EUROPEAN
COMMISSION

Brussels, 8.12.2021
COM(2021) 784 final

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

{SEC(2021) 421 final} - {SWD(2021) 378 final} - {SWD(2021) 379 final}

EXPLANATORY MEMORANDUM

CONTEXT OF THE PROPOSAL

• Reasons for the proposal

Criminality across Europe undermines EU citizens' security and well-being. Law enforcement authorities need robust and performant tools to fight crime effectively. Cooperation and information sharing are the most powerful means to combat crime and pursue justice.[1] In 2021, more than 70% of organised crime groups were found to be present in more than three Member States.[2] Even the seemingly most local crime may have links to other places in Europe where the same perpetrator carried out his/her criminal acts. Similarly, links of presumably local crime to organised crime structures and operations are often not obvious. Therefore, to be able to effectively fight crime, law enforcement authorities need to be able to exchange data in a timely manner. The EU has already provided law enforcement with a range of tools to facilitate the exchange of information, which have proven crucial in uncovering criminal activities and networks,[3] but there are still information gaps that need to be addressed. Moreover, with data stored separately in various national IT systems as well as large-scale IT systems at the EU level, there is a need to ensure the systems can communicate with each other.

In an area without internal border controls (the 'Schengen' area), there are still borders and obstacles when it comes to data exchange between law enforcement authorities,[4] which leads to blind spots and loopholes for numerous criminals and terrorists that act in more than one Member State. This initiative, together with the proposal, adopted in parallel, for a Directive on information exchange between law enforcement authorities of Member States,[5] aim to reinforce the exchange of information between Member States and therefore provide EU law enforcement authorities with enhanced tools to fight crime and terrorism.[6]

For more than ten years, the Prüm framework has enabled law enforcement authorities across the EU to exchange information. The Prüm Decisions,[7] adopted in 2008 with the aim of supporting cross-border police and judicial cooperation related to criminal matters, provide for the automated exchange of specific data (DNA profiles, fingerprints and vehicle registration data) between authorities responsible for the prevention, detection and investigation of criminal offences. The Prüm framework is successfully contributing to fighting crime and terrorism in the EU, but there are still loopholes in the field of information exchange and therefore there is room for further improvement.

The Council Conclusions on the implementation of the Prüm Decisions ten years after their adoption underlined the importance of the automated searching and comparison of DNA profiles, dactyloscopic data and vehicle registration data for tackling terrorism and cross-border crime. The

[1] See the 2020 EU Security Union Strategy - COM(2020) 605 final (24.7.2020).
[2] EU Serious and Organised Crime threat assessment 2021
[3] EU Strategy to tackle Organised Crime 2021-2025, COM(2021) 170 final (14.4.2021).
[4] Such as the way certain categories of data are exchanged, the channel used for these exchanges, the time limits applicable, etc.
[5] [Reference].
[6] Communication on a Strategy towards a fully functioning and resilient Schengen area, COM(2021) 277 final (2.6.2021).
[7] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA. The Council Decisions are based on the 2005 Prüm Convention.

Council also invited the Commission to consider revising the Prüm Decisions with a view to broadening their scope and to updating the necessary technical and legal requirements.[8]

Prüm II builds on the existing Prüm framework, reinforcing and modernising the framework and allowing interoperability with other EU information systems. It will ensure that all the relevant data that is available for law enforcement authorities in a Member State can be used by law enforcement authorities in other Member States. It will also ensure that Europol can provide support to Member States in the context of the Prüm framework. This initiative provides for the creation of a new architecture that allows for easier and faster exchange of data between Member States and that ensures a high level of protection of fundamental rights.

- **Objectives of the proposal**

The general objective of this proposal results from the Treaty-based goal of contributing to the internal security of the European Union. Among measures to do so, the collection, storage, processing, analysis and exchange of relevant information is listed.[9] The general objective of this instrument is thus to improve, streamline and facilitate the exchange of information for the purpose of the prevention, detection and investigation of criminal and terrorist offences between Member States' law enforcement authorities, but also with Europol as the EU criminal information hub.

The specific policy objectives of this proposal are to:

(a) Provide a technical solution for efficient automated exchange of data between law enforcement authorities to make them aware of relevant data that is available in the national database of another Member State;

(b) Ensure that more relevant data (in terms of data categories) from national databases in other Member States is available to all competent law enforcement authorities;

(c) Ensure that relevant data (in terms of sources of data) from Europol's databases is available to law enforcement authorities;

(d) Provide law enforcement authorities with efficient access to the actual data corresponding to a 'hit' that is available in the national database of another Member State.

- **Consistency with existing policy provisions in the policy area**

The recent Schengen Strategy[10] announced several measures to step up police cooperation and information exchange between law enforcement authorities to enhance security in an inherently interdependent area without internal borders. Together with the proposal for a Directive on information exchange between law enforcement authorities of Member States, this proposal contributes to the objectives of this strategy by ensuring that law enforcement authorities in one Member State have access to the same information that is available to their colleagues in another Member State.

The proposal comes within the wider landscape of the large-scale EU information systems that has developed substantially since the adoption of the Prüm framework. This includes the three EU central information systems that are in operation: the Schengen Information System (SIS), the Visa Information System (VIS) and the Eurodac system.[11] In addition, three new systems are currently in

[8] Council Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption (document 11227/18), https://data.consilium.europa.eu/doc/document/ST-11227-2018-INIT/en/pdf.

[9] Point (a) of Article 87(2) TFEU.

[10] Communication from the Commission to the European Parliament and the Council on a Strategy towards a fully functioning and resilient Schengen area, COM(2021)277 final (2.6.2021).

[11] The SIS assists competent authorities in the EU to preserve internal security in the absence of internal border checks and the VIS allows Schengen States to exchange visa data. The Eurodac system establishes an EU asylum

development phase: the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS) and the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN system).[12] All these current and future systems are linked through the interoperability framework for the EU information systems[13] for security, border and migration management, adopted in 2019, and which is currently being put in place. The revisions included in this proposal seek to align the Prüm framework with the interoperability framework, notably when it comes to the exchange of data and the overall architecture provided by the interoperability of EU information systems. This would provide for fast and controlled access to the information that law enforcement officers need to perform their tasks and for which they have access rights.

The SIS already contains alerts on missing persons and allows searches based on fingerprints. The SIS is a hit/no hit, actionable centralised information system directly accessible to a large number of frontline end-users containing alerts and providing immediate response on the spot, with actions to be taken related to the subject of the alert. The SIS is mostly used at police, border and custom checks, and by visa and immigration authorities in their routine procedures and checks.

In contrast, the Prüm framework does not have any central component/database at EU level and it is used only in criminal investigations. It allows other Member States to access the de-personalised sub-sets of national criminal DNA and fingerprint databases of all connected Member States. This access is granted to national contact points only. While the hit/no hit response is provided within seconds or minutes, it may take weeks or even months to receive the corresponding personal data related to the hit.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis of this proposal are the following provisions of the Treaty on the Functioning of the European Union (TFEU): Article 16(2), Article 87(2)(a) and Article 88(2).

Under Article 16(2), the Union has the power to adopt measures relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Under point (a) of Article 87(2), the Union has the power to adopt measures on the collection, storage, processing, analysis and exchange of relevant information to ensure police cooperation among Member States' competent authorities, including police, customs and other specialised enforcement services in relation to the prevention, detection and investigation of criminal offences. Under Article 88(2), the European Parliament and the Council can determine Europol's structure, operation, field of action and tasks.

• Subsidiarity

The improvement of information exchange among police and law enforcement authorities within the EU cannot be sufficiently achieved by Member States in isolation, owing to the cross-border nature of crime fighting and security issues. Member States must rely on one another in these matters.

---

fingerprint database enabling Member States to compare the fingerprints of asylum applicants in order to see whether they have previously applied for asylum or entered the EU irregularly via another Member State.

[12] The EES and ETIAS will strengthen security checks on visa-free travellers by enabling advance irregular migration and security vetting. The ECRIS-TCN system will address the identified gap in the exchange of information between Member States on convicted non-EU nationals.

[13] Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

Through several implementation projects at EU level,[14] Member States have tried to take action to address the shortcomings of the current Prüm framework.[15] Despite all these actions, many of the shortcomings remained the same as the ones described in the 2012 report on the implementation of the Prüm Decision.[16] This shows the need for EU action as measures implemented by Member States alone have not proved sufficient to address the limitations of the current Prüm framework.

Moreover, common EU level rules, standards and requirements facilitate information exchanges while providing compatibility between different national systems. This in turn allows for a certain level of automation in information exchange workflows that release law enforcement officers from labour-intensive manual activities.

- **Proportionality**

As explained in full detail in the impact assessment accompanying this proposed Regulation, the policy choices made in this proposal are considered proportionate. This is because they do not go beyond what is necessary to achieve the identified objectives.

The proposal envisages the creation of **central routers** (the Prüm II router and EPRIS) that would each act as a connecting point between Member States. This is a hybrid approach between a decentralised and centralised solution without any data storage at central level. It will imply that national databases in each Member State will all connect to the central router instead of connecting to one another. These routers would serve as message brokers forwarding search transactions and replies to national systems, without creating new data processes, enlarging access rights or replacing national databases. This approach would ensure that law enforcement authorities have fast and controlled access to the information that they need to perform their tasks, in line with their access rights. The router would facilitate the implementation by Member States of existing and future data exchanges in the context of the Prüm framework.

The **automated exchange of additional data categories**, such as facial images and police records, is crucial for effective criminal investigations and for identifying criminals. The introduction of these additional data categories would not lead to storing new categories of data as Member States already collect them under national law and store them in national databases. The exchange of these new data categories would constitute a new processing of data. However, it would be limited to the extent necessary to achieve its purpose and it would only allow for comparison of data in case-by-case situations. A set of several safeguards (e.g. sharing full data only if there is a "hit" following a query) are also foreseen in the proposal.

With this proposal, **Europol** will form an integral part of the Prüm framework, firstly by enabling Member States to automatically check third country-sourced biometric data held at Europol. Secondly, Europol could also check third country-sourced data against Member States' national databases. These two aspects of Europol's involvement in the new Prüm framework, in accordance with Europol's tasks as set out in Regulation (EU) 2016/794, would guarantee that no gaps occur in relation to data related to serious crime and terrorism received from third countries. In an open society in a globalised world, data provided by third countries on criminals and terrorists is crucial. It would allow for the potential identification of criminals known by countries outside the EU, while

[14] For instance, the Mobile Competence Team (MCT) project (2011–2014) was initiated by Germany and funded by the Commission's Prevention of and Fight against Crime programme (ISEC). The MCT aimed at providing expert knowledge and support to EU Member States which were not yet operational for DNA and fingerprint data exchange.

[15] Through a project led by Finland, Member States analysed the national procedures applied following a hit. The outcome of this project recommended a series of good and non-mandatory practices to streamline the post-hit information exchange throughout the EU (see document 14310/2/16 REV2, not public).
Moreover, Europol supported in 2012-2013 the development of standardized forms to be used for the follow-up information exchange, independently from the communication channel used (see document 9383/13 for more information). It is, however, not known to what extent National Contact Points use these forms.

[16] COM(2012) 732 final.

at the same time benefitting from strong safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals established in the Europol cooperation agreements with third countries.

The revised **hit-follow-up exchange process** would contribute to the internal security of the European Union by simplifying and streamlining the exchange of law enforcement information. Compared to the current situation where the exchange of information following a hit is governed by national law and is thereby subject to different rules and procedures, common rules harmonising this second step of the Prüm process would give predictability to all users, as they would all know what data they would get in this step. The exchange of data would be facilitated through partial automation, which means that human intervention would still be needed before any comprehensive follow-up data exchange can take place. Member States would retain ownership/control over their data.

- **Choice of the instrument**

A Regulation of the European Parliament and the Council is proposed. The proposed legislation builds on an existing framework of Council Decisions contributing to cross-border cooperation between EU Member States in the fields of justice and home affairs.[17]

In view of the need for the proposed measures to be directly applicable and uniformly applied across Member States, as well as to enhance the exchange of information, a Regulation is therefore the appropriate choice of legal instrument.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations of existing legislation**

Overall, the evaluation of the Prüm framework[18] showed that searching and comparing DNA, fingerprint and vehicle registration data in other Member States' databases for the prevention and investigation of criminal offences, are of paramount importance for safeguarding the internal security of the EU and the safety of its citizens. The evaluation further demonstrated that the Prüm Decisions have helped to establish common EU level rules, standards and requirements, to facilitate information exchange and provide compatibility between different national systems.

However, since the expiration of the deadline for the implementation of the Prüm framework ten years ago, the EU has adopted several other measures on the facilitation of the exchange of information between law enforcement authorities,[19] including the interoperability framework.[20] Additionally, provisions on the technical specifications of queries, security measures and communication have not been updated since the adoption of the Prüm Decisions in 2008.[21] Some of

[17] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA.

[18] Annex 4 to the accompanying Staff Working Document [Prüm impact assessment reference].

[19] Such as the Europol Information system (EIS), Interpol's information systems and the Schengen Information System (SIS).

[20] 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;
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.

[21] Contained in Council Decision 2008/616/JHA.

these rules are outdated as forensic science and technology have significantly developed in the past decade.

The evaluation also found that the implementation of the Prüm Decisions in the past ten years has been slow and that not all Member States have taken the necessary steps to implement the Decisions.[22] As a consequence, a number of bilateral connections have not been established, and queries cannot be launched to some Member States' databases. Findings of the evaluation also showed that the follow-up to hits occurs based on national law and therefore falls outside the scope of the Prüm Decisions. Differences in national rules and procedures can cause, in several instances, significant time-lags for competent authorities to receive information following a hit. This state of play affects the functioning of the Prüm system as well as the effective exchange of information between Member States by decreasing the possibility that criminals are identified, and cross-border links between crimes are detected.

The findings of the evaluation supported the preparation of the impact assessment and of this proposal.

- **Stakeholder consultations**

The preparation of this proposal involved targeted consultations of concerned stakeholders, including end-users of the system, namely Member States' authorities using the Prüm automated data exchange ranging from law enforcement and judicial authorities, national vehicle registration authorities, to national database custodians and forensic laboratories. Europol and eu-LISA were also consulted in view of their respective expertise and their potential role in the new Prüm framework.

The FRA, as well as non-governmental organisations such as EDRi (European Digital Rights) and intergovernmental organisations (Eucaris – European car and driving licence information systems) also provided input in light of their expertise.

Consultation activities in the context of the preparation of the impact assessment underpinning this proposal gathered feedback from stakeholders in various fora. These activities included notably an inception impact assessment, a public consultation and a series of technical workshops. A feasibility study was conducted based on desk research, interviews with subject matter experts, questionnaires and three expert workshops, and examined the feasibility of improving information exchange under the Prüm Decisions.

Regular discussions on law enforcement information exchange and specifically on the Prüm Decisions in the Council Working Party DAPIX/IXIM[23] also contributed to preparing this proposal.

An **inception impact assessment** was published for feedback from August to October 2020, with a total of six contributions received.[24]

A **public consultation** advertised on the European Commission's website targeted the general public. Replies confirmed that the existing Prüm framework is relevant for the prevention and investigation of criminal offences, and has improved the exchange of data between Member States' law enforcement authorities. By preventing the need to query each Member State bilaterally, the automated data exchange under the Prüm framework has also brought efficiency gains. Replies

[22] The Commission launched infringement proceedings against five Member States in 2016. As of October 2021, two of these infringement cases are still open.

[23] Council Working Party on Information Exchange and Data Protection (DAPIX), and as from 1 January 2020, Working Party on Justice and Home Affairs Information Exchange (IXIM).

[24] The inception impact assessment and contributions are available here.

further confirmed the coherence of the framework with EU and international actions in this field, and that it has added-value compared to what Member States could achieve in the field of law enforcement information exchange in the absence of the Prüm framework. In terms of strengthening the current framework, most respondents agreed that the fact that some data categories are not covered by the framework and are therefore exchanged by sending manual queries is a shortcoming.

The Commission's services also organised a series of targeted informal **technical workshops** with experts from Member States and Schengen Associated Countries. The workshops aimed at bringing together end-users for an exchange of views on the options, which were being envisaged and assessed to strengthen the Prüm framework, from a technical perspective.

The accompanying impact assessment sets out a more detailed description of the stakeholder consultation (Annex 2).

- **Impact assessment**

The proposal is supported by an impact assessment as presented in the accompanying Staff Working Document [Prüm impact assessment reference]. The Regulatory Scrutiny Board reviewed the draft impact assessment at its meeting of 14 July 2021 and delivered its positive opinion on 16 July 2021.

The impact assessment concluded that:

(1) To meet the objective of providing a technical solution for efficient automated exchange of data, a hybrid solution between a decentralised and a centralised approach without data storage at central level should be applied.

(2) To meet the objective of ensuring that more relevant data (in terms of data categories) is available to law enforcement authorities, the exchange of facial images and police records should be introduced.

(3) To meet the objective of ensuring that relevant data from Europol's databases is available to law enforcement authorities, Member States should be able to check automatically third country-sourced biometric data at Europol as part of the Prüm framework. Europol should also be able to check third country-sourced data against Member States' national databases.

(4) To meet the objective of providing efficient access to the actual data corresponding to a 'hit' that is available in the national database of another Member State or at Europol, the follow-up process should be regulated at EU level with a semi-automated exchange of the actual data corresponding to a 'hit'.

The major positive impact of this proposal will be to respond effectively to the identified problems and reinforce the current Prüm framework with targeted and strong additional capabilities to step up its support to Member States in reinforcing information exchange with the final objective of preventing and investigating criminal and terrorist offences, in full compliance with fundamental rights.

The ultimate beneficiaries of all preferred options are the citizens, who will directly and indirectly benefit from better crime fighting and lower crime rates. In terms of efficiency, the main beneficiaries are national law enforcement authorities.

The immediate financial and economic impacts of the proposal will require investments at both EU and Member States' level. It is expected that the projected investments costs will be outweighed by benefits and savings, notably at the Member States' level. Despite the initial investments, the creation of the central Prüm router will save costs for Member States as the router would not require

each Member State to create (and maintain) as many connections as there are Member States and data categories.

- **Fundamental rights**

In accordance with the EU Charter of Fundamental Rights, to which EU institutions and Member States are bound when they implement EU law (Article 51(1) of the Charter), and with the principle of non-discrimination, the opportunities offered by the options presented need to be balanced with the obligation to ensure that interferences with fundamental rights that may derive from them are limited to what is strictly necessary to genuinely meet the objectives of general interest pursued, subject to the principle of proportionality (Article 52(1) of the Charter).

The proposed solutions offer the opportunity to adopt targeted preventive measures to enhance security. As such, they can contribute pursue the legitimate objective of facilitating the fight against crime, which also implies a positive obligation on authorities to take preventive operational measures to protect an individual whose life is at risk, if they know or ought to have known of the existence of an immediate risk.[25]

- **Protection of personal data**

Exchange of information has an impact on the right to the protection of personal data. This right is established by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union, and in Article 8 of the European Convention on Human Rights. As underlined by the Court of Justice of the EU,[26] the right to the protection of personal data is not an absolute right but must be considered in relation to its function in society. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter.

As regards Prüm, the applicable data protection legislation is Directive (EU) 2016/680. Indeed, the Prüm framework provides for processing of personal data carried out in the context of the exchange of information between law enforcement authorities responsible for the prevention and investigation of criminal offences.

The free movement of data within the EU is not to be restricted for reasons of data protection. However, a series of principles must be met. Indeed, to be lawful, any limitation on the exercise of the fundamental rights protected by the Charter must comply with the following criteria, laid down in its Article 52(1):

(1) it must be provided for by law;

(2) it must respect the essence of the rights;

(3) it must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;

(4) it must be necessary; and

(5) it must be proportional.

This proposal embeds all these data protection rules, as set out in full detail in the impact assessment accompanying this proposed Regulation. The proposal is based on the principles of data protection by design and by default. It includes all appropriate provisions limiting data processing to what is necessary for the specific purpose and granting data access only to those entities that

[25] European Court of Human Rights, Osman v United Kingdom, No. 87/1997/871/1083, 28 October 1998, para. 116.

[26] Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.

'need to know'. Access to data is reserved exclusively for duly authorised staff of Member States' authorities or EU bodies that are competent for the specific purposes of the revised Prüm framework and limited to the extent that the data are required for the performance of tasks in accordance with these purposes.

The Commission will, at the time of publishing the report assessing the effect given to [Council Recommendation on operational police cooperation] by the Member States referred to under point 9(d) of that Recommendation, decide whether there is a need for EU legislation on cross-border operational police cooperation. Should there be a need for such legislation, the Commission will make a legislative proposal on cross-border operational police cooperation, which will also ensure the alignment of the provisions of Decision 2008/615/JHA and Decision 2008/616/JHA which were not covered under this proposal with Directive 2016/680, in line with the results of the assessment under Article 62(6) of Directive 2016/680. Should there not be a need for EU legislation on cross-border operational police cooperation, the Commission will make a legislative proposal to ensure this same alignment, in line with the results of the assessment under Article 62(6) of Directive 2016/680.

4. BUDGETARY IMPLICATIONS

This legislative initiative would have an impact on the budget and staff needs of eu-LISA and Europol.

For eu-LISA, it is estimated that an additional budget of around EUR 16 million and around 10 additional posts would be needed for the overall MFF period to ensure that eu-LISA has the necessary resources to enforce the tasks attributed to the Agency in this proposed Regulation. The budget allocated to eu-LISA will be offset against the BMVI.

For Europol, it is estimated that an additional budget of around EUR 7 million and around 5 additional posts would be needed for the overall MFF period to ensure that Europol has the necessary resources to enforce the tasks attributed to the Agency in this proposed Regulation. The budget allocated to Europol will be offset against the ISF.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will ensure that the necessary arrangements are in place to monitor the functioning of the measures proposed and evaluate them against the main policy objectives. Two years after the new functionalities are put in place and operating, and every two years thereafter, Union Agencies should submit to the European Parliament, the Council and the Commission a report on the technical functioning of the new proposed measures. In addition, three years after the new functionalities are put in place and operating, and every four years thereafter, the Commission should produce an overall evaluation of the measures, including on any direct or indirect impact on fundamental rights. It should examine results achieved against objectives and assess the continuing validity of the underlying rationale and any implications for future options. The Commission should submit the evaluation reports to the European Parliament and the Council.

- **Detailed explanation of the specific provisions of the proposal**

Chapter 1 sets out the general provisions for this Regulation with its subject matter, purpose and scope. It provides a list of definitions and recalls that the processing of personal data for the purposes of this Regulation shall respect the principle of non-discrimination and other fundamental rights.

Chapter 2 sets out the provisions for the exchange of the categories of data under this Regulation, namely the exchange of DNA profiles, dactyloscopic data, vehicle registration data, facial images

and police records. The principles for the exchange, the automated search of data, the rules for requests and answers are detailed in a separate section for each category of data respectively. Chapter 2 also contains common provisions for the exchange of data, the setting up of national contact points and implementing measure.

Chapter 3 sets out the details for the new (technical) architecture for the exchange of data. The first section of this chapter includes provisions describing the central router, the use of the router and the launching of queries. Implementing acts will be needed to specify the technical procedures for these queries. This section also includes provisions on the interoperability between the router and the Common Identity Repository for the purposes of law enforcement access, the keeping of logs of all data processing operations in the router, the quality check and the notification procedures in case of technical impossibility to use the router. A second section provides details on the use of the European Police Records Index System (EPRIS) for the exchange of police records. This section also includes provisions on the keeping of logs of all data processing operations in EPRIS, and the notification procedures in case of technical impossibility to use EPRIS.

Chapter 4 sets out the processes for exchange of data following a match. It includes a provision on the automated exchange of core data, with data limited to what is necessary to enable the identification of the individual concerned, and a provision on the exchange of data at any stage of the process under this Regulation which is not explicitly described under this Regulation.

Chapter 5 contains provisions on the access by Member States to third country-sourced biometric data stored by Europol and on the access by Europol to data stored in Member States' databases.

Chapter 6 on data protection contains provisions ensuring that data under this Regulation are processed lawfully and appropriately, in line with the provisions of 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.[27] It explains who the data processor will be for the processing of data pursuant to this Regulation. It sets out measures required from eu-LISA and Member States' authorities to ensure the security of data processing, the appropriate handling of security incidents and the monitoring of compliance with the measures in this Regulation. The chapter also sets out the provisions relating to supervision and audit in relation to data protection. It underlines the principle that data processed under this Regulation shall not be transferred or made available to any third country or international organisation in an automated manner.

Chapter 7 details the responsibilities of Member States, Europol, and eu-LISA respectively in the implementation of the measures in this Regulation.

Chapter 8 concerns amendments to other existing instruments, namely Decisions 2008/615/JHA and 2008/616/JHA, Regulation (EU) 2018/1726, Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

Chapter 9 on final provisions sets out the details relating to reporting and statistics, costs, notifications, transitional provisions and derogations. It also sets out the requirements for the start of operations of the measures proposed under this Regulation. The chapter also provides for the setting up of a committee and the adoption of a practical handbook to support implementation and management of this Regulation. It also includes a provision on monitoring and evaluation and a provision on the entry into force and applicability of this Regulation. Notably, this Regulation replaces Articles 2 to 6 and Sections 2 and 3 of Chapter 2 of Council Decision 2008/615/JHA and Chapters 2 to 5 and Articles 18, 20 and 21 of Council Decision 2008/616/JHA which will

[27] Following the Commission's findings in its Communication of 24 June 2020 on the way forward on aligning the former third pillar acquis with data protection rules (COM(2020) 262 final).

consequently be deleted from those Council Decisions from the date of application of this Regulation. The effect of those amendments will be that the replaced and deleted provisions no longer apply to any Member State.

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 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[28],

Having regard to the opinion of the Committee of the Regions[29],

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.

(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[30] (Europol) as the Union criminal information hub.

(4) Council Decisions 2008/615/JHA[31] and 2008/616/JHA[32] 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.

[28] OJ C , , p. .
[29] OJ C , , p. .
[30] 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).
[31] 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).
[32] 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).

(5) This Regulation should lay down the conditions and procedures for the automated transfer of DNA profiles, dactyloscopic data, vehicle registration 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.

(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.

(7) By providing for the automated search or comparison of DNA profiles, dactyloscopic data, vehicle registration data, facial images and police records, the purpose of this Regulation is also to allow for the search of missing persons and unidentified human remains. 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.[33]

(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*].

(9) For the automated searching of vehicle registration 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.

(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

[33] 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).

query other Member States' databases if they do not make their own data available for queries by other Member States.

(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 is necessary for better prevention and investigation of criminal offences. It also contributes to building synergies between different law enforcement tools.

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

(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[34] and Article 6 of Regulation (EU) 2019/818 of the European Parliament and of the Council[35] 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.

(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, the requested Member State should return a limited set of core data via the router within 24 hours. 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.

---

[34] 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).

[35] 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).

(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. Any automated exchange of data in accordance with this Regulation should use the UMF standard. 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.

(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.[36]

(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[37] (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.

(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

---

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

[37] 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).

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[38] and delivered an opinion on [XX][39].

HAVE ADOPTED THIS REGULATION:

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 the rules regarding the exchange of core data following a match.

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 5 of the Treaty on the Functioning of the European Union, 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 missing persons and unidentified human remains by authorities responsible for the prevention, detection and investigation of criminal offences.

Article 3

Scope

This Regulation applies to the national databases used for the automated transfer of the categories of DNA profiles, dactyloscopic data, facial images, police records and certain vehicle registration data.

Article 4

Definitions

[38] 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).

[39] [OJ C …].

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

(1) ‘loci’ means the particular molecular structure at the various DNA locations;

(2) ‘DNA profile’ means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, the particular molecular structure at the various 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 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;

(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;

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

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

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

(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 any information available in the national 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 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[40];

[40] 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

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

(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[41] [*proposal NIS 2*].

CHAPTER 2

EXCHANGE OF DATA

SECTION 1

DNA profiles

Article 5

Establishment of national DNA analysis files

1. Member States shall open and keep national DNA analysis files for the investigation of criminal offences.

Processing of 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 DNA analysis files as referred to in paragraph 1.

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

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

Article 6

Automated searching of DNA profiles

1. Member States shall 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 DNA profiles 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.

---

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).

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

2. Should an automated search show that a supplied DNA profile matches DNA profiles entered in the requested Member State's searched file, 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. The national contact point of the requesting Member State shall confirm a match of DNA profiles data with DNA reference data held by the requested Member State following the automated supply of the DNA reference data required for confirming a match.

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

Reporting about DNA analysis files

Each Member State shall inform the Commission and eu-LISA of the national DNA analysis files, to which Articles 5 to 7 apply, 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 Articles 47 and 48;

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

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

Article 10

Principles of DNA reference data exchange

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 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 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 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 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 declarations sent pursuant to Article 8. Those 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 national automated fingerprint identification systems established for the prevention, detection and investigation of criminal offences.

2. Dactyloscopic reference data shall not contain any 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 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 confirm a match of dactyloscopic data with dactyloscopic reference data held by the requested Member State following the automated supply of the dactyloscopic reference data required for confirming a match.

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 Articles 47 and 48;

(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 shall be carried out in accordance with a uniform data format. The Commission shall adopt implementing acts to specify the uniform data format in accordance with the procedure referred to in Article 76(2).

2. Each Member State shall ensure that the dactyloscopic data it transmits are of sufficient quality for a comparison by the automated fingerprint identification systems.

3. Member States 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 shall ensure that its search requests do not exceed the search capacities specified by the requested Member State.

Member States shall inform the Commission 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.

2. The Commission shall adopt implementing acts to specify the maximum numbers of candidates accepted for comparison per transmission 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.

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 operators;

(b) data relating to vehicles.

2. Searches may be conducted only with a full chassis number or a full registration number.

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 to 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 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 one year 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

1. Member States shall ensure the availability of facial images from their national databases 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.

Member States shall not make available in this context any data from which an individual can be directly identified.

2. Facial images which are not attributed to any individual (unidentified facial images) 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 facial images stored in their national databases, 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 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 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 Articles 47 and 48;

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

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.

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 from their national police records indexes established for the investigation of criminal offences. This set of data, if available, shall contain the following data:

(a) first name(s);

(b) family name(s);

(c) 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), (c), (e) and (f) shall be pseudonymised.

Article 26

Automated searching of police records

1. For the investigation of criminal offences, Member States shall allow national contact points of other 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 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 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 Articles 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 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.

SECTION 6

Common provisions

Article 29

National contact points

Each Member State shall designate a national contact point.

The national contact points shall be responsible for supplying the data referred to in Articles 6, 7, 13, 18, 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, 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, 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, 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 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 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;

(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 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 one year 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 shall be used in the development of the router referred to in Article 35 and EPRIS.

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

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, retrieving 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 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

1. The router users referred to in Article 36 shall request a query by submitting biometric data to the router. The router shall dispatch the request for a query to the 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 the replies in accordance with the score of the correspondence between the biometric data used for querying and the biometric data stored in the Member States' databases and 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 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 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 year 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 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 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 police records 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 central infrastructure, including a search tool enabling the simultaneous querying of Member States' databases;

(b) 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, 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) 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 points (a), (b) and (c) of paragraph 2 used for queries shall be pseudonymised.

Article 44

Queries

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 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 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 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. Europol shall keep logs of all data processing operations in EPRIS. 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 to which a request for a query was sent;

(e) the national databases that provided an answer.

2. Each 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 year 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 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.

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 third country-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 to data stored in Member States' databases

1. Europol shall, in accordance with Regulation (EU) 2016/794, have access to data, which are stored by Member States in their national databases 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 as a search criterion shall be carried out using Eucaris.

4. Europol queries performed with police records as a search criterion shall be carried out using EPRIS.

5. Europol shall carry out the searches in accordance with paragraph 1 only when carrying out its tasks referred to in Regulation (EU) 2016/794.

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), and upon confirmation of that match by Europol, the requested Member State shall decide whether to 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.

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 database 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

1. Processing of personal data by the requesting Member State or Europol shall be permitted solely for the purposes for which the data have been supplied by the requested Member State in accordance with this Regulation. Processing for other purposes shall be permitted solely with the prior authorisation of the requested Member State.

2. Processing of data supplied pursuant to Articles 6, 7, 13, 18 or 22 by the searching or comparing Member State shall be permitted solely in order to:

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

(b) prepare and submit a police request for legal assistance if those data match;

(c) logging within the meaning of Articles 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 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 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 shall ensure the accuracy and current relevance of personal data. 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. All requesting Member States 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 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;

(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 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 instead of being deleted. Blocked data may be supplied or used 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 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.

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

Without prejudice to Article 34 of Regulation (EU) 2016/794, 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 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 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 to comply with its obligations under this Regulation causes damage to the router or EPRIS, that Member State 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 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.

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) 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[42], 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 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 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.

   Therefore, Articles 2 to 6 and Sections 2 and 3 of Chapter 2 of Decision 2008/615/JHA are deleted from the date of application of the provisions of this Regulation related to the router as set out in Article 74.

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.

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

* 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.'

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 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(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(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.

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 paragraphs.

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).

3. Member States shall notify the Commission, Europol and eu-LISA of the national contact points.

Article 74

Start of operations

1. The Commission shall determine the date from which the Member States and the Union agencies may start using 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 must start using 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 must 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).

2. The Commission shall determine the date from which the Member States and the Union agencies 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 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 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 of data.

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*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE LEGISLATIVE INITIATIVE

1.1. Title of the legislative initiative

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, Regulation (EU) 2019/817 and Regulation (EU) 2019/818 of the European Parliament and of the Council

1.2. Policy area(s) concerned

Policy area: Home Affairs

Activity: Security

1.3. The proposal relates to

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[43]

☒ **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

In response to pressing operational needs, and calls from the Council to consider revising the Prüm Decisions[44] with a view to broadening their scope and to updating the necessary technical and legal requirements, this initiative is expected to strenghthen the automated data exchange under the Prüm framework to help Member States' law enforcement authorities fighting crime.

1.4.2. Specific objective(s)

The initiative seeks to achieve the following objectives:

1) **Specific objective I:** Providing a technical solution for efficient automated exchange of data between EU law enforcement authorities to make them aware of relevant data that is available in the national database of another Member State;

2) **Specific objective II:** Ensuring that more relevant data (namely facial images and police records) from national databases in other Member States is available to all competent EU law enforcement authorities;

3) **Specific objective III:** Ensuring that relevant data (in terms of sources of data) from Europol's database is available to national law enforcement authorities and that Europol uses its data to its full potential;

[43] As referred to in Article 58(2)(a) or (b) of the Financial Regulation.

[44] Council Decisions 2008/615/JHA and 2008/616/JHA

4) **Specific objective IV:** Providing law enforcement authorities with efficient access to the actual data corresponding to a 'hit' that is available in the national database of another Member State or at Europol.

1.4.3. *Expected result(s) and impact*

Specify the effects which the legislative initiative should have on the beneficiaries/groups targeted.

The initiative will effectively address the identified problems and reinforce the current Prüm framework with targeted and strong additional capabilities to step up its support to Member States in reinforcing information exchange, with the final objective of preventing and investigating criminal and terrorist offences, in full compliance with fundamental rights.

The ultimate beneficiaries of all preferred options are the **citizens**, who will directly and indirectly benefit from **better crime fighting and lower crime rates**. In terms of efficiency, the main beneficiaries are **national law enforcement authorities**. The initiative provides for efficient solutions to challenges which would otherwise have to be addressed at higher costs or which would be less efficient.

1.4.4. *Indicators of performance*

Specify the indicators for monitoring progress and achievements.

The development of the router and EPRIS will start once the prerequisites are fulfilled i.e. the legal proposal is adopted by the co-legislators and the technical prerequisites fulfilled. While the work on the router starts as a new project, the work on EPRIS should build on the current ADEP.EPRIS project.

Specific objective: ready for operations by the target due date

By 2023, the proposal is sent to the co-legislators for their adoption. The assumption is made that the adoption process will be completed during 2024 by analogy with the time taken for other proposals.

Under this assumption, the start of the development period is set at the beginning of 2025 (= T0) in order to have a reference point from where durations are counted and not absolute dates. If adoption by co-legislators occurs at a later date, the schedule shifts accordingly.

The development of the router and EPRIS is assumed to take place during 2025 and 2026, with the start of operations planned in 2027.

The following main indicators will allow the monitoring of the implementation and performance of the specific objectives:

Specific objective I: Providing a technical solution for efficient automated exchange of data.

- The number of use cases executed (= number of requests for queries that can be handled by the router) per time period.

- The number of use cases executed (= number of requests for queries that can be handled by EPRIS) per time period.

Specific objective II: ensuring more relevant data is available

- Number of requests for querying with facial images
- Number of requests for querying with police records
- Number of matches following queries with facial images
- Number of matches following queries with police records

Specific objective III: Ensuring that relevant data (in terms of sources of data) from Europol's database is available to national law enforcement authorities and that Europol uses its data to its full potential.

- Number of requests for querying third country sourced Europol biometric data
- Number of matches agaisnt third country sourced Europol biometric data
- Number of requests for querying issued by Europol
- Number of matches resulting from queries issued by Europol

Specific objective IV: Providing law enforcement authorities with efficient access to the actual data corresponding to a 'hit' that is available in the national database of another Member State or at Europol.

- Number of matches following requests for queries compared to number of times the exchange of core data was requested

1.5. Grounds for the legislative initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the legislative initiative

The roll-out of the implementation of the legislative initiative requires technical and procedural measures at EU and national level, which should start implementation when the revised legislation enters into force. The relevant resources – in particular human resources - should be scaled up over time in line with the measures.

The main requirements following entry into force of the proposal are as follows:

To create the Prüm router:

To meet the objective of providing Prüm II users with a single connection to all Member States databases and Europol data to send requests for querying with biometric data.

To provide for a new follow-up process at EU level with a semi-automated exchange of actual data corresponding to a 'hit'.

To create/enlarge EPRIS

To meet the objective of providing Prüm II users with a single connection to all participating Member States databases containing police records to send requests for querying with police records.

To enable Member States to exchange new categories of data

To allow exchange of facial images and police records via Prüm II.

To enable Member States to check automatically third-country sourced data at Europol as part of the Prüm framework:

To allow Member States to check third country sourced biometric data via Prüm II.

To enable Europol to check third-country sourced data against the national databases of Member States:

To allow Europol to use third-country sourced data to search Member States' databases via Prüm II.

Since all objectives must be met, the complete solution is a combination of the above.

1.5.2. *Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.*

Serious crime and terrorism are of a transnational nature. Therefore, action at national level alone cannot counter them effectively. This is why Member States choose to work together within the framework of the EU to tackle the threats posed by serious crime and terrorism.

Moreover, evolving security threats, driven by the different ways criminals exploit the advantages that the digital transformation, globalisation and mobility bring about, also call for effective EU level support to the work of national law enforcement authorities. EU action provides for an effective and efficient way to step up the support to Member States in fighting serious crime and terrorism in order to cope with these evolving threats.

The proposal will create significant economies of scale by shifting the tasks and services that can be performed more efficiently at the EU level from the national level to Europol. The proposal therefore provides for efficient solutions to challenges, which would otherwise have to be addressed at higher costs by means of 27 individual national solutions, or to challenges which cannot be addressed at the national level at all in view of their transnational nature.

1.5.3. *Lessons learned from similar experiences in the past*

The evaluation of the Prüm Decisions showed that:

- The Prüm framework is relevant in view of current and future needs and challenges related to security and more precisely criminal investigations. Cooperation and exchange of information between Member States' law enforcement authorities, and the possibility to search and compare DNA, fingerprint and vehicle registration data in other Member States' databases for the prevention and investigation of criminal offences, are deemed to be of paramount importance for safeguarding the internal security of the EU and the safety of its citizens.

- The concept of the Prüm Decisions meet the needs of criminal investigators, of victims of crime, of forensic specialists, of database custodians and of legal practitioners regarding the categories of data that are available in the framework.

- By preventing the need to query each Member State bilaterally, the automated data exchange under the Prüm framework brings efficiency gains in the law enforcement information exchange to the extent that it improves the speed of exchanges and decreases the administrative burden to a certain extent. It has been found that these benefits outweigh the investment required for the implementation of the Prüm framework. Moreover, the automated Prüm system provides substantial savings in working time. However, there is still an administrative burden related to the verification of hits and reporting, and also to receipt/transmission of second-step information.

- Considerable developments and changes have also materialized in terms of the EU legal framework, operational needs, and technical and forensic possibilities since the adoption of the Prüm Decisions in 2008. Several EU and international initiatives and systems aiming at facilitating the exchange of information between law enforcement authorities have been developed. There are mostly complementarities between the Prüm Decisions and other relevant EU/international legislation, including the interoperability framework. There are also

complementarities with some of the EU central information systems that have different purposes. Potential synergies can be identified regarding Europol and the interoperability framework.

- However, the implementation of the Prüm Decisions has been slow. Indeed, nearly ten years after the implementation deadline of 26 August 2011, all Member States have not completed the evaluation procedure and a number of bilateral connections have not been established due to the technical complexity and the important financial and human resources entailed. As a consequence, queries cannot be checked against the data in some Member States if the relevant bilateral connection has not been established. This hampers the capacity to identify criminals and detect cross-border links between crimes, which hinders the exchange of information and the functioning of the Prüm system.

- The fact that the follow-up to hits under the Prüm framework takes place under national law and therefore outside the scope of the Prüm Decisions has also been raised as an issue that hinders the functioning of the Prüm system. Indeed, due to differences in national rules and procedures, the exchange of hit follow-up data is fragmented to the extent that it sometimes takes weeks or even months to receive the relevant information behind a hit.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The investments required at EU level are compatible with the 2021-2027 multiannual financial framework, with funding provided under heading Security and Defence and heading Migration and Borders.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The appropriations needed to finance the development of the Prüm II framework have not been planned under the Europol and eu-LISA MFF allocations, as this is a new proposal for which amounts were not known at the time of the proposal. It is proposed to increase Europol's and eu-LISA's allocations in years 2024, 2025, 2026 and 2027 by corresponding reductions in the Internal Security Fund (ISF) and the Border Management and Visa Policy Instrument (BMVI), respectively.

1.6. Duration and financial impact of the legislative initiative

☐ **limited duration**

☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY

☒ **unlimited duration**

Implementation with a start-up period from 2024 to 2026

followed by full-scale operation.

1.7. Management mode(s) planned[45]

☒ **Direct management** by the Commission

– X by its departments, including by its staff in the Union delegations;

– ☐ by executive agencies

☒ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 70 and 71;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

Comments

Blocks	Development phase	Operations phase	Management mode	Actor
Development and maintenance (of the router and EPRIS)	X	X	Indirect	eu-LISA Europol
Adaptation of the Europol databases	X	X	Indirect	Europol

[45] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Blocks	Development phase	Operations phase	Management mode	Actor
Development or improvements to existing national databases, integration of national systems	X	X	Shared (or direct)	COM + Member States

The development period starts from 2024 and lasts till the delivery of each part of the intiative, running from 2024 to 2027.

1. Direct management by DG HOME: During the development period, if necessary, actions may also be implemented directly by the Commission. This could include, in particular, Union financial support for activities in the form of grants (including to Member State national authorities), public procurement contracts and/or reimbursement of costs incurred by external experts.

2. Shared management: During the development phase, Member States will be required to adapt their national systems in order to connect to the router and EPRIS as well as provide for the necessary measures to ensure exchanges of facial images and police records.

3. Indirect management: eu-LISA and Europol will cover the development part of the IT strands of the project, i.e. the router and EPRIS respectively. This would include any necessary changes to their existing architecture to ensure the capabilities described in the proposal.

During the period of operations, eu-LISA and Europol will execute all technical activities linked to the maintenance of the router and EPRIS respectively.

Europol will cover the development and maintenance of its systems to ensure that their data is available in the context of the Prüm framework.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

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

No later than one year after the adoption of the proposed Regulation, and every year thereafter during the development phase of the router, eu-LISA shall submit a report to the European Parliament and to the Council on the state of play of the development of the router. The 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.

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 were achieved, in particular relating to planning and costs, as well as justifying any divergences.

No later than one year after adoption of the proposed 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 on any risks which may impact the overall costs to be borne by the general budget of the Union.

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 were achieved, in particular relating to planning and costs, as well as justifying any divergences.

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

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.

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 the router, including the security thereof.

Three years after the start of operations of all elements of the proposed Regulation 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.

The Member States and Europol shall provide eu-LISA and the Commission with the information necessary to draft the above mentioned reports. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

The Member States shall provide Europol and the Commission with the information necessary to draft the above mentioned reports. This information shall not jeopardise working methods or include information that reveals sources, staff members or investigations of the designated authorities.

eu-LISA and Europol shall provide the Commission with the information necessary to produce its evaluations.

2.2. Management and control system(s)

2.2.1. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The following risks are identified:

- strained operational resources due to increasing data flows and constantly evolving criminal activities landscape

- to multiplication of tasks and requests for both eu-LISA and Europol

- lack of adequate levels of financial and human resources to match operational needs

- lack of ICT resources, resulting in delays in necessary core system developments and updates

- risks related to Europol's processing of personal data and the need to regularly evaluate and adapt procedural and technical safeguards in order to ensure the protection of personal data and fundamental rights.

- dependencies between the preparations to be done by eu-LISA with regard to the router and the preparations to be done by Member States and Europol with regard to setting up a technical interface to transmit data via the router

These risks can be mitigated by applying project management techniques, including contingency in development projects and staffing sufficiently in order to be able to absorb peaks of work. Estimation of effort is indeed usually done by assuming an even workload spread over time while the reality of projects is of uneven workloads that are absorbed by higher resource allocations.

There are several risks related to the use of an external contractor for this development work, in particular:

1. the risk that the contractor fails to allocate sufficient resources to the project or that it designs and develops a system that is not state of the art;

2. the risk that administrative techniques and methods to IT projects are not fully respected as a way of reducing costs by the contractor;

3. the risk of the contractor facing financial difficulties for reasons external to this project.

These risks are mitigated by awarding contracts on the basis of strong quality criteria, verifying contractors' references and maintaining a close relationship with them. Finally, as a last resort, strict penalty and termination clauses can be included and applied when required.

Europol implements a specific Internal Control Framework based on the Internal Control Framework of the European Commission and on the original Committee of Sponsoring Organisations' integrated internal control framework. The Single Programming Document must provide information on the internal control systems, while the Consolidated Annual Activity Report (CAAR) must contain information on the efficiency and effectiveness of the internal control systems, includind as regards risk assessment. The CAAR 2019 reports that, based on the analysis of the internal control components and principles which have been monitored in the course of 2019, using both quantitative and qualitative elements, the Europol Internal Control System is assessed as present and functioning in an integrated manner across the agency.

For the budget implemented by eu-LISA, a specific Internal Control Framework based on the Internal Control Framework of the European Commission is required. The Single Programming Document must provide information on the internal control systems, while the Consolidated Annual Activity Report (CAAR) must contain information on the efficiency and effectiveness of the internal control systems, including as regards risk assessment. The CAAR 2019 reports that, management of the Agency has reasonable assurance that appropriate internal controls are in place and that they are functioning as intended. Throughout the year, the major risks were appropriately identified and managed. This assurance is further confirmed by the results of the internal and external audits performed.

For both Europol and eu-LISA, an additional level of internal supervision is also provided by Europol's Internal Audit Capability, on the basis of an annual audit plan, notably taking into consideration the assessment of risks in Europol. The Internal Audit Capability helps Europol in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate the effectiveness of risk management, control, and governance processes, and by issuing recommendations for their improvement.

Moroever, the European Data Protection Supervisor (EDPS) and the data protection officer in both agencies (an independent function attached directly to the Mangement Board Secretariat) supervise the processing of personal data by the agencies.

Finally, as partner DG of Europol and eu-LISA, DG HOME runs an annual risk management exercise to identify and assess potential high risks related to agencies' operations. Risks considered as critical are reported annually in DG HOME management plan and are accompanied by an action plan stating the mitigating action.

2.2.2. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The ratio of "control costs/value of the related funds managed" is reported on by the Commission. The 2020 AAR of DG HOME reports 0.21% for this ratio in relation to Indirect Management Entrusted Entities and Decentralised Agencies, including Europol and eu-LISA.

The European Court of Auditors confirmed the legality and regularity of both Europol's and eu-LISA's annual accounts for 2019, which implies an error rate below 2%. There are no indications that the error rate will worsen in the coming years.

Moreover, for both Europol and eu-LISA, article 80 of their respective Financial Regulation provides for the possibility for the agency to share an internal audit capability with other Union bodies functioning in the same policy area if the internal audit capability of a single Union body is not cost-effective.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The measures envisaged to combat fraud are laid down in Article 35 of Regulation (EU) 1077/2011.

The measures related to combating fraud, corruption and any other illegal activities are outlined, inter alia, in article 66 of Europol's Regulation and under Title X of Europol's Financial Regulation.

Europol shall notably participate in fraud prevention activities of the European Anti-fraud Office and inform the Commission without delay on cases of presumed fraud and other financial irregularities – in line with its internal anti-fraud strategy.

An update to the Europol anti-fraud strategy was adopted by the Management Board in 2020.

The measures related to combating fraud, corruption and any other illegal activities are outlined, inter alia, in article 50 of eu-LISA's Regulation and under Title X of eu-LISA's Financial Regulation.

eu-LISA shall notably participate in fraud prevention activities of the European Anti-fraud Office and inform the Commission without delay on cases of presumed fraud and other financial irregularities – in line with its internal anti-fraud strategy.

Moreover, as partner DG, DG HOME has developed and implemented its own anti-fraud strategy on the basis of the methodology provided by OLAF. Decentralised agencies, including Europol and eu-LISA, fall within the scope of the strategy. DG HOME 2020 AAR concluded that the fraud prevention and detection processes worked satisfactorily and therefore contributed to the assurance on the achievement of the internal control objectives.

3. ESTIMATED FINANCIAL IMPACT OF THE LEGISLATIVE INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[46]	from EFTA countries[47]	from candidate countries[48]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation

[46] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[47] EFTA: European Free Trade Association.

[48] Candidate countries and, where applicable, potential candidates from the Western Balkans.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
5	12.02.01 – Internal Security Fund	Diff.	NO	NO	NO	NO
5	12.01.01 - Support expenditure for the Internal Security Fund	Non-diff.	NO	NO	NO	NO
5	12.10.01 - European Union Agency for Law Enforcement Cooperation (Europol)	Non-diff.	NO	NO	NO	NO
4	11.10.02 – European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)	Non-diff.	NO	NO	NO	NO

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	5	Security and Defence

Europol			Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Title 1: Staff expenditure	Commitments	(1)		0.551	1.102	0.847	0.847	**3.347**
	Payments	(2)		0.551	1.102	0.847	0.847	**3.347**
Title 2: Infrastructure and operating expenditure	Commitments	(1a)		1.49	1.052	0.516	0.516	**3.574**
	Payments	(2a)		1.49	1.052	0.516	0.516	**3.574**
Title 3: Operational expenses	Commitments	(3a)						
	Payments	(3b)						
TOTAL appropriations for Europol	Commitments	=1+1a +3a		**2.041**	**2.154**	**1.363**	**1.363**	**6.921**
	Payments	=2+2a +3b		**2.041**	**2.154**	**1.363**	**1.363**	**6.921**

Comment: The additional appropriations requested in the context of this proposal for Europol will be covered from the Internal Security Fund (ISF) under Heading 5.

EUR million (to three decimal places)

Heading of multiannual financial framework	4	–Migration and Borders

eu-LISA			Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Title 1: Staff expenditure	Commitments	(1)		0.456	0.988	1.52	1.45	**4.414**
	Payments	(2)		0.456	0.988	1.52	1.45	**4.414**
Title 2: Infrastructure and operating expenditure	Commitments	(1a)		4.15	3.55	1.4	0	**9.1**
	Payments	(2a)		4.15	3.55	1.4	0	**9.1**
Title 3: Operational expenses	Commitments	(3a)		0	0	1	1.2	**2.2**
	Payments	(3b)		0	0	1	1.2	**2.2**
TOTAL appropriations for eu-LISA	Commitments	=1+1a +3a		**4.606**	**4.538**	**3.92**	**2.65**	**15.714**
	Payments	=2+2a +3b		**4.606**	**4.538**	**3.92**	**2.65**	**15.714**

Comment: The additional appropriations requested in the context of this proposal for eu-LISA will be covered from the Border Management and Visa Policy Instrument (BMVI) under Heading 4.

Heading of multiannual financial framework	5	Resilience, Security and Defence

DG HOME			Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Internal Security Fund	Commitments	(1)		13.64	40	40		**93.64**
	Payments	(2)		4.68	6.55	9.39		**34.65**
TOTAL appropriations for DG HOME	Commitments			13.64	40	40		**93.64**
	Payments			4.68	6.55	9.39		**34.65**

Comment: The appropriations requested in the context of this proposal will be covered by appropriations already foreseen in the LFS underlying the ISF Regulation. No additional financial or human resources are requested in the context of this legislative proposal.

The costs per Member State include:

- upgrading their infrastructure to support the exchange of web services and set up the connection with the central router, implying efforts to analyse and define the new architectural landscape;
- upgrading their infrastructure to support the exchange of web services and set up the connection with the central router;
- configuring a web service exchange system and the setup of the connection with the central router;
- designing a new national architecture and the specifications to ensure the access of national data through the developed solutions (router and EPRIS);
- setting up a new index or making an already existing index available for police record exchange;

- setting up a new facial images database or making an already existing facial images database available for exchange.
- integrating the national solution;
- generic costs linked to project management.

The following table indicates the costs per category:

Indicate objectives and outputs **DG Home** ⇩			Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		**TOTAL**	
	Type		No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
Router	Connection to the router of existing databases				26	2.314	26	6.787	26	6.787			26	15.89
Facial images	Creation of new database				13 *	2.84	13	8.329	13	8.329			13	19.5
	Connection of database to the router				26	2.72	26	7.996	26	7.996			26	18.72
Police records	Creation of police records database and connection to EPRIS				26	5.763	26	16.959	26	16.959			26	39.7

Total				**13.64**		**40**		**40**			**93.64**

*Estimated MS without a facial images database

Heading of multiannual financial framework	**7**	'Administrative expenditure'

EUR million (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
DG: HOME							
• Human Resources			0.608	0.684	0.608	0.608	**2.508**
• Other administrative expenditure			0.225	0.225	0.186	0.186	0.822
TOTAL DG HOME	Appropriations						

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)		0.833	0.833	0.794	0.794	**3.330**

EUR million (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments		20.287	46.692	45.283	4.013	**116.275**
	Payments		11.329	13.247	14.647	18.059	**57.282**

3.2.2. Estimated impact on Europol's appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year		Year		Year		Year		Year		TOTAL	
			2023		**2024**		**2025**		**2026**		**2027**			
⇩	Type	Average cost[49]	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost
Europol costs (not linked to human ressources)														
- Output	Infrastructure and maintenance					0.764		0.326		0.226		0.226		1.542
- Output	Contractors					0.726		0.726		0.290		0.290		2.032
TOTAL COSTS						1.490		1.052		0.516		0.516		3.574

[49] Due to their specific operational nature, it is not possible to identify precise unit costs per output, nor exact expected volume of outputs, notably as some outputs are related to law enforcement activities reactive to unpredictable criminal activities.

3.2.3. Estimated impact on eu-LISA's appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☒ The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year		Year		Year		Year		Year		TOTAL	
			2023		**2024**		**2025**		**2026**		**2027**			
⇩	Type	Average cost[50]	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost
Eu-LISA costs (not linked to human ressources)														
- Output	Infrastructure[51]					1.85		2.15		0.7		0		4.7

[50] Due to their specific operational nature, it is not possible to identify precise unit costs per output, nor exact expected volume of outputs, notably as some outputs are related to law enforcement activities reactive to unpredictable criminal activities.

[51] Includes hardware, software, network provisions, security.

- Output	Contractors[52]					1.4		0.7		0.7		0		2.8
- Output	Micro matching mechanism					0.9		0.7		0		0		
- Output	Maintenance					0		0		1		1.2		2.2
TOTAL COSTS						4.15		3.55		2.4		1.2		11.3

[52] Includes professional services, design & testing costs.

3.2.4. Estimated impact on Europol's human resources

3.2.4.1. Summary

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Temporary agents - Baseline						
Temporary agents – Additional compared to the baseline (cumulative)	0	0.551	1.101	0.847	0.847	**3.347**
Temporary agents - TOTAL						
Contract staff - Baseline						
Seconded National Experts - Baseline (Draft Budget Request 2021)						
TOTAL only additional costs	0	0.551	1.101	0.847	0.847	**3.347**
TOTAL – including baseline and additional costs						

Staff requirements (FTE):

	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
Temporary agents – Baseline	**0**	**9.5**	**9.5**	**21.5**	**19.5**
Temporary agents – Additional compared to the baseline (cumulative)	0	6.5	6.5	5	5
Temporary agents – TOTAL		**16**	**16**	**26.5**	**24.5**
Contract staff					
Seconded National Experts					

TOTAL	**0**	**16.5**	**16.5**	**26.5**	**24.5**

The human ressources necessary to implement the objectives of this proposal have been estimated in cooperation with Europol. The estimates take into consideration the expected increase in workload as stakeholders make more use of Europol's services over time, as well as the time needed for Europol to absorb resources in order to avoid a situation where the agency would not be able to fully implement its EU contribution and commit appropriations in due time.

The human ressources necessary to implement the objectives of this proposal will be partially covered by existing staff at Europol's (baseline) and partially by additional ressources (additional staff compared to baseline scenario).

No increase in contract agents is foreseen in the LFS.

For the implementation of Prüm II, the resources needed for Europol can be divided into 3 categories:

1) ICT costs for connecting to the biometric router at eu-LISA, necessary development works in Europol informations systems to expose Third Party sourced data for searches from Member States and integrate the searches in Prum with Third Party data in Europol single search interface USE-UI,

2) costs for staff in Europol Operations Directorate to perform the searches with Third Party sourced data and biometrics experts to perform the verification of hits,

3) hosting a central router for police records. This will include one off hardware costs (including different environments for production and testing for Member States), ICT staff to ensure the development and change management of ADEP.EPRIS software, testing with Member States, 24/7 helpdesk to support Member States in case of issues. In order to ensure full support to Member States, it requires the availability of different profiles of ICT staff, e.g. general coordination, requirements engineers, developers, testers, system administrators. It is foreseen to still need a slightly higher amount of ICT staff in the first year after entry into operation.

Due to security constraints and the agreed ceiling of contract agents, the majority of Prüm related tasks have to be performed by Europol staff. Certain less sensitive activities are foreseen to be outsourced to contractors (testing, some development tasks).

Temporary Agents in FTE (baseline + additional staff)	**2023**	**2024**	**2025**	**2026**	**2027**
Project management		1,0	1,0	0,5	0,5
Experts (total)		14,5	14,5	18,0	16,0
• ***biometrics***		*1,0*	*1,0*	*4,0*	*4,0*
• ***operational staff***		*0,5*	*0,5*	*4,0*	*4,0*

• ***ICT***		*13,0*	*13,0*	*10,0*	*8,0*
Helpdesk support/monitoring		0,0	0,0	7,0	7,0
General Coordination		1,0	1,0	1,0	1,0
Total		**16,5**	**16,5**	**26,5**	**24,5**

3.2.5. Estimated impact on eu-LISA's human resources

3.2.5.1. Summary

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Temporary agents - Baseline						
Temporary agents – Additional compared to the baseline (cumulative)		0.456	0.988	1.52	1.368	**4.332**
Temporary agents - TOTAL						
Contract staff - Baseline						
Contract staff - Additional					0.082	**0.082**
Seconded National Experts - Baseline (Draft Budget Request 2021)[53]						
TOTAL only additional costs		0.456	0.988	1.52	1.45	**4.414**
TOTAL – including baseline and additional costs						

Staff requirements (FTE):

	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
Temporary agents – Baseline					

[53] Staff levels indicated in Draft Budget 2021, calculated on the basis of the average staff unit costs to be used for LFS A half of the corresponding annual appropriation is calculated for the year during which staff is recruited.

Temporary agents – Additional compared to the baseline (cumulative)		6	7	10	9
Temporary agents – TOTAL					
Contract staff - baseline					
Contract staff – additional					2
Seconded National Experts					
TOTAL		**6**	**7**	**10**	**11**

The human ressources necessary to implement the objectives of the new mandate have been estimated in cooperation with eu-LISA. The estimates take into consideration the expected increase in workload as stakeholders make more use of eu-LISA's services over time, as well as the time needed for eu-LISA to absorb resources in order to avoid a situation where the agency would not be able to fully implement its EU contribution and commit appropriations in due time.

These estimates are based on the following staffing levels:

	Phase								
	Analysis & Design			Build & Development			Operations		
Contract type	TA	CA	Total	TA	CA	Total	TA	CA	Total
Profile	No.	No.		No.	No.		No.	No.	
IT Architect	1		1	1		1	1		1
Test Management	1		1	1		1	0,5		0.5
Release & Change Management			0	1		1	1		1
Network Administrator	1		1	1		1	1		1
Security Management	2		2	2		2	2		2
1st level support operator (24x7)			0			0		1	1
2nd level support			0			0		1	1

administrator (24x7)									
Programme and Project management	1		1	1		1	0.5		0.5
Product Owner			0	1		1	1		1
Biometric Expert	1		1	1		1	1		1
System Administrator/Infra	1		1	1		1	1		1
Total (CA+TA)	**8**		**8**	**10**		**10**	**9**	**2**	**11**

Profiles	Year -1 (Preparation & Design)	Year 1	Year 2	Year 3	Year 4	Year 5
IT Architect (TA)	1	1	1	1	1	1
Test Management (TA)		1	1	0.5	0.5	0.5
Release & Change Management (TA)			1	1	1	1
Network Administrator (TA)	1	1	1	1	1	1

Security Management (TA)	1	1	2	2	2	2
1st level support operator (24x7) – (CA)				1	1	1
2nd level support administrator (24x7) – (CA)				1	1	1
Programme and Project management (TA)	1	1	1	0.5	0.5	0.5
Product Owner (TA)			1	1	1	1
Biometric Expert (TA)	1	1	1	1	1	1
System Administrator/ Infrastructure (TA)	1	1	1	1	1	1
TOTAL	**6**	**7**	**10**	**11**	**11**	**11**

3.2.5.2. Estimated requirements of human resources for the partner DG

☐ The proposal/initiative does not require the use of human resources.

☒ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
• **Establishment plan posts (officials and temporary staff)**						
XX 01 01 01 (Headquarters and Commission's Representation Offices)			5	5	4	4
XX 01 01 02 (Delegations)						
XX 01 05 01 (Indirect research)						
10 01 05 01 (Direct research)						
• **External staff (in Full Time Equivalent unit: FTE)**[54]						
XX 01 02 01 (AC, END, INT from the 'global envelope')						
XX 01 02 02 (AC, AL, END, INT and JPD in the Delegations)						
XX 01 04 ***yy***[55]	- at Headquarters[56]					
	- in Delegations					
XX 01 05 02 (AC, END, INT – Indirect research)						
10 01 05 02 (AC, END, INT – Direct research)						
Other budget lines (specify)						
TOTAL			**5**	**5**	**4**	**4**

XX is the policy area or budget title concerned.

The human resources required will be partially (3 FTE) met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints. The DG will also require additional staff (2 FTE).

[54] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

[55] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

[56] Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

Description of tasks to be carried out:

Five officials for the follow-up. The staff deal with taking up the Commission's duties in the delivery of the programme: checking compliance with legal proposal, addressing compliance issues, preparing reports to European Parliament and Council, assessing Member State progress, keeping secondary legislation up-to-date including any development concerning the standards. As the programme is an additional activity compared with existing workloads, additional staff are required (2 FTE). One of the staff increase is limited in terms of duration and covers only the development period, the second one represents the absortion of the tasks of the Council Secretariat, as the Council Decisions are transformed into a Regulation, the Commission must take over the Council Secretariat tasks its workload is 1 FTE.

3.2.6. Compatibility with the current multiannual financial framework

☐ The proposal/initiative is compatible the current multiannual financial framework.

☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[57].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts. […]

3.2.7. Third-party contributions

The proposal/initiative does not provide for co-financing by third parties.

The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[57] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

3.3. Estimated impact on revenue

☒ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

- ☐ on own resources
- ☐ on other revenue
- ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[58]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

[…]

Specify the method for calculating the impact on revenue.

[…]

[58] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

ANNEX 5

to the
COMMISSION DECISION

on the Internal Rules on the implementation of the general budget of the European Union (European Commission section) for the attention of the Commission departments

ANNEX
to the LEGISLATIVE FINANCIAL STATEMENT

ANNEX
to the LEGISLATIVE FINANCIAL STATEMENT

Name of the proposal:

Proposal on automated data exchange for police cooperation ("Prüm II"), amending Regulation (EU) 2018/1726, Regulation (EU) 2019/817 and Regulation (EU) 2019/818, and repealing Council Decisions 2008/615/JHA and 2008/616/JHA

1. NUMBER AND COST OF HUMAN RESOURCES CONSIDERED NECESSARY

2. COST OF OTHER ADMINISTRATIVE EXPENDITURE

3. TOTAL ADMINISTRATIVE COSTS

4. METHODS OF CALCULATION USED FOR ESTIMATING COSTS

4.1. Human resources

4.2. Other administrative expenditure

This annex must accompany the legislative financial statement when the inter-services consultation is launched.

The data tables are used as a source for the tables contained in the legislative financial statement. They are strictly for internal use within the Commission.

(1) Cost of human resources considered necessary

☐ The proposal/initiative does not require the use of human resources

X☐ The proposal/initiative requires the use of human resources, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework		2024		2025		2026		2027								TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)																	
20 01 02 01 - Headquarters and Representation offices	AD	5	0.608	5	0.684	4	0.608	4	0.608							4	2.508
	AST																
20 01 02 03 - Union Delegations	AD																
	AST																
• External staff [59]																	
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC																
	END																
	INT																
20 02 03 – External personnel - Union Delegations	AC																
	AL																
	END																

[59] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT= agency staff; JPD= Junior Professionals in Delegations.

	INT																
	JPD																
Other HR related budget lines (*specify*)																	
Subtotal HR – HEADING 7		5	0.608	5	0.684	4	0.608	4	0.608							4	2.508

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

(2) Cost of other administrative expenditure

☐ The proposal/initiative does not require the use of administrative appropriations
☑ The proposal/initiative requires the use of administrative appropriations, as explained below:

EUR million (to three decimal places)

HEADING 7 of the multiannual financial framework	**2024**	**2025**	**2026**	**2027**				**Total**
At headquarters or within EU territory:								
20 02 06 01 - Mission and representation expenses	0.035	0.035	0.035	0.035				**0.140**
20 02 06 02 - Conference and meeting costs	0.125	0.125	0.125	0.125				**0.500**
20 02 06 03 – Committees (Prüm II Committee)[60]	0.065	0.065	0.026	0.026				**0.182**
20 02 06 04 Studies and consultations								
20 04 – IT expenditure (corporate)[61]								
Other budget lines non-HR related (*specify where necessary*)								
In Union delegations								
20 02 07 01 - Missions, conferences and representation expenses								

[60] Prüm II Committee, aprox 10 meetings per year in 2024 and 2025 and 4 meetings per year after with only half being accounted for in the costs (the other half being in videoconference format).

[61] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7).

20 02 07 02 - Further training of staff								
20 03 05 – Infrastructure and logistics								
Other budget lines non-HR related (*specify where necessary*)								
Subtotal Other - HEADING 7 of the multiannual financial framework	0.225	0.225	0.186	0.186				**0.822**

EUR million (to three decimal places)

Outside HEADING 7 of the multiannual financial framework	**2024**	**2025**	**2026**	**2027**				**Total**
Expenditure on technical and administrative assistance (not including external staff) from operational appropriations (former 'BA' lines):								
- at Headquarters								
- in Union delegations								
Other management expenditure for research								
Policy IT expenditure on operational programmes[62]								
Corporate IT expenditure on operational programmes[63]								

[62] The opinion of DG DIGIT – IT Investments Team is required (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020, page 7).

Other budget lines non-HR related (*specify where necessary*)								
Sub-total Other – Outside HEADING 7 of the multiannual financial framework								
Total Other admin expenditure (all MFF Headings)	0.225	0.225	0.186	0.186				**0.822**

[63] This item includes local administrative systems and contributions to the co-financing of corporate IT systems (see the Guidelines on Financing of IT, C(2020)6126 final of 10.9.2020).

(3) Total administrative costs (all Headings MFF)

EUR million (to three decimal places)

Summary	2024	2025	2026	2027				Total
Heading 7 - Human Resources	0.608	0.684	0.608	0.608				**2.508**
Heading 7 – Other administrative expenditure	0.225	0.225	0.186	0.186				**0.822**
Sub-total Heading 7								
Outside Heading 7 – Human Resources								
Outside Heading 7 – Other administrative expenditure								
Sub-total Other Headings								
TOTAL HEADING 7 and Outside HEADING 7	0.833	0.833	0.794	0.794				**3.330**

The administrative appropriations required will be met by the appropriations which are already assigned to management of the action and/or which have been redeployed, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of existing budgetary constraints.

4. METHODS OF CALCULATION USED TO ESTIMATE COSTS

4.1. Human resources

This part sets out the method of calculation used to estimate the human resources considered necessary (workload assumptions, including specific jobs (Sysper 2 work profiles), staff categories and the corresponding average costs)

HEADING 7 of the multiannual financial framework
NB: The average costs for each category of staff at Headquarters are available on BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
Officials and temporary staff: In line with Circular note of DG BUDGET to RUF/2020/23 of 30/11/2020 (see annexe 1, Ares(2020)7207955 of 30/11/2020), 1AD represents a cost of 152 000 EUR per annum. Half of the corresponding annual appropriation is calculated for the year during which staff is recruited and phased out. The human resources required will be partially (3 FTE) met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints. The DG will also require additional staff (2 FTE). Description of tasks to be carried out: Five officials for the follow-up. The staff deal with taking up the Commission's duties in the delivery of the programme: checking compliance with legal proposal, addressing compliance issues, preparing reports to European Parliament and Council, assessing Member State progress, keeping secondary legislation up-to-date including any development concerning the standards. As the programme is an additional activity compared with existing workloads, additional staff are required (2 FTE). One of the staff increase is limited in terms of duration and covers only the development period, the second one represents the absortion of the tasks of the Council Secretariat, as the Council Decisions are transformed into a Regulation, the Commission must take over the Council Secretariat tasks its workload is 1 FTE.
• External staff

Outside HEADING 7 of the multiannual financial framework
• Only posts financed from the research budget
• External staff

4.2. Other administrative expenditure

Give details of the method of calculation used for each budget line

and in particular the underlying assumptions (e.g. number of meetings per year, average costs, etc.)

HEADING 7 of the multiannual financial framework

It is estimated that an average of 35 missions will take place per year, including missions for the statutory meetings (Advisory Group, Working Groups of both eu-LISA and Europol and meetings related to EPRIS and Eucaris), to attend Prüm related meetings and conferences. The unit cost per mission is calculated based on 1 official travelling for an average of 2 days for each mission and is set at EUR 500 per mission per day.

The unit costs per expert meeting/conference is set at EUR 25 000 for 50 participants. It is estimated that 5 meetings will be organised per year.

The unit costs per Committee is set at EUR 13 000 for 26 participants, assuming the reimbursement of 1 participant per MS for a one-day mission to attend the Committee. It is estimated that 10 meetings will be organised per year during 2024 and 2025 (5 in physical format and 5 in videoconference format) and 4 meetings will be organised per year as of 2026 (2 in physical format and 2 in videoconference format).

Outside HEADING 7 of the multiannual financial framework