***72*** ~~24~~ hours***, except if a judicial authorisation is required under national law***.

(17a) In the specific case of DNA, the requested Member State may also confirm a match between two DNA profiles, where relevant for the prevention, detection and investigation of criminal offences. Thereby, upon confirmation of this match by the requested Member State and upon transmission of a description of the facts and indication of the underlying offence using the common table of offences categories referred to in Annex A of Decision 2009/316/JHA, the requesting Member State should return a limited set of core data via the router within 72 hours, except if a judicial authorisation is required under national law.

(17b) The deadline would ensure fast communication exchange between Member States' authorities. Member States should retain control over the release of this limited set of core data. A certain degree of human intervention should be maintained at key points in the process, including for the decision to release personal data to the requesting Member State in order to ensure that there would be no automated exchange of core data.

(17c) Data lawfully supplied and received should not be deleted by Member States or Europol if they are used in an ongoing investigation.

~~(18) Any exchange between Member States' authorities or with Europol at any stage of one of the processes described under this Regulation, which is not explicitly described in this Regulation, should take place via SIENA to ensure that a common, secure and reliable channel of communication is used by all Member States.~~

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

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

(20a) Each Member State should notify other Member States, the Commission, Europol and eu-LISA of the content of their national databases made available via the Prüm II framework (data subjects) and the conditions for automated searches.

(21) 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 and the data elements to be exchanged. In order to ensure uniform conditions for the implementation of this Regulation 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.[9]

(21a) Data quality is of utmost importance as a safeguard. In the context of the automated searches of biometric data, and in order to ensure that the data transmitted are of sufficient quality, a minimum quality standard should be established to minimise adverse effects on uninvolved persons by reducing false positives.

[9] 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).

(22) As this Regulation provides for the establishment of the new Prüm framework, relevant provisions of Decisions 2008/615/JHA and 2008/616/JHA should be deleted. Those Decisions should therefore be amended accordingly.

(23) As the router should be developed and managed by the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice established by Regulation (EU) 2018/1726 of the European Parliament and of the Council[10] (eu-LISA), it is therefore necessary to amend Regulation (EU) 2018/1726 by adding that to the tasks of eu-LISA. In order to allow for the router to be connected to the European Search Portal to carry out simultaneous searches of the router and the Common Identity Repository it is therefore necessary to amend Regulation (EU) 2019/817. In order to allow for the router to be connected to the European Search Portal to carry out simultaneous searches of the router and the Common Identity Repository and in order to store reports and statistics of the router on the Common Repository for Reporting and Statistics it is therefore necessary to amend Regulation (EU) 2019/818. Those Regulations should therefore be amended accordingly.

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

[10] 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).

(25) ~~[~~In accordance with Article 3 of the 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 Treaty on European Union and the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation.~~] OR [In accordance with Articles 1 and 2 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 Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]~~

(26) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[11] and delivered an opinion on ***2 March 2022*** ~~[XX]~~[12].

HAVE ADOPTED THIS REGULATION:

~~11~~ ~~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).~~

12 [OJ C …].

CHAPTER 1

GENERAL PROVISIONS

Article 1

Subject matter

This Regulation establishes a framework for the exchange of information between authorities responsible for the prevention, detection and investigation of criminal offences (Prüm II).

This Regulation lays down the conditions and procedures for the automated searching of DNA profiles, dactyloscopic data, facial images, police records***,*** ~~and~~ certain vehicle registration data ***and driving licence data,*** and the rules regarding the exchange of core data following a ***confirmed*** match ***on biometric data***.

Article 2

Purpose

The purpose of Prüm II shall be to step up cross-border cooperation in matters covered by Part III, Title V, Chapter***s 4 and*** 5 of the Treaty on the Functioning of the European Union, ***facilitating*** ~~particularly~~ the exchange of information between authorities responsible for the prevention, detection and investigation of criminal offences.

The purpose of Prüm II shall also be to allow for the search ~~for~~ ***of*** missing persons and ***to facilitate the identification of*** unidentified human remains ***in accordance with Article 28a*** by authorities responsible for the prevention, detection and investigation of criminal offences.

Article 3

Scope

This Regulation applies to the ~~national~~ databases***, established in accordance with national law and*** used for the automated transfer of ***data of*** the categories of DNA profiles, dactyloscopic data, facial images, police records***,*** ~~and~~ certain vehicle registration data ***and driving licence data***.

Article 4

Definitions

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

(1) 'loci' ***(singular: 'locus')*** means ~~the particular molecular structure at the various~~ 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*** ~~identification characteristics of the non-coding part of an analysed human DNA sample~~, ***or*** the particular molecular structure at the various ***loci*** ~~DNA locations~~;

~~(3) 'non-coding part of DNA' means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism;~~

(4) 'DNA reference data' means DNA profile and the reference number referred to in Article 9;

(5) '~~reference~~ ***identified*** DNA profile' means the DNA profile of an identified person;

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

(7) ‘dactyloscopic data’ means fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database;

(8) ‘dactyloscopic reference data’ means dactyloscopic data and the reference number referred to in Article 14;

(8a) ‘identified dactyloscopic data’ means the dactyloscopic data of an identified person;

(8b) ‘unidentified dactyloscopic data’ means the dactyloscopic data collected during the investigation of criminal offences and belonging to a person not yet identified, including those obtained from traces;

(9) ‘individual case’ means a single investigation file;

(10) ‘facial image’ means digital image***s*** of the face;

(10a) ‘facial image~~s~~ reference data’ means the facial images and the reference number referred to in Article 23;

(10b) ‘identified facial image’ means the facial images of an identified person;

(10c) ‘unidentified facial image’ means the facial images collected during the investigation of criminal offences and belonging to a person not yet identified, including those obtained from traces;

(11) ‘biometric data’ means DNA profiles, dactyloscopic data or facial images;

(11a) ‘alphanumeric data’ means data represented by letters, digits, special characters, spaces and punctuation marks;

(12) ‘match’ means the existence of a correspondence as a result of an automated comparison between personal data recorded ~~or being recorded~~ in an information system or database;

(13) ‘candidate’ means data with which a match occurred;

(14) ‘requesting Member State’ means the Member State which is conducting a search through Prüm II;

(15) ‘requested Member State’ means the Member State in which databases the search is conducted through Prüm II by the requesting Member State;

(16) ‘police records’ means ***biographical data of suspects and convicted persons*** ~~any information~~ available in ~~the~~ national ***databases established*** ~~register or registers recording data of competent authorities,~~ for the prevention, detection and investigation of criminal offences;

(17) ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

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

(19) ‘supervisory authority’ means an independent public authority established by a Member State pursuant to Article 41 of Directive (EU) 2016/680 of the European Parliament and of the Council~~13~~;

~~13 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).~~

(20) ‘SIENA’ means the secure information exchange network application, managed ***and developed*** by Europol~~, aimed at facilitating the exchange of information between Member States and Europol~~;

(20a) ‘security incident’ means 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 them, 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.

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

(22) ‘significant cyber threat’ means a cyber threat with the intention, opportunity and capability to cause a significant incident;

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

(24) ‘incident’ means an incident within the meaning of Article 4(5) of Directive (EU) …/… of the European Parliament and of the Council[14] [*proposal NIS 2*].

[14] Directive (EU) …/… of the European Parliament and of the Council… (OJ..).

CHAPTER 2

EXCHANGE OF DATA

SECTION 1

DNA profiles

Article 5

***DNA reference data*~~Establishment of national DNA analysis files~~**

1. Member States shall open and keep national DNA ***database(s)*** ~~analysis files~~ for the ***prevention, detection and*** investigation of criminal offences.

Processing of ***DNA reference*** data ~~kept in those files, under this Regulation,~~ shall be carried out in accordance with this Regulation, in compliance with the national law of the Member States applicable to the processing of those data.

2. Member States shall ensure the availability of DNA reference data from their national ***database(s) established for the prevention, detection and investigation of criminal offences*** ~~DNA analysis files as referred to in paragraph 1~~.

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

4. DNA reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.

5. The Commission shall adopt an implementing act to specify the characteristics of a DNA profile which shall be exchanged. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 6

Automated searching of DNA profiles

1. ***For the prevention, detection and investigation of criminal offences, Member States shall, at the initial connection to the router via their national contact points, conduct an automated search by comparing all their DNA profiles, with all DNA profiles stored in all other Member States' databases and Europol. Member States and Europol shall agree bilaterally on the modalities of these automated searches.***

Member States may agree bilaterally to conduct automated searches also at a later stage by comparing DNA profiles, with all DNA profiles stored in all other Member States' databases and Europol. Member States and Europol shall agree bilaterally on the modalities of these automated searches.

2. For the prevention, detection and investigation of criminal offences, Member States shall***, via their*** ~~allow~~ national contact points***,*** ~~referred to in Article 29 and Europol access to the DNA reference data in their DNA analysis files, to~~ conduct automated searches by comparing ***all their new*** DNA profiles ***added to their DNA database, with all DNA profiles stored in all other Member States' databases and Europol*** ~~for the investigation of criminal offences~~.

Searches may be conducted only ~~in individual cases and~~ in compliance with the national law of the requesting Member State.

~~2~~ ***3***. Should an automated search show that a supplied DNA profile matches DNA profiles ~~entered~~ ***stored*** in the requested Member State's ~~searched file~~***database(s)***, the national contact point of the requesting Member State shall receive in an automated way the DNA reference data with which a match has been found.

If there is no match, the requesting Member State shall be notified about it in an automated manner.

~~3~~ ***4***. The national contact point of the requesting Member State ~~shall~~ ***may decide to*** confirm a match ~~of~~ ***between two*** DNA profiles ~~data~~***. If so decided, it shall inform the requested Member State and shall manually confirm this match*** with DNA reference data ***received from*** ~~held by~~ the requested Member State ~~following the automated supply of the DNA reference data required for confirming a match~~.

5. Where relevant for the prevention, detection and investigation of criminal offences, the national contact point of the requested Member State may also decide to confirm a match between two DNA profiles. If so decided, it shall inform the requesting Member State and shall manually confirm this match with DNA reference data received from the requesting Member State.

~~*Article 7*~~

~~**Automated comparison of unidentified DNA profiles**~~

~~1. Member States may, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA analysis files for the investigation of criminal offences. Profiles shall be supplied and compared in an automated manner.~~

~~2. Should a requested Member State, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA analysis files, it shall, without delay, supply the national contact point of the requesting Member State with the DNA reference data with which a match has been found.~~

~~3. The confirmation of a match of DNA profiles with DNA reference data held by the requested Member State shall be carried out by the national contact point of the requesting Member State following the automated supply of the DNA reference data required for confirming a match.~~

Article 8

***Notifications of*~~Reporting about~~ DNA *databases*~~analysis files~~**

Each Member State shall inform***, in accordance with Article 73, other Member States,*** the Commission***, Europol*** and eu-LISA of the ***content of*** national DNA ***databases*** ~~analysis files~~, to which Articles 5 ***and 6***~~to 7~~ apply, ***and the conditions for automated searches***~~, in accordance with Article 73~~.

Article 9

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 case of a match, to retrieve further data and other information in their databases referred to in Article 5 in order to supply it to one, several or all of the other Member States in accordance with Article~~s~~ 47 ~~and 48~~***, or to Europol in accordance with Article 50(6)***;

(a bis) a reference number allowing Europol, in case of a match, to retrieve further data and other information referred to in Article 49(1) in order to supply it to one, several or all of the other Member States in accordance with Articles 49(2);

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

(c) a code to indicate the type of DNA profile (~~reference~~ ***identified*** DNA profiles or unidentified DNA profiles).

Article 10

Principles ~~of DNA reference data~~*for the* exchange *of DNA profiles*

1. The digitalisation of DNA profiles and their transmission to the other Member States or Europol shall be carried out in accordance with European or international standards. The Commission shall adopt implementing acts to specify the relevant European or international standards for DNA profiles exchange that shall be used by Member States and Europol. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

2. Each Member State and Europol shall ensure that the DNA profiles it transmits are of sufficient quality for automated comparison. A minimum quality standard shall be established to allow for comparison of DNA profiles. The Commission shall adopt implementing acts to specify that minimum quality standard. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

3. Member States and Europol shall take appropriate measures to ensure the confidentiality and integrity of DNA profiles being sent to other Member States, including their encryption.

~~1. Appropriate measures shall be taken to ensure confidentiality and integrity for DNA reference data being sent to other Member States, including their encryption.~~

~~2. Member States shall take the necessary measures to guarantee the integrity of the DNA profiles made available or sent for comparison to the other Member States and to ensure that those measures comply with the relevant European or international standards for DNA data exchange.~~

~~3. The Commission shall adopt implementing acts to specify the relevant international standards that are to be used by Member States for DNA reference data exchange. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).~~

Article 11

Rules for requests and answers regarding DNA profiles

1. A request for an automated search ~~or comparison~~ shall include only the following information:

(a) the code of the requesting Member State;

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

(c) DNA profiles and their reference numbers referred to in Article 9;

(d) the types of DNA profiles transmitted (unidentified DNA profiles or ~~reference~~ ***identified*** DNA profiles).

2. The answer to the request 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, time and indication number of the request;

(c) the date, time and indication number of the answer;

(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) the type of DNA profiles transmitted (unidentified DNA profiles or ~~reference~~ ***identified*** DNA profiles);

(g) the matching DNA profiles.

3. Automated notification of a match shall only be provided if the automated search ~~or comparison~~ has resulted in a match of a minimum number of loci. The Commission shall adopt implementing acts to specify this minimum number of loci, in accordance with the procedure referred to in Article 76(2).

4. Where a search ~~or comparison~~ with unidentified DNA profiles results in a match, each requested Member State with matching data may insert a marking***, including the reference number from the DNA profile of the Member State of which data resulted in the match,*** in its national database indicating that there has been a match for that DNA profile following another Member State's search ~~or comparison~~.

5. Member States shall ensure that requests are consistent with ***notifications*** ~~declarations~~ sent pursuant to Article 8. Those ***notifications*** ~~declarations~~ shall be reproduced in the practical handbook referred to in Article 78.

SECTION 2

Dactyloscopic data

Article 12

Dactyloscopic reference data

1. Member States shall ensure the availability of dactyloscopic reference data from ~~the file for~~ the***ir*** national ~~automated fingerprint identification systems~~ ***database(s)*** 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. Dactyloscopic reference data which is not attributed to any individual (unidentified dactyloscopic data) shall be recognisable as such.

Article 13

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 the***ir national databases*** ~~automated fingerprint identification systems which they have established for that purpose~~, to conduct automated searches by comparing dactyloscopic reference data.

Searches may be conducted only in individual cases and in compliance with the national law of the requesting Member State.

2. The national contact point of the requesting Member State ~~shall~~ ***may decide to*** confirm a match ~~of~~ ***between two*** dactyloscopic data***. If so decided, it shall inform the requested Member State and shall manually confirm this match*** with dactyloscopic reference data ***received from*** ~~held by~~ the requested Member State ~~following the automated supply of the dactyloscopic reference data required for confirming a match~~.

Article 13a

Notifications of dactyloscopic databases

Each Member State shall inform, in accordance with Article 73, other Member States, the Commission, Europol and eu-LISA of the content of national dactyloscopic databases, to which Articles 12 and 13 apply, and the conditions for automated searches.

Article 14

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 case of a match, to retrieve further data and other information in their databases referred to in Article 12 in order to supply it to one, several or all of the other Member States in accordance with Article~~s~~ 47 ~~and 48~~***, or to Europol in accordance with Article 50(6)***;

(a bis) a reference number allowing Europol, in case of a match, to retrieve further data and other information referred to in Article 49(1) in order to supply it to one, several or all of the other Member States in accordance with Articles 49(2);

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

Article 15

Principles for the exchange of dactyloscopic data

1. The digitalisation of dactyloscopic data and their transmission to the other Member States ***or Europol*** shall be carried out in accordance with ***European or international standards***~~a uniform data format~~. The Commission shall adopt implementing acts to specify ~~the uniform data format~~ ***the relevant European or international standards for dactyloscopic data exchange that shall be used by Member States and Europol. Those implementing acts shall be adopted*** in accordance with the procedure referred to in Article 76(2).

2. Each Member State ***and Europol*** shall ensure that the dactyloscopic data it transmits are of sufficient quality for a***utomated*** comparison~~ by the automated fingerprint identification systems~~. ***A minimum quality standard shall be established to allow for comparison of dactyloscopic data. The Commission shall adopt implementing acts to specify that minimum quality standard. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).***

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

~~4. The Commission shall adopt implementing acts to specify the relevant existing standards for dactyloscopic data exchange that are to be used by Member States. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).~~

Article 16

Search capacities for dactyloscopic data

1. Each Member State ***and Europol*** shall ensure that ~~its~~ ***their*** search requests do not exceed the search capacities specified by the requested Member State ***or Europol to ensure national system readiness and avoid overloading of national systems***.

Member States ***and Europol*** shall inform ***other Member States,*** the Commission***, Europol*** and eu-LISA ~~in accordance with Article 79(8) and (10)~~ about their maximum search capacities per day for dactyloscopic data of identified persons and for dactyloscopic data of persons not yet identified. ***Those search capacities can be raised by Member States or Europol at any time including in case of urgency.***

2. The Commission shall adopt implementing acts to specify the maximum numbers of candidates accepted for comparison per transmission ***as well as the distribution of unused search capacities between Member States*** in accordance with the procedure referred to in Article 76(2).

Article 17

Rules for requests and answers regarding dactyloscopic data

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

(a) the code of the requesting Member State;

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

(c) the dactyloscopic data and their reference numbers referred to in Article 14.

2. The answer to the request 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, time and indication number of the request;

(c) the date, time and indication number of the answer;

(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 are consistent with notifications sent pursuant to Article 13a. Those notifications shall be reproduced in the practical handbook referred to in Article 78.

SECTION 3

Vehicle registration data

Article 18

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 owners~~,~~ ***or holders*** ~~or operators~~;

(b) data relating to vehicles.

2. Searches may be conducted only with a full chassis number**,** ***with*** ~~or~~ a full registration number ***or, if authorised by the national law of the requested Member State, with identification data relating to the owner or the holder of the vehicle (first name(s), family name(s), date of birth, name of registered company)***.

3. Searches may be conducted only in compliance with the national law of the requesting Member State.

Article 19

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. The information exchanged via Eucaris shall be transmitted in encrypted form.

3. The Commission shall adopt implementing acts to specify the data elements of the vehicle registration data which ~~to~~ ***may*** be exchanged. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 20

Keeping of logs

1. Each Member State shall keep logs of queries that the staff of its authorities duly authorised to exchange vehicle registration data make as well as 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) the Member State or ~~Union agency~~ ***Europol*** launching the request for a query;

(b) the date and time of the request;

(c) the date and time of the answer;

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

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

2. The logs referred to in paragraph 1 may be used only for the collection of statistics and 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 ***two*** ~~one~~ year***s*** 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 56.

SECTION 3a

Driving licence data

Article 20a

Automated searching of driving licence 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 driving licence data to conduct automated searches in individual cases. Member States may allow access to facial images as part of driving licence data, if available.

2. Searches may be conducted only with the driving licence number or, if authorised by the national law of the requested Member State, with data relating to the driving licence holder (first name(s), family name(s), place and date of birth).

3. Searches may be conducted only in compliance with the national law of the requesting Member State.

Article 20b

Principles of automated searching of driving licence data

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

2. The information exchanged via Eucaris shall be transmitted in encrypted form.

3. The Commission shall adopt implementing acts to specify the data elements of the driving licence data which may be exchanged. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 20c

Keeping of logs

1. Each Member State shall keep logs of queries that the staff of its authorities duly authorised to exchange driving licence data make as well as 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 driving licence data. Those logs shall include the following:

(a) the Member State or Europol launching the request for a query;

(b) the date and time of the request;

(c) the date and time of the answer;

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

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

2. The logs referred to in paragraph 1 may be used only for the collection of statistics and 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 two 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 56.

SECTION 4

Facial images

Article 21

Facial images *reference data*

1. Member States shall ensure the availability of facial images ***reference data*** from their national database***(***s***)*** established for the prevention, detection and investigation of criminal offences. ~~Those data shall only include facial images and the reference number referred to in Article 23, and shall indicate whether the facial images are attributed to an individual or not~~.

2. Facial images reference data~~Member States~~ shall not ***contain***~~make available in this context~~ any ***additional*** data from which an individual can be directly identified.

3~~2~~. Facial images ***reference data*** which are not attributed to any individual (unidentified facial images) ***shall***~~must~~ be recognisable as such.

Article 22

Automated searching of facial images

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*** facial images ***reference data*** ~~stored~~ in their national databases, to conduct automated searches ***by comparing facial images reference data***.

Searches may be conducted only in 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 facial images. If so decided, it shall inform the requested Member State and shall manually confirm this match with facial images reference data received from the requested Member State.*** ~~The requesting Member State shall receive a list composed of matches concerning likely candidates. That Member State shall review the list to determine the existence of a confirmed match.~~

~~3. A minimum quality standard shall be established to allow for search and comparison of facial images. The Commission shall adopt implementing acts to specify that minimum quality standard. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).~~

Article 22a

Notifications of facial images databases

Each Member State shall inform, in accordance with Article 73, other Member States, the Commission, Europol and eu-LISA of the content of national facial images databases, to which Articles 21 and 22 apply, and the conditions for automated searches.

Article 23

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 case of a match, to retrieve further data and other information in their databases referred to in Article 21 in order to supply it to one, several or all of the other Member States in accordance with Article~~s~~ 47 ~~and 48~~**, *or to Europol in accordance with Article 50(6);***

(a bis) a reference number allowing Europol, in case of a match, to retrieve further data and other information referred to in Article 49(1) in order to supply it to one, several or all of the other Member States in accordance with Articles 49(2)

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

Article 23a

Principles for the exchange of facial images

1. The digitalisation of facial images and their transmission to the other Member States or Europol shall be carried out in accordance with European or international standards. The Commission shall adopt implementing acts to specify the relevant European or international standards for facial images exchange that shall be used by Member States and Europol. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

2. Each Member State and Europol shall ensure that the facial images it transmits are of sufficient quality for automated comparison. A minimum quality standard shall be established to allow for comparison of facial images. The Commission shall adopt implementing acts to specify that minimum quality standard. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

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

Article 23b

Search capacities for facial images

1. Each Member State and Europol shall ensure that their search requests do not exceed the search capacities specified by the requested Member State or Europol to ensure national system readiness and avoid overloading of national systems.

Member States and Europol shall inform other Member States, the Commission, Europol and eu-LISA about their maximum search capacities per day for facial images exchanges. Those search capacities can be raised by Member States or Europol at any time including in case of urgency.

2. The Commission shall adopt implementing acts to specify the maximum numbers of candidates accepted for comparison per transmission as well as the distribution of unused search capacities between Member States in accordance with the procedure referred to in Article 76(2).

Article 24

Rules for requests and answers regarding facial images

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

(a) the code of the requesting Member State;

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

(c) the facial images and their reference numbers referred to in Article 23.

2. The answer to the request 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, time and indication number of the request;

(c) the date, time and indication number of the answer;

(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 are consistent with notifications sent pursuant to Article 22a. Those notifications shall be reproduced in the practical handbook referred to in Article 78.

SECTION 5

Police records

Article 25

Police records

1. Member States may decide to participate in the automated exchange of police records. Member States participating in the automated exchange of police records shall ensure the availability of biographical data of suspects and ~~criminals~~ ***convicted persons*** from their national police records indexes***, based on their national databases*** established for the ***prevention, detection and*** investigation of criminal offences. This set of data~~, if available,~~ shall contain the following data***, if available***:

(a) first name(s);

(b) family name(s);

(c) ***previously used name(s) and*** alias(es);

(d) date of birth;

(e) nationality or nationalities;

(f) place and country of birth;

(g) gender.

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

Article 26

Automated searching of police records

1. For the ***prevention, detection and*** investigation of criminal offences, 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 records indexes, to conduct automated searches.

Searches may be conducted only in individual cases and in compliance with the national law of the requesting Member State.

2. The requesting Member State shall receive ~~the~~ ***in an automated manner the*** list of matches with an indication of the quality of the matches.

The requesting Member State shall also be informed about the Member State whose database contains data that resulted in the match.

Article 26a

Notifications about databases used for police records exchanges

Each Member State shall inform, in accordance with Article 73, other Member States, the Commission and Europol, of their national databases used for establishing their national police records indexes and of the content of their national police records indexes, to which Articles 25 and 26 apply, and the conditions for automated searches.

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 case of a match, to retrieve personal data and other information in their indexes referred to in Article 25 in order to supply it to one, several or all of the Member States in accordance with Article~~s~~ ***44***~~47 and 48~~;

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

Article 28

Rules for requests and answers regarding police records

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

(a) the code of the requesting Member State;

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

(c) the ***data referred to in Article 25 as far as available*** ~~police records and their reference numbers referred to in Article 27~~.

2. The answer to the request 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, time and indication number of the request;

(c) the date, time and indication number of the answer;

(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 are consistent with notifications sent pursuant to Article 26a. Those notifications shall be reproduced in the practical handbook referred to in Article 78.

SECTION 6

Common provisions

Article 28a

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 via the Prüm framework solely for the purposes of:

a. searching missing persons;

b. identifying unidentified human remains.

2. Member States wishing to avail themselves of the possibility provided for in paragraph 1 shall adopt national legislative measures designating the competent national authorities and laying down the procedures, conditions and criteria.

Article 29

National contact points

Each Member State shall designate ~~a~~ ***one or more*** national contact point~~s~~.

~~The national contact points shall be responsible for supplying the data~~ referred to in Articles 6, ~~7,~~ 13, 18, ***20a,*** 22 and 26.

Article 30

Implementing measures

The Commission shall adopt implementing acts to specify the technical arrangements for the procedures set out in Articles 6, ~~7,~~ 13, 18, ***20a,*** 22 and 26. Those implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 31

Technical specifications

Member States and Europol shall observe common technical specifications in connection with all requests and answers related to searches ~~and comparisons~~ of DNA profiles, dactyloscopic data, vehicle registration data, ***driving licence data,*** facial images and police records. The Commission shall adopt implementing acts to specify these technical specifications in accordance with the procedure referred to in Article 76(2).

Article 32

Availability of automated data exchange at national level

1. Member States shall take all necessary measures to ensure that automated searching ~~or comparison~~ of DNA profiles, dactyloscopic data, vehicle registration data, ***driving licence data,*** facial images and police records is possible 24 hours a day and seven days a week.

2. National contact points shall immediately inform each other, the Commission, Europol and eu-LISA of ***any*** ~~the technical fault causing~~ unavailability of the automated data exchange.

National contact points shall agree on temporary alternative information exchange arrangements in accordance with the applicable Union law and national legislation.

3. National contact points shall re-establish the automated data exchange ***by any means necessary and*** without delay.

Article 33

Justification for the processing of data

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

Europol shall keep a justification of the queries it makes.

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

(a) the purpose of the query, including a reference to the specific case or investigation;

(b) an indication on whether the query concerns a suspect or a perpetrator of a criminal offence***, a victim, a missing person or human remains***;

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

3. The justifications referred to in paragraph 2 ***shall be traceable to the logs stored in accordance with articles 20, 20c, 40 and 45, and*** shall only be used 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 erased ***two*** ~~one~~ year***s*** 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. 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 56.

Article 34

Use of the universal message format

1. The universal message format (UMF) standard ***as referred to in Article 38 of Regulation (EU) 2019/817 and in Article 38 of Regulation (EU) 2019/818*** shall be used in the development of the router referred to in Article 35 and EPRIS ***as far as applicable***.

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

CHAPTER 3

ARCHITECTURE

SECTION 1

Router

Article 35

The router

1. A router is established for the purposes of facilitating the establishment of connections between Member States and with Europol for querying with ***biometric data***, retrieving ***biometric data and alphanumeric data,*** and scoring biometric 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 Member States' databases referred to in Articles 5, 12 and 21 as well as of Europol data;

(b) a secure communication channel between the central infrastructure**,** Member States and ***Europol*** ~~Union agencies that are entitled to use the router~~;

(c) a secure communication infrastructure between the central infrastructure and the European Search Portal for the purposes of Article 39.

Article 36

Use of the router

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

Article 37

~~Queries~~*Processes*

1. The router users referred to in Article 36 shall ***submit to the router a*** request ***for*** a query ~~by submitting~~ ***with*** biometric data ~~to the router~~. The router shall dispatch the request for a query to ~~the~~ ***all or specific*** Member States' databases and Europol data simultaneously with the data submitted by the user ~~and in accordance with their access rights~~.

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

3. Any matches resulting from the query in each Member States' databases and Europol data shall be sent back in an automated manner to the router.

4. The router shall rank***, on the initiative of the requesting Member State and where applicable,*** the replies ~~in accordance with the score of the correspondence between~~ ***by comparing*** the biometric data used for querying and the biometric data ***supplied in the answers by*** ~~stored in~~ the ***requested*** Member State***(***s***)***~~' databases and~~ ***or*** Europol ~~data~~.

5. The list of matching biometric data and their scores shall be returned to the router user by the router.

6. The Commission shall adopt implementing acts to specify the technical procedure for the router to query Member States' databases and Europol data, the format of the router replies and the technical rules for ~~scoring~~ ***comparing and ranking*** the correspondence between biometric data. These implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 38

Quality check

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

Should the data be unsuitable for an automated comparison, the requested Member State shall inform the requesting Member State about it via the router without delay.

Article 39

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

1. The router users referred to in Article 36 may launch a query to Member States' databases and Europol data simultaneously with a query to the Common Identity Repository where the relevant conditions under Union law are fulfilled and in accordance with their access rights. For this purpose, the router shall query the Common Identity Repository via the European Search Portal.

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 the queries shall be transmitted via the European Search Portal.

Only designated authorities defined in Article 4, point 20, of Regulation (EU) 2019/817 and Article 4, point 20, of Regulation (EU) 2019/818 may launch these simultaneous queries.

Simultaneous queries of the Member States' databases and Europol data and the Common Identity Repository may only be launched in cases where ~~it is likely~~ ***there is a suspicion*** that data on a suspect, perpetrator or victim of a terrorist offence or other serious criminal offences as defined respectively in Article 4, points 21 and 22, of Regulation (EU) 2019/817 and Article 4, points 21 and 22, 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) the Member State or Union agency launching the request for a query;

(b) the date and time of the request;

(c) the date and time of the answer;

(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 an answer;

(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 its competent authorities and the staff of those authorities duly authorised to use the router make as well as 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 may be used only for the collection of statistics and 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 ~~one~~ ***two*** year***s*** 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 56.

Article 41

Notification procedures in case of technical impossibility 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, the router users ***referred to in Article 36*** shall be notified in an automated manner by eu-LISA. eu-LISA shall take 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 or Europol data because of a failure of the national infrastructure in a Member State, that Member State shall notify the other Member States, eu-LISA and the Commission in an automated manner. Member States ***concerned*** shall take measures to address the technical impossibility to use the router without delay.

3. 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 infrastructure of Europol, Europol shall notify the Member States, eu-LISA and the Commission in an automated manner. Europol shall take measures to address the technical impossibility to use the router without delay.

SECTION 2

EPRIS

Article 42

EPRIS

1. For the automated searching of ***national*** police records ***indexes*** referred to in Article 26, Member States and Europol shall use the European Police Records Index System (EPRIS).

2. EPRIS shall be composed of:

(a) a ***de***central***ised*** infrastructure ***in the Member States***, including a search tool enabling the simultaneous querying of ***national police records indexes, based on national*** ~~Member States'~~ databases;

(b) a central infrastructure, supporting the search tool enabling the simultaneous querying of national police records indexes, based on national databases;

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

Article 43

Use of EPRIS

1. For the purposes of searching police records via EPRIS, ***at least two of*** the following sets of data shall be used:

(a) first name(s);

(b) family name(s);

(c) date of birth.

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

(a) ***previously used name(s) and*** alias(es);

(b) nationality or nationalities;

(c) place and country of birth;

(d) gender.

3. The data referred to in points (a) and (b) of paragraph 1 and in point~~s~~ (a)~~, (b) and (c)~~ of paragraph 2 used for queries shall be pseudonymised.

Article 44

~~Queries~~*Processes*

1. Member States and Europol shall request a query by submitting the data referred to in Article 43.

EPRIS shall dispatch the request for a query to the Member States' databases with the data submitted by the requesting Member State and in accordance with this Regulation.

2. On receiving the request for a query from EPRIS, each requested Member State shall launch a query of their national police records index in an automated manner and without delay.

3. Any matches resulting from the query in each Member State's database shall be sent back in an automated manner to EPRIS.

4. The list of matches shall be returned to the requesting Member State by EPRIS. The list of matches shall indicate the quality of the match as well as the Member State whose database contains data that resulted in the match.

5. Upon reception 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, as well as*** any additional relevant information to the requested Member State(s) via SIENA.

6. The requested Member State(s) shall process such requests without delay to decide whether to share the data stored in their database.

Upon confirmation, the requested Member State(s) shall share ***at least*** the data referred to in Article 43 where available. This exchange of information shall take place via SIENA.

7. The Commission shall adopt implementing acts to specify the technical procedure for EPRIS to query Member States' databases and the format ***and the maximum number*** of the replies. These implementing acts shall be adopted in accordance with the procedure referred to in Article 76(2).

Article 45

Keeping of logs

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

(a) the Member State or ~~Union agency~~ ***Europol*** launching the request for a query;

(b) the date and time of the request;

(c) the date and time of the answer;

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

(e) the national databases that provided an answer.

2. Each ***participating*** Member State shall keep logs of the requests for queries that its competent authorities and the staff of those 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 may be used only 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 ~~one~~ ***two*** year***s*** 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 56.

Article 46

Notification procedures in case of technical impossibility to use EPRIS

1. Where it is technically impossible to use EPRIS to query one or several national databases because of a failure of the infrastructure of Europol, Member States shall be notified in an automated manner by Europol. Europol shall take measures to address the technical impossibility to use EPRIS without delay.

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

CHAPTER 4

EXCHANGE OF DATA FOLLOWING A MATCH

Article 47

Exchange of core data

~~Where the procedures referred to in Articles 6, 7, 13 or 22 show a match between the data used for the search or comparison and data held in the database of the requested Member State(s), and upon confirmation of this match by the requesting Member State, the requested Member State shall return a set of core data via the router within 24 hours. That set of core data, if available, shall contain the following data:~~

~~(a) first name(s);~~

~~(b) family name(s);~~

~~(c) date of birth;~~

~~(d) nationality or nationalities;~~

~~(e) place and country of birth;~~

~~(f) gender~~.

1. A set of core data shall be returned via the router within 72 hours, except if a judicial authorisation is required under national law, where all the following conditions have been met:

(a) the procedures referred to in Articles 6, 13 or 22 show a match between the data used for the search and data stored in the database of the requested Member State(s);

(b) upon confirmation of this match by the requesting Member State as referred to in Articles 6(4), 13(2) and 22(2), or by the requested Member State(s) in the specific case of DNA as referred to in Article 6(5);

(c) upon transmission of a description of the facts and indication of the underlying offence, using the common table of offences categories referred to in Annex A of Decision 2009/316/JHA, by the requesting Member State as referred to in Articles 6(4), 13(2) and 22(2), or by the requested Member State(s) in the specific case of DNA as referred to in Article 6(5).

2. The set of core data shall be returned by the requested Member State, or by the requesting Member State in the specific case of DNA as referred to in Article 6(5).

3. That set of core data shall contain the following data, if available:

(a) In case of a confirmed match with identified data (person):

i. ~~(a)~~ first name(s);

ii. ~~(b)~~ family name(s);

iii. ~~(c)~~ date of birth;

iv. ~~(d)~~ nationality or nationalities;

v. ~~(e)~~ place and country of birth;

vi. ~~(f)~~ gender***;***

vii. previously used name(s) and alias(es);

viii. date and place of biometric acquisition;

ix. the criminal offence in the framework of which the biometric acquisition was carried out;

x. the criminal case number;

xi. the responsible authority of the criminal case.

(b) In case of a confirmed match with unidentified data (trace):

i. date and place of biometric acquisition;

ii. the criminal offence in the framework of which the biometric acquisition was carried out;

iii. the criminal case number;

iv. the responsible authority of the criminal case.

~~*Article 48*~~

~~**Use of SIENA**~~

~~Any exchange which is not explicitly provided for in this Regulation between Member States' competent authorities or with Europol, at any stage of one of the procedures under this Regulation, shall take place via SIENA.~~

CHAPTER 5

EUROPOL

Article 49

Access by Member States to *biometric data provided by* third countr*iesy*~~-sourced biometric data~~ 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 has 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 this procedure results in a match between the data used for the search and Europol data, the follow-up shall take place in accordance with Regulation (EU) 2016/794.

Article 50

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

1. ***For the objectives of Article 3 of Regulation (EU) 2016/794,*** Europol shall, in accordance with Regulation (EU) 2016/794, have access to data, which are stored by Member States in their national databases ***and police records indexes*** in accordance with this Regulation.

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 ***and driving licence data*** as a search criterion shall be carried out using Eucaris.

4. Europol queries performed with ~~police records~~ ***biographical data of suspects and convicted persons as referred to in Articles 25 and 26*** as a search criterion***,*** shall be carried out using EPRIS.

5. Europol shall carry out the searches ***with data provided by third countries*** in accordance with paragraph***s*** 1 ***to 4*** only when ***necessary for*** carrying out its tasks ~~referred to~~***for the purpose of Article 18(2), points (a) and (c)*** ~~in~~ ***of*** Regulation (EU) 2016/794***, and where all of the following conditions have been fulfilled:***

(a) the data provided by third countries have been cross-checked with data held by Europol for the purpose of Article 18(2), points (a) and (c) of Regulation (EU) 2016/794;

(b) Europol transmits the name of the third country which provided the data.

6. Where the procedures referred to in Articles 6, ~~7,~~ 13 or 22 show a match between the data used for the search ~~or comparison~~ and data held in the national database of the requested Member State(s), ***Europol shall only inform the Member State(s) involved.*** ~~and u~~ ***U***pon confirmation of that match by Europol ***and upon transmission of a description of the facts and indication of the underlying offence using the common table of offences categories referred to in Annex A of Decision 2009/316/JHA***, the requested Member State shall decide whether to return a set of core data via the router within ***72*** ~~24~~ hours***, except if a judicial authorisation is required under national law***. That set of core data~~, if available,~~ shall contain the following data***, if available***:

(a) first name(s);

(b) family name(s);

(c) date of birth;

(d) nationality or nationalities;

(e) place and country of birth;

(f) gender.

7. Europol's use of information obtained from a search made in accordance with paragraph 1 and from the exchange of core data in accordance with paragraph 6 shall be subject to the consent of the Member State in ~~which~~ ***the*** database ***of which*** the match occurred. If the Member State allows the use of such information, its handling by Europol shall be governed by Regulation (EU) 2016/794.

CHAPTER 6

DATA PROTECTION

Article 51

Purpose of the data *processing*

1. Processing of personal data ***received*** by ~~the requesting~~***a*** Member State or Europol shall be permitted solely for the purposes for which the data have been supplied by the ~~requested~~ 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 ~~requested~~ Member State ***which provided the data***.

2. Processing of data supplied pursuant to Articles 6, ~~7,~~ 13, 18***, 20a,*** ~~or~~ 22 ***or 26,*** by ~~the searching or comparing~~***a*** Member State ***or Europol*** shall be permitted solely ~~in order to~~***for the purpose of***:

(a) establish***ing*** whether the compared DNA profiles, dactyloscopic data, vehicle registration data, ***driving licence data,*** facial images and police records match;

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

(b) prepar~~e~~***ing*** and submit***ting*** a police ***or judicial*** request for legal assistance ***by Member States,*** if those data match;

(c) logging within the meaning of Articles ***20, 20c,*** 40 and 45.

3. ~~The requesting Member State may process the data supplied to it in accordance with Articles 6, 7, 13 or 22 solely where this is necessary for the purposes of this Regulation.~~ The ~~supplied~~ data ***received by a Member State or Europol*** shall be deleted immediately following ~~data comparison or~~ automated replies to searches unless further processing is necessary ~~by the requesting Member State~~ for the purposes ***referred to in points aa, b and c of paragraph 2 or authorised in accordance with paragraph 1*** ~~of the prevention, detection and investigation of criminal offences~~.

~~4. Data supplied in accordance with Article 18 may be used by the requesting Member State solely where this is necessary for the purposes of this Regulation. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 20. The requesting Member State shall use the data received in a reply solely for the procedure for which the search was made.~~

Article 52

Accuracy, relevance and data retention

1. Member States ***and Europol*** shall ensure the accuracy and current relevance of personal data ***processed based on this Regulation***. Should ~~a requested~~ ***the*** Member State ***which provided the data or Europol*** become aware that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to ~~any requesting~~ ***the*** Member State ***which received the data or Europol***. All ~~requesting~~ Member States concerned ***or Europol*** shall ~~be obliged to~~ correct or delete the data accordingly ***without undue delay***. ~~Moreover, personal data supplied shall be corrected if they are found to be incorrect.~~ If the ~~requesting~~ Member State ***which received the data or Europol*** has reason to believe that the supplied data are incorrect or should be deleted***,*** the ~~requested~~ Member State ***which provided the data*** shall be informed.

2. Where a data subject contested the accuracy of data in possession of a Member State, where the accuracy cannot be reliably established by the Member State concerned and where it is requested by the data subject, the data concerned shall be marked with a flag. Where such a flag exists, Member States may remove it only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

3. Data supplied 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; ***or***

(b) following the expiry of the maximum period for keeping data laid down under the national law of the ~~requested~~ Member State ***which provided the data*** where ~~the requested~~ ***that*** Member State informed the ~~requesting~~ Member State ***which received the data or Europol*** of that maximum period at the time of supplying the data.

Where there is reason to believe that the deletion of data would prejudice the interests of the data subject, the data shall be ~~blocked~~***restricted to be processed*** instead of being deleted. ~~Blocked~~ ***Restricted*** data may be ~~supplied or used~~***processed*** solely for the purpose which prevented their deletion.

Article 53

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 for the processing of personal data via EPRIS.

Article 54

Security of processing

1. Europol, eu-LISA and Member States' authorities shall ensure the security of the processing of personal data that takes place pursuant to this Regulation. Europol, eu-LISA and Member States' authorities 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 as well as their related communication infrastructure.

3. In particular, eu-LISA and Europol shall adopt the necessary measures concerning the router and EPRIS respectively, including a security plan, a business continuity plan and a disaster recovery plan, 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 that persons authorised to access the router and EPRIS have access only to the data covered by their access authorisation, by means of individual user identities and confidential access modes only;

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

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

(j) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data to or from the router and EPRIS 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 and EPRIS 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.

Article 55

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 them 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.~~ Security incidents shall be managed so as to ensure a quick, effective and proper response.

In the event of a security incident concerning the router, eu-LISA and the Member States concerned or Europol shall cooperate in order to ensure a quick, effective and proper response.

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

2 ~~3~~. Member States shall notify ~~its~~ ***their*** competent ~~supervisory~~ authorities of any security incidents without undue delay.

Without prejudice to Article 34 of Regulation (EU) 2016/794, ***in the event of a security incident in relation to the central infrastructure of EPRIS,*** 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.

In the event of a security incident in relation to the central infrastructure of the router, eu-LISA 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.

3 ~~4~~. 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.

4 ~~5~~. 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 56

Self-monitoring

1. Member States and ~~the relevant Union agencies~~***Europol*** shall ensure that each authority entitled to use Prüm II takes the measures necessary to monitor its compliance with this Regulation and cooperates, where necessary, with the supervisory authority.

2. The data controllers shall take the necessary measures to monitor the compliance of data processing pursuant to this Regulation, including through frequent verification of the logs referred to in Articles ***20, 20c,*** 40 and 45, and cooperate, where necessary, with the supervisory authorities ~~and~~ ***or*** with the European Data Protection Supervisor.

Article 57

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 58*~~

~~**Burden of proof**~~

~~1. Member States shall take the necessary measures to ensure that persons who consider themselves as having been discriminated against due to the processing or exchange of their personal data do not bear the burden of proof. In cases where a person considers that he or she has been allegedly discriminated against in the context of an automated comparison in the context of this Regulation in front of a court or other competent judicial authority, the Member State authorities having processed the data shall justify why there was no discrimination.~~

~~2. Paragraph 1 shall not apply to criminal procedures.~~

~~3. Member States shall not take specific measures in the meaning of paragraph 1 to proceedings in which it is for the court or competent judicial body to investigate the facts of the case.~~

Article 59

Liability

If any failure of a Member State ***or Europol when performing queries in accordance with Article 50,*** 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 insofar 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 60

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. Europol and eu-LISA 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.

Article 61

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 and ensure 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 Prüm II communication channels.

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. The European Data Protection ***Supervisor*** ~~Board~~ shall send a joint report of its activities under this Article to the European Parliament, to the Council, to the Commission, to Europol and to eu-LISA by [*2 years after entry into operation of the router and EPRIS*] and every two years thereafter. That report shall include a chapter on each Member State prepared by the supervisory authority of the Member State concerned.

Article 62

Communication of personal data to third countries and international organisations

~~Data processed in accordance with this Regulation shall not be transferred or made available to third countries or to international organisations in an automated manner.~~

Any transfer to a third country or an international organisation of data obtained by a Member State in accordance with this Regulation, shall require the consent of the Member State which provided the data.

CHAPTER 7

RESPONSIBILITIES

Article 63

Responsibilities of Member States

1. ~~Each~~ Member State*s* shall be responsible for:

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

(b) the integration of the existing national systems and infrastructures 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 the existing national systems and infrastructures 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 the competent national 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 the competent national 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 the competent national 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 of a match as referred to in Article 6(~~3~~***4***), Article ***6(5)***~~7(3)~~, Article 13(2)~~,~~ ***and*** Article 22(2) ~~and Article 26(2)~~;

(k) ensuring the availability of the data necessary for the exchange of data in accordance with Article 6, ~~Article 7,~~ Article 13, Article 18, ***Article 20a,*** Article 22 and Article 26;

(l) the exchange of information in accordance with Article 6, ~~Article 7,~~ Article 13, Article 18, ***Article 20a,*** Article 22 and Article 26;

(m) ***correcting or*** deleting any data received from a requested Member State within 48 hours following the notification from the requested Member State that the personal data submitted was incorrect, no longer up-to-date or was unlawfully transmitted.

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

2. ~~Each~~ Member State***s*** shall be responsible for connecting their competent national authorities to the router, EPRIS and Eucaris.

Article 64

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 also be responsible for the processing of 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. 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 provide 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 interrogation of the national databases in accordance with the technical specifications.

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

6. Europol shall be responsible for the procedures referred to in Articles 49 and 50.

Article 65

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 66(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.

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

eu-LISA shall define the design of the physical architecture of the router including its communication infrastructures and the technical specifications and its evolution as regards the central infrastructure and the secure communication infrastructure. This design shall be adopted by the Management Board, 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.

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).

The development shall consist of the elaboration and implementation of the technical specifications, testing and overall project management and coordination.

4. During the design and development phase, the Interoperability 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 Interoperability Programme Management Board shall submit written reports on progress of the project to eu-LISA's Management Board. The Interoperability Programme Management Board shall have no decision-making power, nor any mandate to represent the members of eu-LISA's Management Board.

The Advisory Group referred to in Article 77 shall meet regularly until the start of operations of the router. It shall report after each meeting to the Interoperability Programme Management Board. It shall provide the technical expertise to support the tasks of the Interoperability Programme Management Board and shall follow up on the state of preparation of the Member States.

Article 66

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

1. Following the entry into 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 fast, efficient and controlled access, full and uninterrupted availability of the router, and a response time in line with the operational needs of the competent authorities of the Member States 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[15], 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 interoperability components. This 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 also perform tasks related to providing training on the technical use of the router.

[15] OJ L 56, 4.3.1968, p. 1.

CHAPTER 8

AMENDMENTS TO OTHER EXISTING INSTRUMENTS

Article 67

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

1. In Decision 2008/615/JHA, Articles ***1(a)***, 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 as set out in Article 74***(1)***.

   Therefore, Articles ***1(a)***, 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 as set out in Article 74***(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 as set out in Article 74.

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 as set out in Article 74.

Article 68

Amendments to Regulation (EU) 2018/1726

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

(1) the following Article 13a is inserted:

"Article 13a

Tasks related to the router

In relation to Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*], the Agency shall perform the tasks related to the router conferred on it by that Regulation.

_____

* Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L …)"

in Article 17, paragraph 3 is replaced by the following:

'3. The seat of the Agency shall be Tallinn, Estonia.

The tasks relating to development and operational management referred to in Article 1(4) and (5) and Articles 3 to 8 and Articles 9, 11 and 13a shall be carried out at the technical site in Strasbourg, France.

A backup site capable of ensuring the operation of a large-scale IT system in the event of failure of such a system shall be installed in Sankt Johann im Pongau, Austria.'

in Article 19, paragraph 1, the following point (eeb) is inserted:

"(eeb) adopt reports on the state of play of the development of the router pursuant to Article 79(2) of the Regulation (EU) …/… of the European Parliament and of the Council* [this Regulation];"

in Article 19, paragraph 1, points (ff) and (hh) are replaced by the following:

> ***"(ff) adopt reports on the technical functioning of 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, of the VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA, of EES pursuant to Article 72(4) of Regulation (EU) 2017/2226, of ETIAS pursuant to Article 92(4) of Regulation (EU) 2018/1240, of the ECRIS-TCN and of the ECRIS reference implementation pursuant to Article 36(8) of Regulation (EU) 2019/816 of the European Parliament and of the Council, of the interoperability components pursuant to Article 78(3) of Regulation (EU) 2019/817 and Article 74(3) of Regulation (EU) 2019/818 and of the router pursuant to Article 79(5) of the Regulation (EU) …/… of the European Parliament and of the Council* [this Regulation];***
>
> ***(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) 2019/818 and Article 60(1) of the Regulation (EU) …/… of the European Parliament and of the Council* [this Regulation] and ensure appropriate follow-up of those audits;"***

Article 69

Amendments to Regulation (EU) 2019/817

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

> "(d) a secure communication infrastructure between the ESP and the router established by Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*].
>
> _____
>
> * Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L …)"

Article 70

Amendments to Regulation (EU) 2019/818

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

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

> "(d) a secure communication infrastructure between the ESP and the router established by Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*].
>
> _____
>
> * Regulation (EU) [number] of the European Parliament and of the Council of xy on [officially adopted title] (OJ L …)"

(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, 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) …/… of the European Parliament and of the Council* [this Regulation]*** ~~Prüm II~~."

"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 ~~65~~***71***(1) of Regulation (EU) …/… ***** [*this Regulation*]. 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 ~~65~~***71***(1) of Regulation (EU) …/… ***** [*this Regulation*]."

CHAPTER 9

FINAL PROVISIONS

Article 71

Reporting and statistics

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

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

(b) number of queries per category of data;

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

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

(e) number of matches against Europol data per category of data;

(f) number of confirmed matches where there were exchanges of core data; and

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

(h) number of matches per type:

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.

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

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

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

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

It shall not be possible to identify individuals from the data.

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

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

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

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

It shall not be possible to identify individuals from the data.

4. eu-LISA shall store the data referred to in ~~those~~ paragraph~~s~~ ***1***.

The data shall allow the authorities referred to in paragraph 1 to obtain customisable reports and statistics to enhance the efficiency of law enforcement cooperation.

Article 72

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 the existing national infrastructures and their connections to the router and EPRIS as well as costs incurred in connection with the establishment of national facial images databases and police national 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 the Eucaris software application referred to in Article 19(1) ***and Article 20b(1)***.

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

Article 73

Notifications

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

2. eu-LISA shall notify the Commission of the successful completion of the tests referred to in Article 74(1), point (b).

2a. Europol shall notify the Commission of the successful completion of the tests referred to in Article 74(2), point (b).

3. Member States shall notify the Commission, Europol and eu-LISA of the national contact points ***referred to in Article 29***.

4. Member States shall notify other Member States, the Commission and eu-LISA of the content of national databases and the conditions for automated searches in accordance with Articles 8, 13a, 22a and 26a.

Article 74

Start of operations

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

(a) the measures referred to in 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' authorities~~,~~ and Europol.

In that implementing act the Commission shall also determine the date from which the Member States and ~~the Union agencies~~***Europol*** ~~must~~ ***shall*** 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 ~~the Union agencies~~***Europol*** ~~must~~ ***shall*** 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. That implementing act shall be adopted in accordance with the procedure referred to in Article 76(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 21, for the purposes of automated searching of facial images as referred to in Article 22.

2. The Commission shall determine the date from which the Member States and ~~the Union agencies~~***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(7) 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' authorities.

3. 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 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 the connection, which it has conducted in cooperation with the Member States' authorities~~,~~ and eu-LISA.

4. The Commission shall determine the date from which Europol is to have access to data stored in Member States' databases in accordance with Article 50 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 the connection, which it has conducted in cooperation with the Member States' authorities~~,~~ and eu-LISA.

5. Member States shall start, two years after the entry into force of this Regulation, the automated searching of driving licence data by means of EUCARIS in accordance with Article 20a, 20b and 20c.

Article 75

Transitional provisions and derogations

1. Member States and the Union agencies shall start applying Articles 21 to 24, Article 47 and Article 50(6) from the date determined in accordance with Article 74(1), the first subparagraph with the exception of Member States, which did not start using the router.

2. Member States and the Union agencies shall start applying Articles 25 to 28 and Article 50(4) from the date determined in accordance with Article 74(2).

3. Member States and the Union agencies shall start applying Article 49 from the date determined in accordance with Article 74(3).

4. Member States and the Union agencies shall start applying Article 50(1), (2), (3), (5) and (7) from the date determined in accordance with Article 74(4).

Article 76

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 77

Advisory group

The responsibilities of eu-LISA's Interoperability Advisory Group 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 78

Practical handbook

The Commission shall, in close cooperation with the Member States, Europol and eu-LISA, 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.

Article 79

Monitoring and evaluation

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

2. By [*one year after entry into force of this Regulation*] and every year thereafter during the development phase of the router, eu-LISA shall respectively submit a report to the European Parliament and to the Council on the state of play of the development of the router. That report shall contain detailed information about the costs incurred and information as to any risks which may impact the overall costs to be borne by the general budget of the Union in accordance with Article 72.

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 as well as justifying any divergences.

3. By [*one year after entry into force of this Regulation*] 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 preparation for the implementation of this Regulation and on the state of play of the development of EPRIS including detailed information about the costs incurred and information as to any risks which may impact the overall costs to be borne by the general budget of the Union in accordance with Article 72.

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 as well as justifying any divergences.

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

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 of the router, including the security thereof.

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 of EPRIS, including the security thereof.

7. Three years after the start of operations of the router and EPRIS as referred to in Article 74 and every four years thereafter, the Commission shall produce an overall evaluation of Prüm II, including:

(a) an assessment of the application of this Regulation;

(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 Prüm II performance and its working practices in light of its objectives, mandate and tasks;

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

The Commission shall transmit the evaluation report to the European Parliament, the Council, the European Data Protection Supervisor and the European Agency for Fundamental Rights.

8. 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. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the ***Member States'*** ~~designated~~ authorities.

9. The Member States shall provide Europol and the Commission with the information necessary to draft the reports referred to in paragraphs 3 and 6. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the ***Member States'*** ~~designated~~ authorities.

10. Member States, eu-LISA and Europol shall provide the Commission with the information necessary to produce the evaluations 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. ***This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the Member States' authorities.***

Article 80

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 Brussels,

For the European Parliament	*For the Council*
The President	*The President*