Council of the European Union

Brussels, 10 March 2022
(OR. fr)

6925/22

LIMITE

IXIM 47
ENFOPOL 112
JAI 295
CODEC 245

Interinstitutional File: 2021/0410(COD)

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	14204/21; 5616/22; 6334/22
No. Cion doc.:	COM(2021) 784 final
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

Delegations will find in annex the Presidency's compromise proposals on blocks 8 and 9 of the abovementioned proposal for a Regulation.

All changes proposed by the Presidency, as compared to the Commission's proposal, appear as ~~strikethrough~~ and **bold underlined**.

ANNEX

CHAPTER 6

DATA PROTECTION

Article 51

Purpose of the data processing

1. Processing of personal data 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 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 **supplied 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 Member State 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 Member State **or Europol**. All requesting Member States **or Europol** concerned shall be obliged to correct or delete the data accordingly. ~~Moreover, personal data supplied shall be corrected if they are found to be incorrect.~~ If the requesting Member State **or Europol** has reason to believe that the supplied data are incorrect or should be deleted the requested Member State 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 where the requested Member State informed the requesting Member State **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.

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.

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.

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

CHAPTER 7

RESPONSIBILITIES

Article 63

Responsibilities of Member States

1. Each Member State 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), Article 7(3), Article 13(2), 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 22 and Article 26;

(l) the exchange of information in accordance with Article 6, Article 7, Article 13, Article 18, 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 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[1], 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.

(…)

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

1 OJ L 56, 4.3.1968, p. 1.

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

(h) number of matches per type:

i. identified profile-unidentified profile;

ii. unidentified profile-identified profile;

iii. unidentified profile-unidentified profile;

iv. identified profile-identified profile.

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).

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.

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 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.

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*