Council of the European Union

Brussels, 9 December 2021
(OR. en)

14204/21
ADD 1

Interinstitutional File:
2021/0410(COD)

IXIM 259
ENFOPOL 459
JAI 1278
CODEC 1518
IA 201

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	9 December 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 378 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council

Delegations will find attached document SWD(2021) 378 final.

Encl.: SWD(2021) 378 final

EUROPEAN
COMMISSION

Brussels, 8.12.2021
SWD(2021) 378 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

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

{COM(2021) 784 final} - {SEC(2021) 421 final} - {SWD(2021) 379 final}

Table of contents

Glossary

Term or acronym	*Meaning or definition*
ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
ANSI/NIST-ITL	The ANSI/NIST-ITL (American National Standard Institute / National Institute of Standards and Technology - Information Technology Institute) standard is a data format standard used by law enforcement authorities for interagency exchange of biometric sample information to be used for the identification or verification process of a subject.
COSI	Standing Committee on Operational Cooperation on Internal Security
Dactyloscopic data	Fingerprint data
DAPIX	Council Working Party on Information Exchange and Data Protection
DNA	Deoxyribonucleic acid
ECRIS-TCN	Centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons
EDRi	European Digital Rights
EES	Entry-Exit System
EIS	Europol Information System
EIXM	The European Information Exchange Model aims at a comprehensive legal and technical architecture for law enforcement purposes in both the EU and Schengen associated countries, allowing for the complementary and effective use of information exchange tools by the authorities concerned while protecting citizens' security as well as their privacy.
EPE	Europol Platform for Experts
ETIAS	European Travel Information and Authorisation System

EUCARIS	European Car and Driving Licence Information System
eu-LISA	EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Eurodac	EU asylum fingerprint database enabling Member States to compare the fingerprints of asylum applicants to assist in determining which Member State is to be responsible for examining an application for international protection lodged in a Member State by a third-country national or a stateless person
GDPR	General Data Protection Regulation
Hit	Instance of finding or matching particular data in a computer search
HLEG	High-level expert group on information systems and interoperability
iARMS	Interpol's Illicit Arms Records and tracing Management System
ICD	The Interface Control Document defines the requirements for the exchange of information between correlated systems.
ISEC	Prevention of and Fight against Crime programme
IXIM	Working Party on Justice and Home Affairs Information Exchange
LED	Directive (EU) 2016/680 (Law Enforcement Directive)
MCT	Mobile Competence Team
NCP	National Contact Points, established as end-to-end communication points for automated Prüm data exchange.
Prüm Decisions	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 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.
Prüm Treaty	Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.

SFD	Council Framework Decision 2006/960/JHA (Swedish Framework Decision)
SIENA	Europol's Secure Information Exchange Network Application
SIS	Schengen Information System
SIS II	Second generation Schengen Information System
SOCTA	Serious and Organised Crime Threat Assessment
SPOC	Single Point of Contact, the 'one-stop shop' for international police cooperation
TESTA	Trans European Services for Telematics between Administrations, used as the communication network for data exchange among the Member States
TFEU	Treaty on the Functioning of the European Union
VIS	Visa Information System
VRD	National Vehicle Registration Data relating to owners or operators, and relating to vehicles

PROLOGUE - WHAT IS PRÜM?

The Prüm Decisions, adopted in 2008, contribute to cross-border cooperation between EU Member States in the fields of justice and home affairs. They provide a mechanism for the exchange of information between authorities responsible for the prevention and investigation of criminal and terrorist offences. The Prüm Decisions lay down, inter alia, the conditions and procedures for mutual on-line access to national databases for automated search and supply of three categories of data: (a) **DNA profiles**, (b) **fingerprint data** and (c) **certain national vehicle registration data**.

DNA and fingerprint exchanges take place based on a hit/no-hit approach. It means that DNA profiles or fingerprints found at a crime scene in one Member State can be automatically compared, in a first step, with profiles held in another Member State's database. If there is a match with data in another Member State's database, a "hit" will be reported to the requesting Member State. Once a hit has been achieved, the corresponding actual information can be exchanged, in a second step, through a manual process.

For example, in a case where a partial fingerprint sample (so-called 'latent print') was found on a crime scene, this latent can be compared against the national criminal fingerprint database. If the search brings no results, i.e. the suspect remains unidentified, the Prüm framework can be used to check other Member States' criminal databases. Indeed, checking the same latent fingerprint data also against other Member States' criminal fingerprint databases could show that there is information available on that suspect in that other Member State's database. As a result, after the exchange of additional data between the two Member States, the suspect can be identified and the criminal investigation can lead to the prosecution and conviction of a criminal.

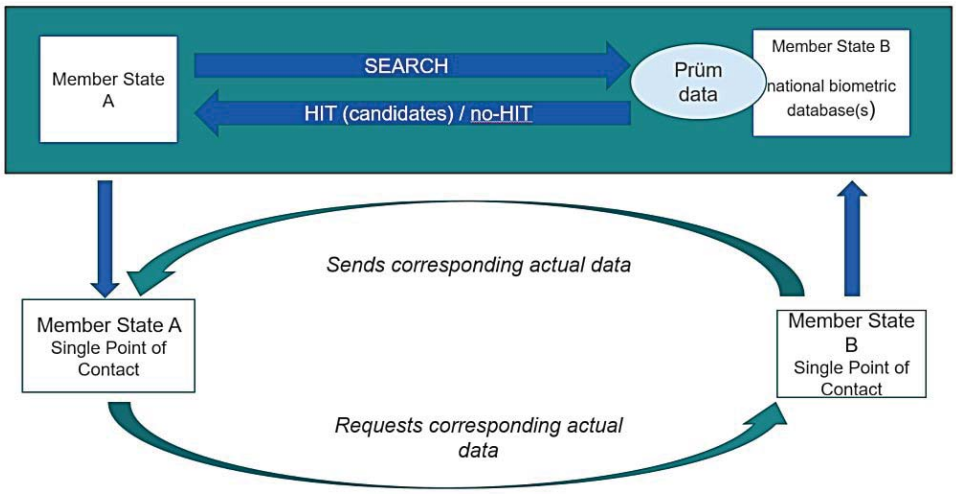


Figure 1: How Prüm works

The situation with regard to **vehicle registration data** ('VRD') exchange is slightly different. Vehicle registration data, including licence plates and vehicle identification number, are exchanged through national platforms that are linked to the online

application EUCARIS. Should there be a match with data in another Member State's database, the corresponding actual **information is provided immediately** to the requesting Member State. There is no need to introduce a separate request manually, in a second step, to receive the corresponding actual information.

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Criminality across Europe undermines EU citizens' security and well-being. As set out in the EU Security Union Strategy,[1] Europe faces a security landscape in flux, with evolving and increasingly complex security threats. These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups that engage in a wide range of criminal activities. In order to fight crime effectively, law enforcement authorities need robust and performant tools. Cooperation and information sharing are the most powerful means to combat crime and pursue justice as mentioned in the EU Security Union Strategy. As stated in the EU Strategy to tackle Organised Crime 2021-2025,[2] the European Union has provided law enforcement with a range of tools to facilitate exchange of information in the EU that have proved crucial in uncovering criminal activities and networks.

According to the EU Serious and Organised Crime threat assessment 2021, more than **70% of organised crime groups are present in more than three Member States**. Even the seemingly most local crime may have links to other places in Europe where the same perpetrator carried out his criminal acts. In that context, **law enforcement authorities need to be able to exchange data, in a timely manner**. However, in an area without internal borders, **there are still borders and obstacles when it comes to data exchange between law enforcement authorities**, which leads to blind spots and loopholes for numerous criminals and terrorists that act in more than one Member State. **Member States alone cannot close the information gap, owing to the cross-border nature of crime fighting and enhancing security.** Member States must rely on one another in these matters.

The Commission has announced at various occasions (most recently in its Strategy towards a fully functioning and resilient Schengen area)[3] its intention to present, by the end of 2021, a proposal for a **Police Cooperation Code**, together with a proposal for a **Prüm Regulation**, to address the above challenges.

The forthcoming Police Cooperation Code will provide a coherent EU 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, the Police Cooperation Code will formalise and clarify the procedures for information sharing among Member States, in particular for investigation purposes, including the role of the 'Single Point of Contact' for such exchanges, and making full use of Europol's information exchange channel SIENA.

The Police Cooperation Code will be complemented by a **proposal to reinforce the automated exchange of important data categories under the Prüm Council**

[1] COM(2020) 605 final (24.7.2020).
[2] COM(2021) 170 final (14.4.2021).
[3] COM(2021) 277 final (2.6.2021).

Decisions. The reinforced Prüm framework will provide specific rules and possibilities for the exchange of specific data categories within the overall framework and general rules for information exchange that the Police Cooperation Code will provide.

The existing Prüm Decisions[4] date back to 2008 and aim to support and step up cross-border police and judicial cooperation related to criminal matters. To this end, the Prüm Decisions create a framework for the **exchange of information** between authorities responsible for the **prevention and investigation of criminal offences**.

In 2018, at the occasion of the 10 years after the adoption of the Prüm Decisions, the Council underlined the importance of its main features: the automated searching and comparison of DNA profiles, dactyloscopic data and vehicle registration data for tackling terrorism and cross-border crime.[5] The Council also invited the Commission to consider revising the Decisions with a view to broadening their scope and to updating the necessary technical and legal requirements, notably to facilitate connections between Member States and speed up the exchange of data between them.

In recent years, the landscape of the large-scale EU information systems has developed substantially. This includes the revision of the three EU central information systems that are in operation: the Schengen Information System (SIS), the Visa Information System (VIS) and the Eurodac system.[6] In addition, three new systems are currently in 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).[7]

All these current and future systems are linked through the **interoperability framework for the EU information systems[8]** for security, border and migration management, adopted in 2019, and which is currently being put in place. The proposed revision of the Prüm Decisions needs to comply with this framework. Notably when it comes to the

[4] 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. See Annex 4 for the evaluation of the functioning of the automated exchange of data pursuant to the Prüm Decisions and the level of implementation and application in each EU Member State since the adoption of the instruments in 2008, according to the five evaluation criteria set out in the Commission's Better Regulation Guidelines.

[5] See the July 2018 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.

[6] The SIS assists competent authorities in Europe 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 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. Please see Annex 7 for more information on these systems.

[7] 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. Please see Annex 7 for more information on these systems.

[8] Regulation (EU) 2019/817 and Regulation (EU) 2019/818. Please see Annex 7 for more information on this framework.

technical architecture for the exchange of data, the proposed revision of the Prüm Decisions has to be consistent and compatible with the overall architecture provided by the interoperability of EU information systems and with the goals and synergies it pursues. This would mean providing for fast and controlled access to the information that law enforcement officers need to perform their tasks and for which they have access rights.

Revising the Prüm Decisions also provides an opportunity to **update the data protection framework** used for the automated exchange of data under these Decisions. The Prüm Decisions contain rules on data protection that predate the 2016 EU data protection reform. There is therefore a need to ensure that a revised Prüm legislation is fully aligned with the Law Enforcement Directive,[9] especially as regards the data protection safeguards. This approach is in line with the Commission's findings laid down in its Communication of 24 June 2020.[10] Compliance with data protection is a legal requirement that applies horizontally, therefore this alignment will be an integral part of any of the various policy options considered in this impact assessment.

When preparing the legal proposal, the Commission will ensure full alignment with the interoperability framework and the data protection framework.

2. PROBLEM DEFINITION

This chapter presents the different problems, their drivers as well as how those problems would evolve without intervention. The following problem tree presents the problems in relation with the objectives and policy options.

[9] 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.

[10] Communication from the Commission to the European Parliament and the Council on the way forward on aligning the former third pillar acquis with data protection rules (COM(2020) 262 final).

problems	specific drivers	specific objectives
Problem I: law enforcement authorities are not always able to find out if data on DNA profiles, fingerprints or vehicle registration which they need to perform their duties is available in the national database of another Member State	➢ **complex architecture** of the Prüm Decisions ➢ **network** of bilateral connections between the national databases, requiring each Member State to establish at least 26 connections for each data category ➢ many bilateral connections between Member States' national databases have not been established due to the technical complexity and the important financial and human resources entailed	***Objective I***: provide for 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 in line with fundamental rights including data protection requirements
Problem II: law enforcement authorities do not have efficient means to query and access other relevant categories of data stored in national databases of other Member States (beyond data on DNA profiles, fingerprints and vehicle registration data), which they need to perform their duties	➢ data is stored in a decentralised way in **national databases** (as compared to SIS, EURODAC, VIS, future ETIAS and future EES). ➢ Member States do not give each other full access to their respective national databases, as would be required by the **principle of availability** ➢ the Prüm Decisions, as the existing instrument to ensure the availability of data, are **limited to certain categories** of data (fingerprints, DNA, vehicle registration)	***Objective II***: 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 in line with fundamental rights including data protection requirements
Problem III: law enforcement authorities do not have efficient means to query and access data on DNA profiles, fingerprints and possible other relevant categories of data that are available in Europol's database, which they need to perform their duties	➢ Europol does not provide a technical tool for efficient access to important categories of data (including fingerprints, DNA) ➢ Europol is not covered by the Prüm Decisions as the existing instrument to ensure the availability of data	***Objective III***: ensure that relevant data (in terms of sources of data) from Europol's database is available to law enforcement authorities in line with fundamental rights including data protection requirements
Problem IV: once law enforcement authorities receive an indication that data is available in the database of another Member State (a "hit"), they do not always have efficient access to the corresponding actual data stored in the national database of that Member State	➢ exchange of "hit follow-up data" is not governed by the Prüm Decisions, but by **national law** ➢ differences in national rules and procedures lead to **fragmentation** in the exchange of hit follow-up data ➢ Member States use different law enforcement cooperation channels, different procedures, different data sets and different time limits when requesting and submitting follow-up data	***Objective IV***: 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 in line with fundamental rights including data protection requirements

2.1 Problem I: Law enforcement authorities are not always able to find out if data on DNA profiles, fingerprints or vehicle registration which they need to perform their duties is available in the national database of another Member State

As showed in the evaluation (see Annex 4), the implementation of the Prüm Decisions has been slow. Indeed, nearly ten years after the implementation deadline on 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 may decrease the possibility that criminals are identified, and cross-border links between crimes are detected, hindering the exchange of information and the functioning of the Prüm system.

2.1.1 What is the problem?

Law enforcement authorities are not always able to find out if data is **available** in the national database of another Member State. This is obviously the case for those data categories that are not covered by the Prüm Decisions (see *problem II*), but it is even the case for those that are covered by Prüm. Even if a search through the Prüm Decisions results in "no hit", this is not a reliable indication for the investigating law enforcement authority that no data is available in another Member State.

2.1.2 What are the problem drivers?

The major driver for this problem lies in the complex technical architecture of the Prüm Decisions that provide for a network of bilateral connections between the national databases of Member States without any EU level central component. As a consequence of this technical architecture, each Member State should establish at least 26 connections – i.e. a connection with each Member State – per each data category.[11] However, as pointed out in the evaluation (see Annex 4), many bilateral connections between Member States' national databases have not been established due to the technical complexity and the important financial and human resources entailed. Indeed, some Member States have explained that setting up all the connections and maintaining them is technically complex and requires considerable financial and human resources. For these reasons, they have decided to focus on establishing connections only with certain Member States.

[11] It should be noted that for VRD, a single connection to the EUCARIS platform needs to be established by a Member State in order to be able to exchange VRD with all other connected Member States. If such a connection has not been established, the Member State concerned will not be able to participate in the exchange and the automated access provided by the Prüm Decisions to VRD will remain incomplete as well.

As a result, the automated access provided by the Prüm Decisions (hit/no-hit) to DNA and fingerprints data remains incomplete. Data cannot be checked against the data in some Member States if the relevant bilateral connection has not been established. These Member States' law enforcement authorities will not be able to find out if relevant data is available in the other Member State, preventing any information exchange from taking place.

As explained in the evaluation (see Annex 4), the fact that some Member States are not exchanging data harms the other Member States and hampers the exchange of data in general, and therefore cross-border cooperation and the fight against crime. Indeed, this may decrease the possibility of having data checked against other Member States' databases, of identifying criminals and of detecting cross-border links between crimes.

2.1.3 How will the problem evolve without intervention?

As examined in the evaluation (see Annex 4), nearly ten years after the implementation deadline on 26 August 2011, a number of bilateral connections have still not been established. As of December 2020, 28% in the case of DNA, 29% in the case of fingerprints and 11,6% in the case of vehicle registration data of all possible connections were still missing.[12] There are also great discrepancies between Member States. While some Member States have introduced connections to almost all other Member States and to the UK, other Member States have not introduced any connection. Moreover, non-legislative action to improve implementation has been taken,[13] but it has not solved the situation regarding the coverage of bilateral connections. Without any intervention, the problem would be unlikely to change in light of the slow progress in the establishment of the bilateral connections and the support and resources which have been made available throughout the years to support the implementation.

2.2 Problem II: Law enforcement authorities do not have efficient means to query and access other relevant categories of data stored in national databases of other Member States (beyond data on DNA profiles, fingerprints and vehicle registration data), which they need to perform their duties

As showed in the evaluation (see Annex 4), one of the key success factors for the Prüm framework is the possibility to search and compare data in an automated manner in other Member States' databases. However, this possibility currently covers only a few categories of data: DNA, dactyloscopic and vehicle registration data. There are some other categories of data in Member States' databases that are often the subject of cross-border information requests for the purpose of criminal investigations, but that are exchanged in an inefficient way.

[12] See, for the latest available version (19 April 2021), Council document 5729/21 (not publicly available).
[13] Such as the Prevention of and Fight against Crime programme (ISEC), the Mobile Competence Team or the Prüm Helpdesk. See the evaluation in Annex 4 for more information.

2.2.1 What is the problem?

The lack of efficient access[14] for law enforcement authorities to all **relevant categories of data**[15] in other Member States' databases impedes their work and undermines their ability to fight crime and terrorism. The 2008 **Prüm Council Decisions**, as the main EU instrument to implement the principle of availability,[16] only partially addressed this problem. The Prüm Decisions allow law enforcement authorities to search for DNA and fingerprints in the databases of other Member States[17] on a hit-no-hit basis through bilateral connections, and to search for vehicle registration data. The Prüm Decisions have proven instrumental in reducing the information gap as regards DNA, fingerprints and vehicle registration data, enabling law enforcement authorities to search and compare these data categories in an automated way in other Member States' databases. This helped solving many crimes in Europe where these three data categories played a role in the investigation.[18] However, beyond DNA, fingerprints and vehicle registration data, there are other categories of data in Member States' databases that are often relevant in criminal investigations and therefore the subject of cross-border information requests, but that are not covered by the Prüm Decisions. Examples include **facial images, driving licences, police records and ballistics**. These data categories are not part of any automated exchange between Member States and are exchanged in an inefficient way only. Indeed, there have been calls[19] to broaden the scope of the automated cross-border exchange to other data categories. Moreover, in reply to the public consultation,[20] most respondents agreed that the fact that these additional data categories are exchanged by sending manual queries, often time-consuming, to other law enforcement authorities is a

[14] Efficient access to data consists of seamless, timely and complete access of law enforcement authorities to relevant data.

[15] Relevant data is data that is necessary for law enforcement authorities for the investigation of a crime.

[16] The principle of availability requires that throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose under conditions equal to those under which it would make available that information to a law enforcement agency in its own Member State, taking into account the requirement of ongoing investigations in that State. If the information requested is available, it must be provided and the grounds for declining to do so are rather limited.

[17] The United Kingdom and Norway participate in the Prüm framework on the basis of international agreements. This participation should be maintained.

[18] As highlighted in the 2012 report on the implementation of the Prüm Decisions (COM(2012) 732 final), "*the following example from Germany illustrates the value of Prüm in a cross-border context: In the late summer of 2011 a man was found stabbed to death in a north-western German city. On the crime scene, police experts discovered a fingerprint on a door frame in the apartment where the man had been found. Although there was no obvious link to another country, an automated Prüm search led to a hit in the Bulgarian AFIS database. The follow-up information requested from Bulgaria the following day was sent within three hours and was immediately entered into the Schengen Information System. Already the next day the individual concerned was arrested in Austria*." For more information on the added value of the exchange of DNA, fingerprint and VRD under the Prüm Decisions, see Annex 4 on the evaluation of the existing policy and legislative framework.

[19] See the July 2018 Council Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption.

[20] The European Commission launched a public consultation in December 2020 to collect opinions on the effectiveness of the current legislative and policy framework and on existing problems and possible options for future initiatives. Please see Annex 2 for more information on the results of the consultation.

shortcoming in the law enforcement information exchange and that EU legislation should be established to standardise and automate the exchange of additional data categories.

2.2.2 What are the problem drivers?

The main drivers for this problem are that the data is stored in a decentralised way (i.e. in national databases, as compared to SIS, EURODAC, VIS, future ETIAS and future EES) and that Member States do not give each other full access to their respective national databases, as national legislation limits access to national authorities. Moreover, the Prüm Decisions, as the existing instrument to ensure the availability of data is limited to certain categories of data (fingerprints, DNA, and vehicle registration data).

2.2.3 How will the problem evolve without intervention?

As mentioned above, the data categories necessary for law enforcement cooperation which are not within the scope of the Prüm Decisions are not part of any automated exchange between Member States. This does not mean the exchange cannot take place, it just means there is no structured way to do so, resulting in inefficient and time-consuming procedures, potentially even discouraging law enforcement authorities to work with their counterparts in other Member States. Without intervention, the current inefficient situation would stagnate.

2.3 Problem III: Law enforcement authorities do not have efficient means to query and access data on DNA profiles, fingerprints and other relevant categories of data that are available in Europol' database, which they need to perform their duties

2.3.1 What is the problem?

Europol is not part of the Prüm framework. Therefore, Europol cannot make **third-country sourced data** accessible to Member States via the Prüm information exchange mechanisms, nor can it perform searches in Member States' Prüm data with Europol data. The gaps can be summarized as follows: 1) Member States cannot use Europol's third-country sourced data as an additional data source in the context of the Prüm framework and 2) Europol cannot check Europol data against relevant criminal data from Member States. These gaps may result in undetected links between criminal and terrorism cases.

While the Europol Regulation[21] provides a legal basis for Member States to have access to these data, there is no technical mechanism in place to do so. There is therefore a need to enable national authorities to search third country-sourced data stored at Europol on the basis of DNA, fingerprints data and facial images (e.g. national authorities cannot directly search data at Europol with a latent fingerprint found at a crime scene while they

[21] Regulation (EU) 2016/794 (11 May 2016), Article 20(1).

could use the Prüm framework to search such data in another Member State's database). Europol as an additional source of data could provide considerable operational benefits notably with regard to third-country sourced DNA and fingerprints that the agency holds, as highlighted by Member States in the Council.[22]

2.3.2 What are the problem drivers?

Member States' law enforcement authorities do not have a technical tool at their disposal for efficient access to Europol's **third-country sourced data** (fingerprints, facial images and DNA). Moreover, there is no legal framework that would allow Europol to use third country-sourced data to query against Member States databases' in the context of the Prüm framework. As a consequence, relevant cross-border information related to serious and organised crime and terrorism may remain undetected.

2.3.3 How will the problem evolve without intervention?

Without any changes to the Prüm Decisions, the DNA, facial images and fingerprints stored at Europol and obtained from third countries would remain outside the exchange governed by these Decisions. In principle, based on its mandate, Europol could establish a direct access to this data for Member States. However, such a parallel approach would partially duplicate the framework established by the Prüm Decisions. This would not only lead to substantial additional costs for Member States, but also require Member States to launch separate requests to search the same type of data at Europol and through the framework established by the Prüm Decisions. Not using this data against the criminal databases of Member States under the Prüm framework may result in missing relevant cross-border information related to serious and organised crime and terrorism and in incomplete criminal analysis.

2.4 Problem IV: Once law enforcement authorities receive an indication that data is available in the database of another Member State (a "hit"), they do not always have efficient access to the corresponding actual data stored in the national database of that Member State

As showed in the evaluation (see Annex 4), 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 hinders the functioning of the Prüm system. Indeed, due to differences in national rules and procedures, the exchange of hit follow-up data is very fragmented, to the extent that it sometimes takes weeks or even months to receive the relevant information behind a hit.

[22] The July 2018 Council Conclusions on Prüm invited that the possibility be examined for Europol „*to become a partner in the Prüm framework with a view to enabling the cross-matching of DNA and dactyloscopic data with third countries, with whom Europol has an operational agreement, while fully taking into account the data owner principle*".

2.4.1 What is the problem?

Even where there is an indication that data is available in the database of another Member State ("hit" under the Prüm Decisions), law enforcement authorities do not always have **efficient access** to the data stored in the national database of another Member State. Automated searches in Member States' DNA and fingerprints databases under the Prüm Decisions are based on reference data only. This reference data does not contain any data from which the data subject can be directly identified. Further personal and other case related data is exchanged only when a hit has been confirmed by a forensic expert.

Already in 2012, in reply to a questionnaire circulated by the Commission in preparation of the 2012 Report on the Implementation of Council Decision 2008/615/JHA (hereinafter the '2012 Report'),[23] 18 out of 24 Member States generally pointed to the need to improve the follow-up to Prüm hits, one third focusing on national structures while a majority saw a need for action primarily at EU level. During the consultations for this Impact Assessment, Member States reiterated that the problem still exists. The automated search function introduced by the Prüm Decisions was a far-reaching step forward in the area of law enforcement information exchange. However, without a proper follow-up, 'hits' have hardly any meaning for investigators. This is why Member States suggested that the exchange of hit-follow-up data be regulated under the Prüm Decisions and sped up.

2.4.2 What are the problem drivers?

The major driver for this problem, as demonstrated in the evaluation (see Annex 4), is that **the exchange of "hit follow-up data" is not governed by the Prüm Decisions, but by national law**.[24] Due to differences in national rules and procedures, the exchange of hit follow-up data is very **fragmented**: Member States use different law enforcement cooperation channels, different procedures, different data sets and different time limits when requesting and submitting follow-up data. As a consequence of this **inefficient follow-up to hits** generated under the Prüm Decisions, the processes are so cumbersome and time-consuming that in some cases, it may take weeks or even months for authorities to obtain the personal data behind a hit, making the access to data inefficient.

In reply to the public consultation, most respondents agreed that the fact that the exchange of further personal data after a hit has been confirmed is not governed by the Prüm Decisions is a shortcoming of the existing Prüm framework and that EU legislation should be established to streamline the hit follow-up exchange of further personal and case-related data.

2.4.3 How will the problem evolve without intervention?

[23] COM(2012) 732 final.
[24] Articles 5 and 10 of Council Decision 2008/615/JHA.

As Member States, despite all problems and limitations, make more and more use of the Prüm Decisions to query data in other Member States' national databases, the problems caused by the inefficient follow-up to hits generated under the Prüm Decisions will increase. The increase of the use of the Prüm Decisions entails an increase in the number of queries and of hits, and therefore an increase in the number of follow-ups to hits, thereby leading to a worsening of the situation. The use of different law enforcement cooperation channels, different procedures, different data sets and different time limits when requesting and submitting follow-up data will further increase the workload on all sides while undermining effectiveness and efficiency. This would not be sustainable in the long run. In any case, due to technical changes and scientific developments since the adoption of the Prüm Decisions, their technical and forensic rules and procedures need to be updated. Otherwise, the Prüm Decisions would become obsolete.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

The legal basis for the instrument is point (d) of the second subparagraph of Article 82(1) and point (a) of Article 87(2) of the Treaty on the Functioning of the European Union.

3.2. Subsidiarity: Necessity of EU action

The improvement of information exchange in the European Union 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.

Through several implementation projects at EU level,[25] Member States have tried to take action to address the shortcomings of Prüm[26] but despite all these actions, the shortcomings remained the same as the ones that were described in the 2012 Report.[27] This is why EU action is needed as action by Member States only has already been tried and is not sufficient.

[25] 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.

[26] Through a project led by Finland, Member States analyzed the national procedures applied following a hit. The final report of this project (see document 14310/2/16 REV2 for more information) recommended a series of non-mandatory good practices to streamline the post-hit information exchange throughout the EU. 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.

[27] COM(2012) 732 final.

3.3. Subsidiarity: Added value of EU action

A Special Eurobarometer[28] survey shows that the EU's strategy of sharing information at EU level to combat crime and terrorism has widespread public support: almost all respondents (92 %) agree that national authorities should share information with the authorities of other Member States to better fight crime and terrorism.

Indeed, cross-border crime can only be tackled by effective cross-border police cooperation and particularly by exchanging information. As examined in the evaluation (see Annex 4), the Prüm Decisions have proven very effective in stepping up the exchange of information between law enforcement authorities and in supporting Member States in fighting crime and terrorism. The stakeholder consultation carried out in the preparation of the impact assessment also showed a very high level of satisfaction with the Prüm Decisions.

Common EU level rules, standards and requirements facilitate these information exchanges while providing compatibility between different national systems. Information exchange at EU level also allows ensuring high-level data security and data protection standards. Additionally, as the experience with the current Prüm framework demonstrates, common standards allow for a certain level of automation in information exchange workflows which release law enforcement officers from certain labour-intensive manual activities.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1 General objectives

The general objective of this initiative results from the Treaty-based goal of contributing to the internal security of the European Union. According to Article 87(2)(a) TFEU, the Union shall establish police cooperation involving all Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences. Among measures to do so, the collection, storage, processing, analysis and exchange of relevant information is listed. The general objective of this instrument is to improve, streamline and facilitate the exchange of criminal information between Member States' law enforcement authorities, but also with Europol as the EU criminal information hub.

Law enforcement work is inherently an information-based activity. Indeed, it is essential for fighting crime that law enforcement authorities exchange data, in an efficient and timely manner. Investigators need to have fast, streamlined and systematic access to all

[28] The 'Report on Europeans' attitudes towards security' analyses the results of the Special Eurobarometer public opinion survey (464b) regarding citizens' overall awareness, experiences and perceptions of security. This survey was carried out by TNS Political & Social network in the 28 Member States between 13 and 26 June 2017. Some 28 093 EU citizens from different social and demographic categories were interviewed.

the information they need and which they are legally entitled to obtain in order to perform their tasks.

4.2 Specific objectives

The specific policy objective of this initiative is to provide law enforcement authorities with fast, streamlined and more effective access to all the information they need and which they are legally entitled to obtain in order to perform their tasks in a timely and efficient manner, while ensuring a high level of protection of fundamental rights. This objective will be achieved by:

1. Providing for 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, in line with fundamental rights including data protection requirements;
2. Ensuring that **more relevant data** (in terms of data categories) from national databases in other Member States is available to all competent law enforcement authorities, in line with fundamental rights including data protection requirements;
3. Ensuring that relevant data (in terms of sources of data) from **Europol**'s database is available to law enforcement authorities, in line with fundamental rights including data protection requirements;
4. 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, in line with fundamental rights including data protection requirements.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1 What is the baseline from which options are assessed?

The baseline is a 'no policy change' scenario.

With regard to **data categories**, the baseline would be to maintain the current data categories covered by the Prüm Decisions (DNA, fingerprints and vehicle registration data).

Regarding the **sources of data**, the baseline scenario would be to not provide for the involvement of Europol.

Regarding the **technical architecture**, the baseline would be to maintain the existing Prüm framework in its fully decentralised nature and therefore not integrated with the interoperability framework. This baseline option would not change the requirement for every Member State to connect to each other Member State's database for each data category (*see graph below*). The access to the data in the first step would be on a hit/no-hit basis only.

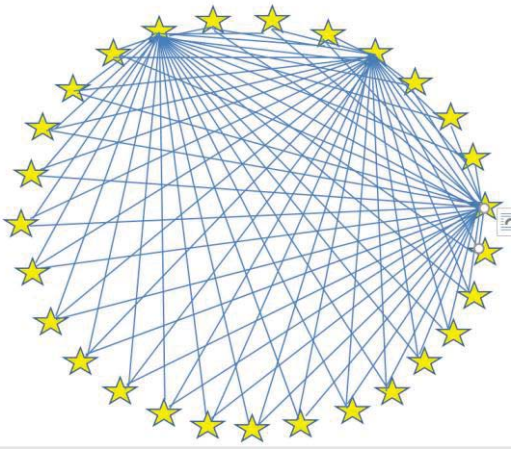


Figure 2: The current architecture of the Prüm framework

When it comes to the **follow-up process**, the baseline would be to continue to apply the follow-up as it currently takes place after a hit in the Prüm framework. In this baseline option, the exchange of "hit follow-up data" would continue to be governed by national law without common rules and processes at EU level.

All the policy options are legislative options, as the objectives could not be achieved by non-legislative options.

5.2 Description of the policy options

The specific objectives identified in section 4.2 lead to *four guiding questions* for the analysis:

a) How should the automated exchange of data be governed to make law enforcement authorities aware of all relevant data that is **available** in the national database of another Member State (**technical architecture**)?
b) What **additional data categories** are relevant and need to be covered by the automated exchange of data?
c) What **additional sources of data** are relevant and need to be covered by the automated exchange of data (**involvement of Europol**)?
d) How should the follow-up to "hits" in the automated exchange of data be governed to provide law enforcement authorities with efficient **access** to all relevant data that corresponds to the 'hit' and that is available in the national database of another Member State (**follow-up process**[29])?

5.2.1 <u>Objective I</u>: Provide for 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, in line with fundamental rights including data protection requirements

[29] The hit/no-hit approach as applied in the existing Prüm Decisions has proven its value both operationally and in terms of data protection and will therefore be maintained for the first step.

In order to address this objective, the following option is being considered: applying a **hybrid solution** between a decentralised and a centralised approach **without data storage at central level.**

This option was assessed in technical meetings with experts and stakeholders of EU Agencies and Member States.

Policy option 1.1: applying a hybrid solution between a decentralised and a centralised approach without any data storage at central level

This policy option consists of applying a **hybrid solution between a decentralised and a centralised approach without any data storage at central level**. This hybrid approach would consist of national databases in each Member State that all connect to a **central router** (*see graph below*). Under this option, the central router would not store any data but provide a **hub between national databases**. The access to the data in the first step would be on a hit/no-hit basis only.

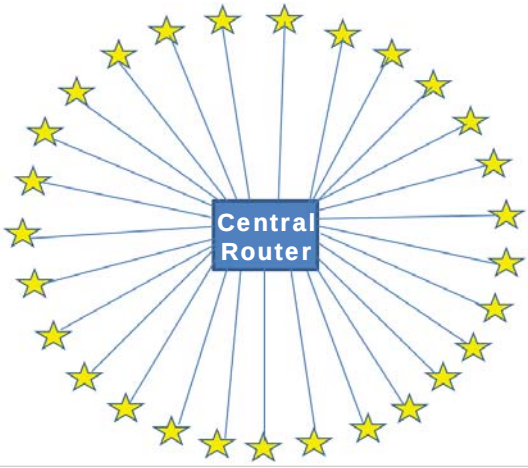


Figure 3: The possible alternative architecture of the Prüm framework, with a central router and without data storage at central level

This option is inspired by the final report of the High-level expert group on information systems and interoperability, which suggested considering "*an alternative* connectivity *via a 'hub-and-spoke' centralised Prüm router (or biometric single-search interface) replacing the current mesh network*", which would "*limit the connectivity to one link per Member State while controlling, managing and reporting on the transactions centrally*".[30] According to the High-level expert group, such a "*hub-and-spoke model could provide an effective solution to overcome the connectivity challenges that Member States are faced with, notably when establishing information exchange facilities with Member States where current traffic is not very frequent*".

The central router would serve as a connecting point between all Member States. It would drastically reduce the number of connections to establish and maintain from a

[30] See the final report of the High-level expert group on information systems and interoperability (May 2017), pp. 19f.

Member State's perspective and would facilitate the implementation of the system by Member States. As it would not store any personal data, there would not be any persistence of data in the router. Member States would retain the ownership/control over their data.

The introduction of a central router would also allow for the collection of **statistics at central level**, without having to ask Member States, on the number of requests and responses received notably, which would provide for necessary and useful transparency. Indeed, the lack of statistics and quantitative data at EU and Member States' level on the functioning of the Prüm Decisions was identified as one of the major limitations in the evaluation (see Annex 4). These statistics would allow to have a clear view of the use of the Prüm framework, per data category and per Member State. A significant use of the framework as well as the detection of matches and hits in other databases would be a strong indication of the success of the measure, as it would mean that the relevant information is at the disposal of our law enforcement authorities. Indeed, a hit indicates that information on the person for which a Member State was launching a query is found in another Member State's database. Hits may lead to solving a crime and protecting a citizen.

However, the use of the hit would fall outside of the scope of the statistics that would be collected via the central router. Indeed, the use of the information would vary according to each individual case and depending on the outcome of the investigation. These statistics could be required from the Member States in a periodical exercise.

Finally, the central router would also offer a biometric matching service. This biometric matching service would not be located in the router. Indeed, the router could use existing technology (e.g. technology similar to the one used for the shared Biometric Matching Service).[31] In doing so, the router could assess the results coming from the national databases and rematch them in order to list the potential matches in accordance with their degree of similarity. It would therefore contribute to boosting efficiency and reducing false-positives cases (matches that do not translate into hits). This service should be provided for at central level, e.g. by a Union agency.

The router would be hosted by a Union agency.

5.2.2 Objective II: Ensure that more relevant data (in terms of data categories) from national databases in other Member States is available to all competent EU law enforcement authorities, in line with fundamental rights including data protection requirements

In order to address this objective, the following three options are being considered:

- introducing the exchange of **facial images** in the Prüm framework;
- introducing the exchange of **police records data** in the Prüm framework; and

[31] See Article 12 of Regulation (EU) 817/2019 and Article 12 of Regulation (EU) 818/2019.

- introducing the exchange of **driving licence data** in the Prüm framework.

All options respond to operational needs that Member States and their law enforcement authorities raised during discussions at Council working group level, in dedicated workshops and consultations. Indeed, there has been a strong demand from Member States in the Council to broaden the scope of the automated cross-border exchange under the Prüm Decisions to other data categories.[32]

Policy option 2.1: introducing the exchange of facial images in the Prüm framework

Policy option 2.1 would allow facial images to be exchanged in an automated way under the Prüm framework.

Currently, the exchange of facial images between Member States' law enforcement authorities takes place, if at all, on a manual and case-by-case basis. This takes time and resources. There is no efficient procedure to compare facial images against images stored in other Member States' databases.

The identification of a criminal is of vital importance for a successful criminal investigation and prosecution. The introduction of facial images (*photos*) of suspects and convicted criminals under the Prüm framework, in line with operational needs, would provide for necessary additional information for successfully identifying criminals and fighting crime. Indeed, in criminal investigations, it often happens that the only lead captured from the crime scene, is an image of a suspect from a nearby security camera. Comparing this image not only to images stored in national databases, but also against images stored in other Member States' databases would significantly increase the possibilities of identifying the criminal, and could also reveal different identities used or different crimes committed by the same person in other Member States.

Member States collect facial images of suspects and criminals under national law in national criminal databases. The processes to collect these images however vary significantly between the EU Member States. In most instances, facial images are collected at police premises across the country during a process where photographs of a person are captured in parallel with the collection of fingerprints, biographic data and case data.

The process of exchanging and comparing facial images relies on the development and availability of facial recognition technology. Facial recognition technology compares images of faces to determine their similarity, which the technology represents using a similarity score. If the score computed for a candidate is under a defined threshold, this candidate is excluded. Facial images are biometric data and are therefore special categories of data in the meaning of the LED.[33]

[32] See the July 2018 Council Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption.
[33] See Article 10.

For criminal investigations, the most common use case is the **retrospective** one-to-many (1:N) search, where an image of an unknown person (e.g. an image taken from a surveillance camera) associated with a criminal event is searched against a database containing facial images of known individuals with the aim to determine the identity of the person, **after a crime has been committed**.[34] The search result is a **list of candidates** which is **reviewed by a human operator** in the requesting Member State and a decision is made on any potential match.

Similarly, under this policy option, the use case would be retrospective and related to a specific criminal investigation. The results of the search would be returned to the requesting Member State, which would proceed to the verification of these results and to the potential confirmation of a match.

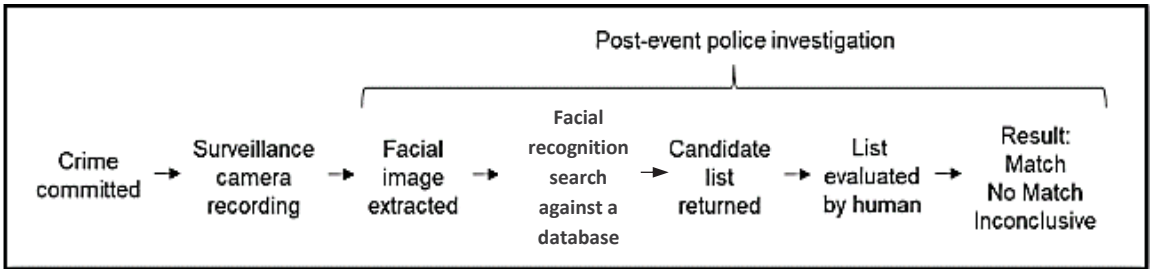


Figure 4: Retrospective use of facial recognition[35]

Finally, the proposed policy option does not require any use of artificial intelligence. The biometric comparison based on facial images should take place on the basis of a comparison of their biometric templates using pre-defined algorithms. This also means that the exchange of facial images under the Prüm framework does not provide for a remote biometric identification system to be used in publicly accessible spaces[36] and is not among the prohibited practices of the proposed Regulation for an Artificial Intelligence Act.[37] There would be no profiling entailed.

<u>Policy option 2.2</u>: introducing the exchange of police records data in the Prüm framework

Policy option 2.2 would allow police records to be exchanged in an automated way under the Prüm framework. The introduction of the exchange of police records, in line with operational needs, would provide for additional information in possibly identifying criminals and fighting crime.

[34] Summary Report of the project "Towards the European Level Exchange of Facial Images" ('Telefi Report') (January 2021), p. 14. The Telefi project was set up to look at how facial recognition is being used for the investigation of crime across EU Member States and to consider the potential for implementing the exchange of facial images within the Prüm framework.
[35] Telefi Report, p. 24.
[36] In reply to the public consultation, one stakeholder raised concerns on the risks of mass surveillance. However, under the Prüm framework, the use case would not be about live scanning/ identification of large groups of people on the street or in public events. The use case would be retrospective and related to a specific criminal investigation.
[37] COM/2021/206 final

The exchange of police records is already the subject of the **ADEP/EPRIS project** implemented by some Member States[38] on the exchange of police records. This project, supported by the Commission and launched in 2017 in order to automate the process of indicating in which Member States' databases the relevant police records could be present, aims at reducing the need for manual work and at facilitating the subsequent bilateral or multilateral exchange of information. The pilot project developed the software and tested the main business cases, and confirmed the technical feasibility of the exchange of police records. From 2019, the second iteration of the project further developed the business-related processes and prepared the rollout of the system. The project is currently being tested in Business Acceptance Tests with "real" operational data. The policy option would extend this project to all Member States and allow for all Member States' participation in the exchange of police records.

Currently, the exchange of police records between Member States' law enforcement authorities takes place, if at all, on a manual and case-by-case basis. This takes time and resources. There is no efficient procedure to find out whether relevant information on police records exists in another Member State's database. Extending the project to all Member States and providing for the automated exchange of police records data under the Prüm framework is the only way to remedy the current information gap due to long and inefficient procedures.

ADEP/EPRIS allows checking whether any police records exist in other Member States' national police records databases on a hit/no hit basis. In case of a hit, a request to exchange further personal and case-related data is sent only to those Member States where a hit occurred. For that purpose, participants have to establish indexes of national police record databases, which will contain the limited data accessible in an automated way under the project. These indexes typically include data from all national databases that the police normally checks when receiving information requests from other law enforcement authorities. Data protection safeguards include **pseudonymisation**, as indexes and queries do not contain clear personal data, but alphanumerical strings.[39]

Under this policy option, a limited data set of data from police records (i.e. surname, first name, date of birth, place of birth, gender) to identify a Member State possibly holding more information on a person under investigation could be exchanged in an automated way, once a "hit" has been confirmed. The following fields of data are pseudonymised: surname, first name and place of birth.

The automation of the process of finding out whether relevant information exists or not in another Member State would reduce the need for manual work and save resources. In case the automated search yields no results, competent law enforcement authorities do

[38] FR, DE, FI, IE, ES, BE. For more information, see https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/Polizei2020/EPRIS_ADEP/EPRIS.html.

[39] Strings that contain only alphabets from a-z, A-Z and some numbers from 0-9.

not have to process the request and retrieve the information, thereby saving time and resources.

This policy option would imply the setting up of national indexes on police records by Member States who have not yet set up such indexes. These indexes would be based on data from national databases containing information on police records (without containing the police records themselves). The definition of the composition of national indexes on police records would be up to each Member State, but should be limited to the sets of data mentioned above.

The creation of national indexes and the connection of these indexes to the central router (see section 5.2.1) would remain optional and on a voluntary basis, due to political feasibility. However, the usefulness of the exchange of police records would grow exponentially the more Member States participate. The exchange of police records would still be useful if only a few Member States participate.

Policy option 2.3: introducing the exchange of driving licence data in the Prüm framework

Policy option 2.3 would allow driving licence data to be exchanged in an automated way under the Prüm framework.

The introduction of the exchange of driving licenses under the Prüm framework would provide for additional information in supporting criminal investigations and possibly identifying criminals.

Member States are already exchanging driving licence information through the Resper application,[40] although not for law enforcement purposes. In the majority of Member States, law enforcement authorities have access to national driving licence databases. Under the principle of availability,[41] law enforcement authorities of other Member States could also be granted access to the same information under the same conditions as the national law enforcement authorities.

Driving licence information would be relevant in cases of possible fake IDs, for either corroborating or nullifying the trustworthiness of the documentation and verifying the identity of a suspect.

5.2.3 Objective III: Ensure that relevant data (in terms of sources of data) from Europol's database is available to law enforcement authorities, in line with fundamental rights including data protection requirements

In order to address this objective, the following two options are being considered:

- enabling Member States to check automatically **third-country sourced data at**

Europol as part of the Prüm framework; and

- enabling **Europol** to check third-country sourced data **against the national databases** of Member States.

Both options were assessed in technical meetings with experts and stakeholders of EU Agencies and Member States. As point of departure, it was understood and agreed by all that in all scenarios Europol's involvement in the automated exchange would need to be in accordance with the objectives and tasks set out in the Europol Regulation,[42] and hence limited to data processing that is necessary to support Member States in preventing and combating serious crime and terrorism.

Policy option 3.1: enabling Member States to check automatically third-country sourced data at Europol as part of the Prüm framework

Policy option 3.1 would allow Member States to search and compare biometric data received by Europol from third countries with their own biometric data.

Biometric data is exchanged between Member States and third countries only bilaterally and on a case-by-case basis. Europol, due to its unique position, has the possibility to facilitate access to relevant third-country sourced data. In recent years, Europol has received from several third countries (e.g. US, Australia, Canada, Western Balkans) a large amount of biometric data of known terrorists and top criminals. Under this policy option, these data could be made available to Member States for searching via the Prüm framework. After a match against Europol third country-sourced data in Prüm, Member States could follow up with the third country in question via bilateral police cooperation channels, if relevant. The information about a match would never be revealed to the third country.

Including third country-sourced data stored at Europol in the already established and functioning Prüm framework would contribute to building synergies between different law enforcement tools and would streamline queries with similar data and for similar purposes.

This policy option in conjunction with policy option 1.1 would not require any additional financial or technical resources from the Member States. However, should policy option 1.1 be discarded, it would require all Member States to establish bilateral connections with Europol to enable the exchange of data. For Europol, this policy option would require certain IT developments, e.g. developing a technical interface to allow for searches with biometric data by Member States, connections to the Prüm architecture, as well as upgrading the capacity of their biometric matching service and network.

Policy option 3.2: enabling Europol to check third-country sourced data against the national databases of Member States

[42]Regulation (EU) 2016/794 (11 May 2016), articles 3 and 4.

Policy option 3.2 would allow Europol to cross-check data received from third countries by directly searching Member States' biometric databases in order to establish links between the information received from third countries and Member States' databases.

Under this policy option, Europol could search Member States' databases under the Prüm framework with data from third countries in order to establish any cross-border matches between criminal cases. In case of a match, only the Member State whose data created a match would be notified of it, no information on a hit would be provided to the third country in question. Once informed of the existence of such matches, the decision on whether to bilaterally follow up on these or not with the third country in question would be incumbent to the Member State(s) concerned. Being able to use Prüm data, next to other databases available for Europol, would allow establishing more complete and informed analysis on the criminal investigations and would allow Europol to provide better support to Member States.

This policy option would increase Europol's contribution to Europe's safety. Indeed, Europol's role has been significantly reinforced in recent years as the EU law enforcement information hub. Moreover, information about criminals and terrorists shared by third countries with the EU is increasingly relevant for EU internal security.

This policy option would require reinforcing Europol with operational staff to conduct searches with third-country sourced data and with biometric experts to verify the search results. Additionally, it would require ICT developments to establish a connection to the Prüm framework. Similarly as for option 3.1, this policy option in conjunction with policy option 1.1 would not require any additional financial or technical resources from the Member States. However, should policy option 1.1 be discarded, it would require all Member States to establish bilateral connections with Europol to enable the exchange of data. In case policy option 3.1 is retained, policy option 3.2 would not require any additional costs for Europol (except operational costs).

5.2.4 Objective IV: 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 in line with fundamental rights including data protection requirements [43]

In order to address this objective, the following option is being considered: regulating the follow-up process at EU level with a **semi-automated exchange of actual data corresponding to a 'hit'**.

This option was assessed in technical meetings with experts and stakeholders of EU Agencies and Member States.

Policy option 4.1: regulating the follow-up process at EU level with a semi-

[43] The hit/no-hit approach as applied in the existing Prüm Decisions has proven its value both operationally and in terms of data protection and will therefore be maintained for the first step.

automated exchange of core data

Policy option 4.1 would allow the exchange of **core data** under the Prüm framework **in a semi-automated way**.

Regulating the exchange of hit-follow-up data under the Prüm framework would speed up the procedure. To that end, once a hit has been confirmed, a well-defined limited set of "core data", with data limited to what is necessary to enable the identification of a person could be returned to the requesting Member State. This set of core data would be well-defined and it would not differ between Member States.

In reply to the public consultation, one stakeholder highlighted the importance of a mandatory manual review in the requested Member State and the possibility for the requested Member State to refuse disclosure of further personal data. Under this option, Member States would retain control over the release of this limited set of core data. Indeed, **a certain degree of human intervention would be maintained at key points in the process**, including a decision to release personal data to a requesting Member State.

After the reception of this core data set and if needed, Member States could request additional information in a third step, using traditional law enforcement cooperation channels such as SIENA. The exchange of information in this third step would remain outside the scope of the Prüm framework.[44]

5.3 Options discarded at an early stage

This section presents different options related to the four identified problems, which were not retained for consideration in this impact assessment for several reasons, as explained below.

- In relation to problem I, one option was to apply an **extended hybrid solution between a decentralised and a centralised approach with some data storage at central level**. This hybrid approach would consist of national databases in each Member State that all connect to a central router, **with some data stored in the central router.** The access to the data in the first step would be on a hit/no-hit basis as regards data in the national databases, and direct access to the data stored in the central router.

  However, this option was not retained as Member States have consistently expressed strong opposition to any storage of data at central level in the context of the Prüm framework, mainly in light of sovereignty concerns. Member States want to retain control/ownership over their data. This policy option would also result in duplication of data, which would have a greater impact on the right to data protection.

[44] This will be further defined under the Police Cooperation Code (PCC) initiative. The Inception Impact Assessment is available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12614-EU-police-cooperation.

- In relation to problem II, one option was to **introduce the exchange of firearms-related data in the Prüm framework**, which would allow firearms-related data to be exchanged in an automated way under the Prüm framework. Under this option, law enforcement authorities in one Member State could search and compare a firearm, which they have apprehended and which is not registered in the national registry, against other Member States' national registries.

  However, this option was not retained due to the **lack of evidence on the necessity to automate these exchanges**. Indeed, national databases contain legal firearms registration data, thus not the information needed for investigations on illegal firearms. Moreover, the most relevant firearms data – illicit, wanted, stolen and lost firearms – is already stored, compared and exchanged in EU and international firearms systems (the Europol Information System (EIS), the Schengen Information System (SIS) and Interpol's Illicit Arms Records and tracing Management System (iARMS)). Additionally, as stems from consultations with Member States, the number of cases in which a firearm used in a crime is not registered in the national database and has not been reported as illicit, wanted, lost or stolen is limited and therefore does not justify the necessity to automate firearms-related data exchanges. Moreover, other solutions could be best suited to achieve this purpose, notably traditional law enforcement cooperation channels such as SIENA and national firearms focal points. The European Commission has promoted the creation of National Firearms Focal Points (NFFPs) in each Member State, where Member States would centralise the national access to all types of firearm-related information and the communication of firearm-related data with other Member States, through secure channels (such as Europol's Secure Information Exchange Network Application (SIENA)).

- In relation to problem II, one option was to **introduce the exchange of ballistic data in the Prüm framework**, which would allow ballistic data to be exchanged in an automated way under the Prüm framework.

  However, this option has not been retained due to the technology not being ready for it at this stage. Indeed, currently, there are **different ballistics identification systems** which are used by Member States across the EU to acquire, compare and exchange ballistic data and which are **not interoperable**. This means that ballistic data cannot be exchanged between two different ballistics identification systems. There are some initiatives ongoing to develop a common standard that would allow for exchanges between users of these different systems, the X3P format. This development of the X3P format could lead to a future re-assessment of this option if it reaches a sufficient level of maturity to allow for exchanges between these systems.

- In relation to problem III, one option was to **enable Europol to check all operational data against the national databases of Member States**. This option is similar to policy option 3.2 except that it would allow Europol to compare **all** operational data it receives from Member States against the national databases of

Member States, to make Member States aware of links that they might not be aware of. Under this option, Europol would be acting on behalf of the Member States, realising operations on their behalf.

This option has been discarded in light of strong opposition expressed by Member States in the technical workshops organised in the context of the revision of the Prüm Decisions. Indeed, Member States can actually perform these checks without necessarily having Europol do it for them. Moreover, non-legislative measures like encouraging Member States to use the data they have access to under Prüm are preferable to this option.

- In relation to problem IV, one option was to **regulate the follow-up process at EU level with an automated exchange of core data**. Under this option, once a hit has been confirmed, a well-defined limited set of "core data", enabling the identification of a person, would be returned to the requesting Member State in an automated way. There would be no human intervention before the release of the core set of data. This option has been discarded as Member States have expressed their wish to manually authorise the release of personal data and their opposition to the fully automated return of core data.[45]

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This chapter assesses all policy options identified in section 5.2 and which have not been discarded in section 5.3 against the baseline options identified in section 5.1. Given that the baseline scenario is evidently unsuited to address the problems identified in section 2 on the problem definition, this impact assessment will not assess the baseline scenario any further.[46]

Given the importance of cross-border cooperation and of the exchange of information between law enforcement authorities for fighting crime, as mentioned in the introduction section 1, the main social impacts of the policy options assessed in this chapter cover the impact on fighting crime and the wider implications for EU citizens' security and well-being.

The following impacts will not be addressed per policy option:

1) **Environmental impact:** No impact is expected on the environment because the policy options do not include any environmental aspect.

[45] The EU Commission mandated a consulting firm (Deloitte) to conduct a study on the feasibility of improving the exchange of information under the Prüm Decisions. "Study on the Feasibility of Improving Information Exchange under the Prüm Decisions: Advanced technical report", https://op.europa.eu/en/publication-detail/-/publication/3236e6ae-9efb-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search ('Feasibility Study'), see p. 63.

[46] For more information on the necessity and proportionality of exchanging DNA, fingerprints and VRD (as the baseline), please see the evaluation of the Prüm Decisions in Annex 4.

2) **Economic impact:** Immediate economic impacts of any of the above options will be limited to the design, development and operation of the new processes. The costs will fall to the EU budget and to Member State authorities operating the systems. The proposed measures are not expected to have an impact on small and medium-sized enterprises as the policy options will not affect small and medium-sized enterprises.

As the exchange of personal data is an important aspect of the various policy options examined in this impact assessment, this chapter puts a particular focus on the assessment of the impact on fundamental rights. Therefore, we explain the methodology used during this exercise.

In accordance with the Charter of Fundamental Rights of the EU, to which EU institutions and Member States, when they implement EU law, are bound (Article 51(1) of the Charter), 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 to the **protection of people's right to life** (Article 2 of the Charter), 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,[47] as well as to uphold the prohibition of slavery and forced labour (Article 5).

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,[48] the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society. In particular, in line with Article 52(1) of the Charter, **limitations may be imposed on the exercise of the right to data protection** as long as the limitations are **provided for by law**, **respect the essence of the right** and freedoms and, **subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest** recognised by the European Union or the need to protect the rights and freedoms of others. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(2) of the General Data Protection Regulation,[49] which indicates that the EU protects

[47] European Court of Human Rights, Osman v United Kingdom, No. 87/1997/871/1083, 28 October 1998, para. 116.
[48] 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.
[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. No potential harmful effect of the policy options on other fundamental rights has been identified, as the impact of these policy options is limited to impacts on the right to the protection of personal data.

With that in mind, when assessing the impact on fundamental rights, two main aspects will first be taken into account:

1) Does the measure **meet an objective of general interest**? And, if so, how does it contribute to said objective?

2) Does the measure have an **impact on the right to data protection**?

Concerning the impact on the right to data protection, it is worth noting that in the context of the Prüm framework, the applicable legislation in the context of the data protection framework is Directive (EU) 2016/680.[50] 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):

- it must be provided for by law;
- it must respect the essence of the rights;
- it must genuinely **meet objectives of general interest** recognised by the Union or the need to protect the rights and freedoms of others;
- it must be **necessary**; and
- it must be **proportional**.

The discussions concern a new legal proposal, which will allow the relevant option to be provided for by law.

Moreover, concerning the respect of the essence of the rights, in the case of the measures proposed, similarly to what happens today with the existing Prüm framework, the right to the protection of personal data is affected only to a limited extent. However, despite

[50] 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.

being limited, the impact on the right to the protection of personal data must be assessed to determine whether it is necessary and proportional.

Each of the options meet an objective of general interest, which is the safeguarding of the interal security of the European Union and which is assessed previously. Therefore, for each option, under the heading 'impact on data protection', the following two criteria will be assessed:

(a) Are they **necessary**?

(b) If so, are they **proportional**?

The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'neutral' (0) and 'negative impact' (-).

6.1 Improve the technical architecture

6.1.1 Policy option 1.1: applying a hybrid solution between a decentralised and a centralised approach without any data storage at central level

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to **support law enforcement authorities** in the exercise of their tasks by ensuring all available data is used in the context of criminal investigations and thus would contribute to enhancing the security and well-being of EU citizens.

b. Impact on national authorities (++)

Very positive impact on national authorities. The central router would serve as a **connecting point between all Member States**. It would **drastically reduce the number of connections** to establish and maintain from a Member State's perspective and would facilitate the implementation of the system by Member States, including any future changes. Any time a new category of data is introduced in the system or a new user is added, they would just require to establish one connection to the router instead of one to each other Member State.

c. Impact on fundamental rights

i. Objective of general interest (+)

Positive impact on the security of the European citizens and societies. The router as described under Section 5.2.1 is a message broker with the specific purpose of ensuring that end-users, namely law enforcement officers, have fast, seamless and controlled access to the information that they need to perform their tasks and in line with their

access rights. It would also facilitate the implementation by Member States of existing and future data exchanges in the context of the Prüm framework. The router would **support information exchange in an effective and efficient way**.

The router would also allow for the **collection of central statistics** on the use of the Prüm framework, which would contribute to its evaluation, to the monitoring of its use and finally to its improvement over the years.

Finally, the router would also **offer a biometric matching service**, contributing to ranking the results of the searches in order to boost efficiency and reducing the cases of false-positives (matches that do not translate to hits).

The router would do all of the above without enlarging access rights and without replacing national databases, thus respecting the national prerogatives of the Member States. Therefore, we consider the measure **proportionate** to the objective of general interest pursued.

ii. Impact on data protection (0)

1. Necessity

The router provides law enforcement authorities a new and more efficient tool to search Member States' data in the Prüm framework. Law enforcement authorities are already legally entitled to establish connections today but sometimes do not have the operational or technical capability to create the necessary connections. Moreover, the current situation requires each Member State to have as many connections as Member States participating in the framework multiplied by the number of data categories. The router would just require every Member State or Union Agency exchanging data via the Prüm framework to create one connection: to the router.

We therefore conclude that the policy option **respects the principle of necessity**.

2. Proportionality

The actual impact of the router in terms of data processing is very limited. The router only envisages a single operation of forwarding search transactions and replies to various national systems. It would serve as a message broker. These data processes can already take place today. **No new data processes would be created by the router**.

The router would not store any data, except the logs, to keep track of the use of the router and facilitate supervision of access rights.

Indeed, the router is consistent with the idea of interoperability: by technical means, it would contribute to facilitating and streamlining access to data to authorities that already have it. Therefore, **access rights are not enlarged** nor is data retention impacted by this policy option.

Creating a router and centralising searches through it delivers economies of scale and efficiency gains.

The revised Prüm framework would provide for the creation of the central router and its functionalities and architecture. Concerning data protection, the applicable legislation regarding the central router will be the Law Enforcement Directive. The future Prüm Regulation will also include a dedicated chapter on data protection laying down any specific provision regarding the router in full respect of the Law Enforcement Directive (e.g. exercise of rights, indication of who is data controller and data processor, data security, logging, etc.).

We therefore conclude that the policy option **respects the principle of proportionality**.

d. Costs (++)

	Member States activities	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	0.611	9.050
Expected yearly recurring costs (in million EUR)	0.122	1.100

The cost estimation for the central router includes both the setup of the router, the setup of middleware handling web services requests, including the integration layer, and the establishment of new connections from Member States to the router. In order to ensure the need for high availability and reliability, redundancy is required to make the tool robust. This cost has been included in the estimations.

A single router (and its redundant/back-up router) will be set up. This router will handle the communication of all biometric data exchanges (fingerprints, DNA and facial images) using the same Web service and NIST standard. The router should be able to handle every request and send the request to the appropriate national systems. The central router is expected to re-use wherever possible already existing IT infrastructure to support its implementation. However, additional infrastructure-related costs are foreseen to complete the already present infrastructure.

Once the router is up and running, **the yearly recurrent costs for Member States for the operation of the Prüm framework should decrease**. Moreover, the router has a positive impact on the costs for the remaining options.

The total cost is distributed as follows:

- Setup of the central router and help to Member States in the connection of their national systems at EU central level.
- Setup of the web services middleware and connecting the national systems to the central router by the Member States.

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;
- generic costs linked to project management.

The costs at EU level include:

- designing the details of the technical architecture, defining clear processes and the harmonization with existing initiatives;
- building the backbone infrastructure, the integration layer(s) at EU level, basic reporting capabilities;
- integrating the router with existing architecture at EU level;
- generic costs linked to project management.

e. Feasibility (+)

Concerning **technical feasibility**, this policy option would imply the creation of a central router, to which Member States would need to establish one connection. It stemmed from discussions in the technical workshops organised in the context of the revision of the Prüm Decisions that there is a common understanding among experts on the general technical feasibility of the introduction of a central router in the Prüm framework. Moreover, technical components offering similar (if not even greater) services are being implemented (e.g. the European Search Portal introduced via the interoperability Regulations). This also probes the feasibility of the Prüm router.

Concerning **political feasibility**, in reply to the public consultation, most respondents agreed that the fact that the existing Prüm framework is a decentralised network of bilateral connections between Member States' national databases is a shortcoming of the existing Prüm framework. When asked what they consider to be the most appropriate means to address this shortcoming, most replied establishing an EU central router for transferring messages between Member States with limited functions at a central level such as technical/operational system monitoring and collection of statistics. One respondent highlighted that if a central router were to be put in place, it should only serve as a pass-through server to transmit messages between Member States, and the collection of statistical data.

We therefore conclude that **the measure is feasible**.

6.2 Automated exchange of additional data categories

6.2.1 Policy option 2.1: introducing the exchange of facial images in the Prüm framework

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks and thus would contribute to enhancing the security and well-being of EU citizens. Only facial images of suspects and convicted criminals would be exchanged.

b. Impact on national authorities (++)

Very positive impact for national law enforcement authorities. In a number of criminal investigations, the only lead or the main lead on a suspect or perpretator of a criminal offence are facial images. While today the exchange is possible, there is no efficient procedure to do so, and it happens in a **time-consuming and inefficient way**. This has negative impacts both on officers' workload as well as in the investigations, even more so in those cases where time is of the essence. Providing for the possibility to know whether another Member State has at its disposal information in your case would provide a significant boost to law enforcement authorities' work regarding criminal investigations and prosecution of criminals.

c. Impact on fundamental rights

i. Objective of general interest (++)

Very positive impact on the internal security of the European Union. The introduction of the automated exchange of facial images in the Prüm framework would provide law enforcement authorities with **faster and more reliable access to relevant information**, which could be crucial in their investigations, and could contribute to identifying criminals and solving criminal cases.

Only facial images of suspect or convicted criminals and terrorists could be exchanged. This means that there would be no matching of facial images to the general population. Moreover, no use of artificial intelligence is provided for. Therefore, we consider the policy option proportionate to its objective of general interest.

ii. Impact on data protection (-)

1. Necessity

As mentioned above, in a number of criminal investigations, the only lead or the main lead on a suspect or perpetrator of a criminal offence are facial images. In an area without

internal borders, cooperation between Member States is crucial in resolving criminal investigations. Therefore, it is necessary for law enforcement authorities to work with their peers in other Member States. Today, exchanges of facial images are possible, but there is no efficient procedure to do so, leading to errors, information gaps and reluctance to use it by law enforcement authorities. Despite this fact, exchanges of information still take place as they are deemed necessary. When it does take place, the current process is currently both time-consuming and inefficient (there are no automated queries, everything needs to be done manually).

Moreover, today, any exchange of facial images would be done manually and in a bilateral framework. For the sake of efficiency, Member States would tend to only send queries to those Member States which they believe could have data on the suspect or convicted criminal concerned. However, experience has already demonstrated that another Member State can sometimes have relevant data for the criminal investigation on that person. This is all the more relevant in an area without internal borders such as the Schengen area. Exchanging facial images via the Prüm framework would ensure that there is no such gap and that all relevant data may be available to law enforcement officers.

Providing for the exchange of this category of data at EU level in the Prüm framework would significantly improve its efficiency. There are no other effective but less intrusive options, the policy option is essential and limited to what is necessary to achieve the specific objective.

We therefore conclude that the measure has a negative impact on data protection as the processing of a new category of data is created but respects the principle of necessity.

2. Proportionality

The exchange of facial images under the Prüm framework will not lead to storing new categories of data. Indeed, Member States already collect facial images of suspects and criminals under national law and store them in national criminal databases.

The exchange of facial images between Member States constitutes a new processing of data. However, it is limited to the extent necessary to achieve its purpose, it only allows for comparison of data in case-by-case situations, and provides several safeguards. As it concerns biometric data, which is considered a special category of personal data under the LED, the processing is permitted in order to protect the vital interests of natural persons (fight against crime and terrorism).

Moreover, still in accordance with the LED, appropriate safeguards must be provided for. First, there is no fully automated exchange. Second, the exchange of facial images will not entail the possibility for live facial recognition screening of a large number of persons in public spaces. This is not the objective of the Prüm framework. Instead, both the scope and the principles used will be similar to those applicable to the exchange of fingerprint data under the Prüm Decisions. Any search and comparison of individual facial images would take place in the course of criminal investigations on a “hit”/”no hit” basis against

Member States' databases of suspects and convicted criminals, **subject to forensic verification** of the results. The exchange of further personal data would take place only after confirmation of a "hit" by experts. Third, there is no envisaged use of artificial intelligence for the comparison of facial images. The comparison should be performed based on pre-defined rules and values detailed in the technical specifications. Profiling would be explicitly prohibited.

National law would be applicable to any data exchanges insofar as it does not go against the obligations and limitations set up in the revised Prüm framework. Concerning data protection, national law transposing the Law Enforcement Directive would be applicable to data exchanges between Member States.

We therefore conclude that the measure respects the principle of proportionality.

d. Costs

	Member States & Europol* ***activities***	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	2.274	0
Expected yearly recurring costs (in million EUR)	0.455	0

*Europol should only be taken into account if policy options 3.1 and 3.2 are kept.

The table presents the costs per Member State, both those expected as initial costs (one-off) and operational costs (yearly recurrent costs). The main cost driver is related to implementation and facial recognition license costs. This cost is estimated at EUR 1.5 million per Member State and will cover the implementation of a facial recognition system (included as part of the expected one-off costs).

The costs per Member State also include:

- the need to organize a tender to purchase the facial recognition system, and update the national architecture based on the system that will be selected and implemented;
- the purchase of a facial recognition system and its installation. However, Member States should already possess a facial images database. Therefore, limited resources should be allocated to a database;
- the setup of an integration layer needed to automatically exchange data with other Member States;
- generic costs linked to project management.

e. Feasibility (+)

Technical aspects and the feasibility of including the exchange of facial images in the Prüm framework were discussed in the Feasibility Study and in the focus group report on facial recognition.[51] Both reached the same conclusion and recommended such an inclusion. The focus group agreed that face recognition technology has advanced and become a highly suitable additional biometric tool in forensics.

Even though not all Member States currently have the necessary technical requirements, such as a national database with reference images or a national facial recognition software, numerous Member States are currently in the process of implementing such databases and facial recognition software.[52]

Concerning political feasibility, the main aspects are the need for explaining that the exchange of facial images is possible today, however not in an automated manner and that the inclusion of facial images under the Prüm framework would not allow for live facial recognition screening of a large number of persons in public spaces.

We therefore conclude that the measure is feasible.

6.2.2 Policy option 2.2: introducing the exchange of police records data in the Prüm framework

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks and thus would contribute to enhancing the security and well-being of EU citizens. Only police records of suspects and convicted criminals would be exchanged.

b. Impact on national authorities (++)

Very positive impact for national law enforcement authorities. While today the exchange of police records is possible, there is no efficient procedure to do so. The automation of the process of finding out whether relevant information exists or not in another Member State would reduce the need for manual work and save resources. In case the automated search yields no results, competent law enforcement authorities would not have to process the request and retrieve the information, thereby saving time and resources.

[51] Four Member States-led focus groups were established in the following areas: DNA, facial recognition, fingerprints and vehicle registration data. Council documents 11264/19, 13356/19, 13511/19 and 13556/19 (not publicly available).

[52] The Telefi Report has found that (as of December 2020), facial recognition has been implemented in 11 EU Member States (Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, The Netherlands and Slovenia) and in the UK, and 7 EU Member States (Croatia, Cyprus, Czech Republic, Estonia, Romania, Spain and Sweden) have reached the stage of preparing for implementation and expect to start using the technology within one to two years.

c. Impact on fundamental rights

i. Objective of general interest (+)

Positive impact on the security of the European citizens and societies. The introduction of the exchange of police records data in the Prüm framework would provide law enforcement authorities with additional information, which could be relevant in their investigations, and could contribute to identifying criminals and solving criminal cases.

This policy option implies only exchanges of police records linked to criminal or terrorist investigations. The measure does not provide for new access rights, and just seeks to enhance cooperation between Member States based on the principle of availability. This is all the more relevant in an area without internal borders such as the Schengen area. Therefore we consider the policy option proportionate with its objective of general interest.

ii. Impact on data protection (-)

1. Necessity

In the context of criminal investigations, information on suspects and perpetrators of criminal offences already in possession of the law enforcement authorities is crucial. In an area without internal borders, cooperation between Member States is crucial in resolving criminal investigations. Therefore, it is necessary for law enforcement authorities to work with their peers in other Member States. Today, exchanges of police records may be possible, but there is no efficient procedure to do so, and it happens in a time-consuming and inefficient way. This led to the creation of the ADEP/EPRIS project by a certain number of Member States. This policy option seeks to formalise and extend the possibility of using a tool such as ADEP/EPRIS across all Member States in the framework of the Prüm Decisions.

Indeed, the only way to improve the situation, and deal with the currently existing information gap due to long and inefficient procedures is by providing for automated exchange of this data at EU level, and therefore, under the Prüm framework. There are no other effective but less intrusive options, the policy option is essential and limited to what is necessary to achieve the specific objective.

We therefore conclude that the measure has a negative impact on data protection as the processing of a new category of data is created but respects the principle of necessity.

2. Proportionality

The exchange of police records under the Prüm framework will not lead to storing new categories of data. Indeed, all Member States possess police records under national law and store them in national criminal databases.

The exchange of police records between Member States constitutes a new processing of data. However, it is limited to the extent necessary to achieve its purpose, it only allows

for comparison of data in a case-by-case situation. The data concerned is pseudonymised, and would only cover a limited data set of data from police records (e.g. name, date of birth, place of birth, gender).

The policy option also provides several safeguards. First, there is no fully automated exchange. Second, in accordance with the privacy-by-design principle, the data would undergo a pseudonymisation process. As mentioned in section 5.2.2, indexes and queries do not contain personal data, but alphanumerical strings.[53] This, together with the fact that the actual data would not be stored, means that Member States' data cannot be automatically accessed.[54] This policy option also presents a two-step approach. In the first step, only a limited set of data from police records is used to identify the Member State possibly holding more information on a person under investigation. In the second step, once the hit has been confirmed, the Member State can ask for the actual information contained in the police record.

National law would be applicable to any data exchanges insofar as it does not go against the obligations and limitations set up in the revised Prüm framework. Concerning data protection, national law transposing the Law Enforcement Directive would be applicable to data exchanges between Member States.

We therefore conclude that the measure respects the principle of proportionality.

d. Costs

	Member States activities	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	1.527	1.666
Expected yearly recurring costs (in million EUR)	0.305	0.333

The cost estimation is based on the implementation of the ADEP/EPRIS solution.

The costs per Member State include:

- designing a new national architecture and the specifications to ensure the access of national data through the developed solution;
- setting up a new index or making an already existing index available. Regardless of the option, costs will have to be borne by Member States. The costs will differ depending on the option chosen;

[53] Strings that contain only alphabets from a-z, A-Z and some numbers from 0-9.
[54] Feasibility Study p. 94.

- integrating the national solution;
- generic costs linked to project management.

The costs at EU level include:

- designing the details of the technical architecture, defining clear processes and harmonizing with existing initiatives;
- the backbone infrastructure and the (possible) need for integration layer(s) at EU level;
- further development of the current ADEP/EPRIS solution.

e. Feasibility (++)

The technical feasibility of establishing an automated exchange of biographical data has been demonstrated in the two iterations of the ADEP/EPRIS project.

Concerning the political feasibility, in their contributions to the public consultation, Member States generally stated their support for the inclusion of the exchange of biographical data in the Prüm framework. Some Member States have expressed concerns as to this inclusion, especially concerning the increase in the number of requests and hence the increase of the burden on the authority processing these requests. It is true that the number of potential requests could potentially increase due to the possibility to query the indexes of all Member States at once. However, as examined above, the automation of the process of finding out whether relevant information exists in another Member State would save time and resources. Moreover, manual work would only be required for the queries, which resulted in a hit.

We therefore conclude that the measure is feasible.

6.2.3 Policy option 2.3: introducing the exchange of driving licence data in the Prüm framework

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks and thus would contribute to enhancing the security and well-being of EU citizens.

However, the measure also has a negative impact for citizens as it means that all citizens who have a driving licence would be potentially subject to information exchange in the context of the Prüm framework. They should be informed about this potential processing of their data.

b. Impact on national authorities (++)

Very positive impact on fighting crime and on the security of the European citizens and societies. The introduction of the exchange of driving licence data in the Prüm framework would provide law enforcement authorities with additional information, which could be relevant in their investigations, and could contribute to identifying criminals and solving criminal cases.

c. Impact on fundamental rights

i. Objective of general interest (-)

Positive impact on the security of the European citizens and societies. Exchanging data on driving licence information would be relevant in cases of possible fake documents, for either corroborating or nullifying the trustworthiness of the documentation and verifying the identity of a suspect or perpetrator.

However, despite bringing a potentially very positive impact on the security of the European citizens, the databases of driving licenses holders is not limited to criminals and terrorist but to the general population. Therefore, it is difficult to justify that the measure is proportionate to the objective pursued. This fact offsets the positive impact on security.

ii. Impact on data protection (--)

1. Necessity

In the context of criminal investigations, any information on suspects and perpetrators of criminal offences is crucial. In an area without internal borders, cooperation between Member States is crucial in resolving criminal investigations. Indeed, if a Member State's national travels to another Member State, this second Member State cannot check its national databases to verify the validity of the document submitted by the other Member State. Indeed, most Member States' law enforcement authorities have access to the national driving licence register in the context of crime investigations.

Therefore, the only way for other Member States' law enforcement authorities to have access to it would be via information exchange at EU level. The Prüm framework provides this, there are no other effective but less intrusive options, the policy option is essential and limited to what is necessary to achieve the specific objective.

We therefore conclude that the measure respects the principle of necessity.

2. Proportionality

There are several means to combat possible fake documents, for either corroborating or nullifying the trustworthiness of the documentation and verifying the identity of a suspect or perpetrator. This includes security features in the identification documents among others.

The data would be of an administrative nature as the needs of exchanging this data would not only be limited to cases of criminal investigations. Therefore, it should also be

explored whether this information exchange could not be done in a different context than the Prüm framework.

In addition, the measure concerns the processing of data of a large share of the population. Moreover, driving licenses are only one among other documents allowing for the identification of a person, such as ID cards or passports. The reason why only driving licenses would be targeted by the measure has not been sufficiently demonstrated.

We therefore conclude that the measure does not respect the principle of proportionality.

d. Costs (0)

The impact in terms of costs of this measure are not estimated as the measure does not respect the principle of proportionality.

e. Feasibility (0)

The technical feasibility of establishing automated exchanges on the basis of alphanumerical data has already been demonstrated (e.g. driving plates). Most Member States have an online driving licence register. As stems from consultations with Member States in the form of targeted questionnaires and discussions in the technical workshops organised in the context of the revision of the Prüm Decisions, most Member States reported that their law enforcement authorities investigating crime have access to the national driving licence register. Therefore, under the principle of availability, access to other Member States' law enforcement authorities could be granted under the same conditions as the access for the national authorities.

Member States have highlighted the added value of the exchange of driving licence information, especially for identification purposes, but also to help in detecting document forgery, use of a false identity, look alike fraud, etc. It stems from contributions to the public consultation and from consultations that there is an overall strong support for the inclusion of this new data category in Prüm.

On the other hand, allowing for exchanges of databases on citizens should only be done where it is strictly necessary and proportionate.

The measure is therefore neutral when it comes to feasibility.

6.3 Involve Europol

6.3.1 Policy option 3.1: enabling Member States to check automatically third-country sourced data at Europol as part of the Prüm framework

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks by ensuring all available data is used in the context of criminal investigations and thus would contribute to enhancing the security and well-being of EU citizens.

b. Impact on national authorities (++)

Very positive impact for national law enforcement authorities. The possibility for Member States' law enforcement authorities to check third-party data held at Europol in the Prüm framework would contribute to the efficiency of their work. Indeed, it would allow for using data which they are already entitled to use in an effective manner and at the same time as checking other Member States' data.

c. Impact on fundamental rights

i. Objective of general interest (++)

Very positive impact on the security of the European citizens and societies. Data provided by third countries on criminals and terrorists is even more important in an open society in a globalised world. It would allow for the potential identification of criminals known by countries outside the EU, while 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. With this option, third-country data would be turned into valuable information for its use in criminal investigations by combining it with data held by Member States.

The measure intends to provide the outmost added value from the data already stored at the Europol information system by making Europol a part of the Prüm framework. The data to be checked is limited to third-country sourced data, which Member States may not have at their disposal. Therefore we consider the measure proportionate to its objective of general interest.

ii. Impact on data protection (0)

1. Necessity

In the context of criminal investigations, information on suspects and perpetrators of criminal offences already in Europol's possession is crucial. The policy option is genuinely effective to achieve the specific objective of improving Europol's ability to support Member States in identifying cases and information with relevance for their criminal investigations, and therefore also essential to the fight against serious crime and terrorism as objectives of general interest in EU law. Alternatively, another option would be to create a dedicated database for this purpose, but as Europol already stores the data, we consider the current policy option less intrusive.

We therefore conclude that the measure respects the principle of necessity.

2. Proportionality

Access to Europol information is already legally possible under the Europol Regulation.[55] The policy option would enable making searches to data stored at Europol on the basis of biometric data (DNA, fingerprints and facial images). For instance, in case Member States' criminal investigators have found a latent fingerprint at a crime scene, national authorities would be able to directly search biometric data at Europol with this latent, which is currently not possible.

In reply to the public consultation, one stakeholder expressed concerns on the inclusion of Europol data intro the Prüm exchange mechanism and highlighted that transfers to third countries and international organisations should be subject to adequate safeguards. In this regard, safeguards related to the transfer of data to third countries laid down in the Europol Regulation would be applicable. The general prohibition of onward transfer of data obtained via the Prüm framework with the exception of well-defined specific cases[56] should be applied.

Chapter VI of the Europol Regulation on *General data protection safeguards* provides a comprehensive set of detailed safeguards to guarantee a robust and high level data protection, transparency and liability to the day-to-day operations of the agency. It consists of a series of general and specific data protection principles, measures, obligations, responsibilities, requirements, limitations, data subject rights and external independent supervision.

We therefore conclude that the measure respects the principle of proportionality.

d. Costs

	Member States activities	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	0	2.042
Expected yearly recurring costs (in million EUR)	0	0.480

The cost estimation for EU activities includes the costs for Europol connection to the Prüm network and developing an interface at its side (QUEST Biometrics).

The costs at EU level include:

- Developing and implementing the interface;

[55] Article 20 of 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.
[56] See Chapter V of the LED.

- Operating and maintaining the connection;
- Generic costs linked to project management.

e. Feasibility

Concerning technical feasibility, the policy option varies depending on whether or not a central router is established for the exchange of information in the Prüm framework (policy option 1.1).

If the central router is in place, it would suffice to make a single connection with the Europol Information System, which would have a high technical feasibility and imply low costs. In the absence of the central router, each Member State would need to connect individually in the context of the Prüm framework. The establishment of such connections would have a low technical feasibility and imply high costs.

Concerning political feasibility, Member State support the involvement of Europol in the Prüm framework and consider that, allowing law enforcement authorities to search and compare their biometric data with third country data held at Europol, would contribute to the fight against crime and terrorism. This policy option would bring added value from an operational perspective, as highlighted by Member States in targeted consultations in the form of questionnaires and discussions in the technical workshops organised in the context of the revision of the Prüm Decisions.

We therefore conclude that the measure is feasible in the case of policy option 1.1 being supported and not feasible in the case of policy option 1.1 not being supported.

6.3.2 Policy option 3.2: enabling Europol to check third-country sourced data against the national databases of Member States

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks by ensuring all available data is used in the context of criminal investigations and thus would contribute to enhancing the security and well-being of EU citizens.

b. Impact on national authorities (0)

The policy option is neutral from national authorities' point of view. Indeed, under this option, it would be Europol taking the responsibility of checking whether the data that it has obtained from third countries is present in Member States. Member States' law enforcement authorities would need to contribute only in case there are "hits" with their data.

c. Impact on fundamental rights

i. Objective of general interest (++)

Very positive impact on the security of the European citizens and societies. Data provided by third countries on criminals is even more important in an open society in a globalised world. It would allow for the potential identification of criminals known by countries outside the EU, while 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. With this option, there would be a guarantee that available data is used to its full potential.

This option combined with the previous policy option ensure that no gaps occur in relation with data related to serious crime and terrorism obtained from third countries.

The measure intends to provide the outmost added value from the data already stored at the Europol information system by making Europol a part of the Prüm framework. The data to be used by Europol is limited to third-country sourced data, which Member States may not have at their disposal. Therefore we consider the measure proportionate to its objective of general interest.

ii. Impact on data protection (0)

1. Necessity

In the context of criminal investigations, information on suspects and perpetrators of criminal offences already in Europol's possession is crucial. The policy option is genuinely effective to achieve the specific objective of improving Europol's ability to support Member States in the fight against serious crime and terrorism. Europol, as the EU body in possession of this data, is best placed to undertake this comparison. Alternatively, this responsibility could be transferred to Member States' law enforcement authorities. But finding a procedure for the allocation of responsibility would be cumbersome and would not make the policy option more effective.

We therefore conclude that the measure respects the principle of necessity.

2. Proportionality

The policy option affects data subjects who are convicted criminals and suspects, falling under Europol's mandate, and whose personal data third countries share with Europol.

The policy option does not have a disproportionate and excessive impact on the persons affected by the limitation, in relation to the specific objective of enabling Europol to cooperate effectively with third countries and hence the fight against serious crime and terrorism as objectives of general interest in EU law, as Europol's data protection regime will provide for adequate safeguards.

The policy option constitutes a proportionate response to the need to solve the problem resulting from limits in Europol's ability to effectively support Member States in countering crimes prepared or committed using data coming from third countries.

In reply to the public consultation, one stakeholder expressed concerns on the inclusion of Europol data intro the Prüm exchange mechanism and highlighted that transfers to third countries and international organisations should be subject to adequate safeguards. In this regard, safeguards related to the transfer of data to third countries laid down in the Europol Regulation would be applicable. There should not be any automated exchange of data with third countries. Transmission of information, if any, should require manual intervention, be related to a specific case and require the consent of the Member State whose data would be concerned.

Chapter VI of the Europol Regulation on *General data protection safeguards* provides a comprehensive set of detailed safeguards to guarantee a robust and high-level data protection, transparency and liability to the day-to-day operations of the agency. It consists of a series of general and specific data protection principles, measures, obligations, responsibilities, requirements, limitations, data subject rights and external independent supervision.

We therefore conclude that the measure respects the principle of proportionality.

d. Costs (+/--)

	Member States activities	***EU activities***
Direct costs		
Expected one-off costs (in million EUR)	0	2.042*
Expected yearly recurring costs (in million EUR)	0	1.291

*non-cumulative with the costs of policy option 3.1.

The cost estimation for EU activities includes the costs for Europol connection to the Prüm network and developing an interface at its side (QUEST Biometrics). Therefore, the expected one-off costs are the same as for policy option 3.1. If policy option 3.1 is chosen, the expected one-off costs for this policy option is 0.

If both policy options 3.1 and 3.2 are retained, the yearly costs for Europol for policy option 3.2 are estimated at EUR 1,291,000. This figure mainly covers the costs of the operational staff to conduct searches and verify biometric results (DNA, fingerprints and facial images). The current estimations only take into account the use of third country sourced data. Operational costs may slightly increase over time due to the increase in the volume of data.

e. Feasibility (+/--)

Concerning technical feasibility, the policy option varies depending on whether or not a central router is established for the exchange of information in the Prüm framework (policy option 1.1).

If the central router is in place, it is positive, it would suffice to make a connection with the Europol Information System, which would not imply high costs. In the absence of the central router, the technical feasibility would be very negative, as Europol would need to connect to each Member State individually in the context of the Prüm framework, which would also imply additional costs

Concerning political feasibility, some Member State expressed certain doubts on this policy option in the technical workshops organized in the context of the revision of the Prüm Decisions, mainly on the basis of the principle of sovereignty and the fact that Europol should not be considered as a Member State and be granted he same prerogatives as Member States. However, this policy option would not entail Member States giving up control over their databases as in case of a match, only the Member State whose data was at the origin of the match would be notified. The decision whether or not to follow up on this match would be solely incumbent to the Member State concerned. A larger number of Member States supported the idea of Europol searching their databases using data obtained from third countries, stating in particular that information provided by third countries to Europol should be made actionable and useable under the Prüm framework.

However, contrary to the previous option, this policy option would require enlarging Europol's mandate.

We therefore conclude that the measure is feasible in the case of policy option 1.1 being supported and not feasible in the case of policy option 1.1 not being supported.

6.4 Regulate the hit-follow-up exchange process

6.4.1 Policy option 4.1: regulating the follow-up process at EU level with a semi-automated exchange of core data

a. Impact on citizens (+)

Positive impact on the security of the European citizens and societies. The measure aims to support law enforcement authorities in the exercise of their tasks and thus would contribute to enhancing the security and well-being of EU citizens.

b. Impact on national authorities (++)

Very positive impact for national law enforcement authorities. The measure would result in an accelerated access to the most relevant information for law enforcement authorities, reduced workload with regard to eliminating possible unnecessary requests for additional information and effort from the requested Member State's authorities to gather that data and, consequently, an increase in law enforcement authorities's capacity to carry out other relevant tasks.

c. Impact on fundamental rights

i. Objective of general interest (++)

Very positive impact on the security of the European citizens and societies. The policy option would contribute to the internal security of the European Union by simplifying and streamlining the exchange of law enforcement information. It would give predictability to all users, as they would all know what data they would get in this step, as compared to the current situation where it depends on the Member State concerned.

The measure aims to facilitate and harmonize the exchange of data in the second step of the Prüm process. It would still require a human intervention, which means that Member States would still keep control of their own data. Therefore, we consider the measure proportionate to its objective of general interest.

ii. Impact on data protection (0)

1. Necessity

The policy option would enable exchanging data in a semi-automated, consistent and harmonized manner across Member States. As a result, the policy option would reduce the workload and improve the efficiency of the work of EU law enforcement authorities. This would have a positive impact on the fight against crime and terrorism. As the Prüm framework is decentralised, meaning that no data is kept at central level, this semi-automated exchange of core data held at Member State level is a powerful tool to bring relevant information to the law enforcement authorities.

We therefore conclude that the policy option respects the principle of necessity.

2. Proportionality

The policy option provides for the exchange of core data. This exchange would provide for a limited access to personal data, based on which the investigator could decide if a more targeted request for more information is required. This measure does not provide for new access rights, as the users could already receive these categories of data, but only for a facilitation of this process.

The policy option also presents a range of safeguards. Indeed, there is only a partial automation: human intervention is needed before any follow-up data exchange, including the core data exchange, can be started. Indeed, it only covers the procedure under which this data is exchanged, after manual validation by the Member State in possession of the data. This human intervention can contribute to ensuring that the data is relevant to the case at hand, that there is no abuse of the framework and that any obligation under national law is respected (e.g. need for judicial authorisation).

The harmonisation of the follow-up under Prüm would also constitute a safeguard as far as it would contribute to the consistency and reliability of the procedure across Member States.

We therefore conclude that the policy option respects the principle of proportionality.

d. Costs (++/--)

Each Member State has its own national system in place. As such, the possible need for additional hardware/software will be dependent on each Member State. In this sense, costs may vary greatly and are exponential to the number of Member State connections and categories of data exchanged.

Since the measure would imply changes in national procedures, Member States might propose training programmes and awareness initiatives for end-users.

However, if the central router is created, the costs at both Member State and EU level of setting up this policy option are already provided for under the costs of policy option 1.1.

e. Feasibility (+/--)

Concerning technical feasibility, in the absence of the central router, it would require adaptations to all existing connections between Member States, which could be a burdensome process. However, should the router of policy option 1.1 be created, the technical feasibility could greatly improve. As the change could be performed at central level, Member States would only require to adapt their connection to the router instead of to each other Member State, limiting the interference with national IT infrastructures and building new synergies.

Concerning political feasibility, in reply to the public consultation, most respondents agreed that a limited set of data could be provided in 'fast track'. In the technical workshops organised in the context of the revision of the Prüm Decisions, there seemed to be a common understanding among experts on the necessity to speed up the follow-up exchange of data with the return of a set of core data, provided there is a certain degree of human intervention before this set is sent back.

We therefore conclude that the measure is feasible in the case of policy option 1.1 being supported and not feasible in the case of policy option 1.1 not being supported.

7. HOW DO THE OPTIONS COMPARE?

As none of the options are mutually exclusive, this chapter compares each option against the baseline scenario (i.e. where no action is taken for that policy option).

7.1 Improve the technical architecture

policy option / *assessment criteria*	**Policy option 1.1: hybrid approach with central router without data storage (hit/no-hit only)**
1) Impact on citizens	+

2) Impact on national authorities	++
3) Objective of general interest	+
4) Data protection	0
5) Costs	++
6) Feasibility	+
Preferred policy option	**X**

Policy option 1.1 is the preferred option. The policy option providing for the creation of a central router without data storage is a key option to provide for efficient automated exchange of data between law enforcement authorities. Indeed, the creation of a central router would improve the current architecture of the Prüm framework. This would contribute to ensuring that connections are made between all Member States' databases, as only one connection would be required. This has also a positive impact when changes occur at the level of Member States' databases, as only this connection would need to be changed. Moreover, the router would allow for the collection of statistics, which would contribute to enhancing the performance of the framework as well as to its monitoring and evaluation. From a costs point of view, the router would result in considerable savings for Member States' authorities over time. The option was also considered feasible, both from a technical and political point of view. Moreover, the more policy options described in this impact assessment are considered, the more benefit for the router. Indeed, the creation of new categories of data, the connection of new entities (e.g. a Member State or Union Agency) or the automation of any follow-up are reinforced by the existence of a central router.

The creation of the central router aims to ensure that all Member States are connected and can make use of the possibilities for exchanging data under the Prüm framework. It would significantly reduce the recurrent costs of maintaining all the bilateral connections as well as significantly reduce the costs of setting up connections for exchanging new categories of data (as the proposed facial images and police records).

The router would not store any data, it would not allow for new types of data processes, it would not enlarge access rights and it would not extend data retention periods. To sum up, the router would lead to a more efficient use of the Prüm framework in order to achieve its purposes. A more efficient use of an existing tool does not entail a greater impact on data protection.

The advantages of the router compared to the baseline scenario are the following: a more efficient use of the current framework, therefore contributing to fighting crime and

terrorism, a cheaper solution (in the medium to long term) and advantages in terms of technical feasibility.

7.2 Automated exchange of additional data categories

policy options / *Assessment criteria*	**Policy option 2.1: facial images**	**Policy option 2.2: police records**	**Policy option 2.3: driving licences**
1) Impact on citizens	+	+	+
2) Impact on national authorities	++	++	++
3) Objective of general interest	++	++	-
4) Data protection	-	-	--
5) Costs	+	+	0
6) Feasibility	+	++	0
Preferred policy options	**X**	**X**	

The policy options are stand-alone options in the sense that policy option 2.1 can be chosen as preferred option irrespective of whether options 2.2 or 2.3 are chosen. The same applies for options 2.2 and 2.3.

Policy options 2.1 and 2.2 are the preferred options. These two policy options aim to enlarge the scope of the Prüm framework to other categories of data (i.e. facial images and police records) in Member States' databases that are often relevant in criminal investigations and therefore the subject of cross-border information requests, but that are not covered today by the Prüm Decisions. These data categories can already be subject to exchanges between Member States but there is no efficient way of doing it. Their integration in the Prüm framework is the most efficient way to ensure that there is no information gap. Moreover, both options are feasible both from a technical (this is even more true for police records and the current ADEP/EPRIS pilot) and political point of view and are considered as meeting the principles of necessity and proportionality. Finally, the inclusion of facial images is in line with the developments of the technology. Indeed, new or recently updated central EU information systems use facial images (e.g. the new Entry-Exit System and the updated Visa Information System and Schengen Information System).

The inclusion of these new data categories in the Prüm framework would lead to a higher intensity of data exchanges. This is because, despite the fact that today it is possible to exchange this data, there is no channel to do it in a timely and efficient manner. This leads to errors, information gaps and reluctance to use it by law enforcement authorities. The inclusion of these data categories in the Prüm framework will provide Member States' law enforcement authorities with an incentive to exchange this data, leading to a higher intensity of data exchanges.

The higher intensity of data exchanges is counter-balanced by the benefit brought to the fight against serious crime and terrorism. The more Member States' law enforcement authorities exchange these new data categories, the smaller the gap in fighting serious crime and terrorism in an area without internal borders as Member States could therefore also search other Member States' databases and not only their own.

Policy option 2.3 is discarded. Despite the fact that the exchange of information across Member States concerning driving licences would provide added value for the citizens and national authorities, the proportionality of the measure could not be demonstrated. Other options could provide a similarly effective but less intrusive way of meeting the policy objectives.

7.3 Involve Europol

policy options / *assessment criteria*	**Policy option 3.1: enabling Member States to check automatically third country sourced data at Europol**	**Policy option 3.2: enabling Europol to check third country sourced data against the databases of Member States**
1) Impact on citizens	+	+
2) Impact on national authorities	++	0
3) Objective of general interest	++	++
4) Data protection	0	0
5) Costs	+/--[1]	+/--[2]
6) Feasibility	+/-[3]	+/--[4]
Preferred policy options	**X**	**X**

[1] "+" in the case of policy option 1.1 being supported, "--" in case it is not

[2] " + " in the case of policy option 1.1 being supported, "--" in case it is not

[3] "+" in the case of policy option 1.1 being supported, "-" in case it is not

[4] " + " in the case of policy option 1.1 being supported, "--" in case it is not

Both policy options are stand-alone options in the sense that policy option 3.1 can be chosen as preferred options irrespective of whether option 3.2 is chosen and vice-versa.

Policy options 3.1 and 3.2 are the preferred options. However, in order for policy options 3.1 and 3.2 to be chosen as preferred options compared to the baseline scenario, policy option 1.1 must be considered. Indeed, the creation of a central router is key in the development of these two policy options. The central router has a significant impact in terms of costs and technical feasibility for these policy options.

On top of the advantages for both these options brought by the central router, the policy options have merits of their own.

Policy option 3.1 would ensure that law enforcement authorities have efficient access to all relevant information that they need in the context of their criminal investigations. Indeed, including third country-sourced data stored at Europol in the framework of Prüm addresses an existing information gap. All the safeguards (including data protection safeguards) provided for in the Europol Regulation concerning the data stored at Europol would also be applicable to this policy option.

Policy option 3.2 would ensure that all relevant information in the context of criminal investigations is used in the most efficient manner. Indeed, allowing Europol to use third country-sourced data that is already stored in their information systems to compare it with Member States data would ensure that this data is used to its full extent. Avoiding situations where a terrorist or criminal is not identified or apprehended due to the impossibility to use this data in the Prüm framework. Similarly to policy option 3.1, all safeguards (including data protection safeguards) provided for in the Europol Regulation concerning the data stored at Europol would also be applicable to this policy option.

7.4 Regulate the hit-follow-up exchange process

policy option / *assessment criteria*	**Policy option 4.1: semi-automated exchange of core data**
1) Impact on citizens	+
2) Impact on national authorities	++
3) Objective of general interest	++

4) Data protection	0
5) Costs	++/--[1]
6) Feasibility	+/-- [2]
Preferred policy option	**X**

[1] "++" in the case of policy option 1.1 being supported, "--" in case it is not

[2] "+" in the case of policy option 1.1 being supported, "--" in case it is not

Policy option 4.1 is the preferred option. However, in order for policy option 4.1 to be chosen as preferred option compared to the baseline scenario, policy option 1.1 must be retained. Indeed, the creation of a central router is key in the development of this policy option. The central router has a significant impact in terms of costs and technical feasibility for this policy option.

This policy option would result in increased efficiency in the information exchange between law enforcement authorities. It would also reduce workload with regard to eliminating possible unnecessary requests for additional information and effort from the requested Member State's authorities to gather that data. Moreover, it would provide for the harmonization of the expected replies. Compared to the current situation where there are different replies and procedures, there would be an increased predictability as regards the obtaining of core data.

8. PREFERRED POLICY OPTIONS: STRENGTHENING THE PRÜM FRAMEWORK

Taken together, the preferred policy options identified in section 7 reinforce the current Prüm framework with targeted and strong tools and 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 this section, we will describe the proposed initiative combining all the preferred policy options as well as assessing their aggregated impact.

Regarding data categories, the scope of the Prüm framework would be enlarged to allow for the exchange of facial images and police records.

The preferred policy option also provides for the creation of a central Prüm router. Under this option, the central router would not store any data but provide a hub between the national databases. The current complex architecture of Prüm would evolve:

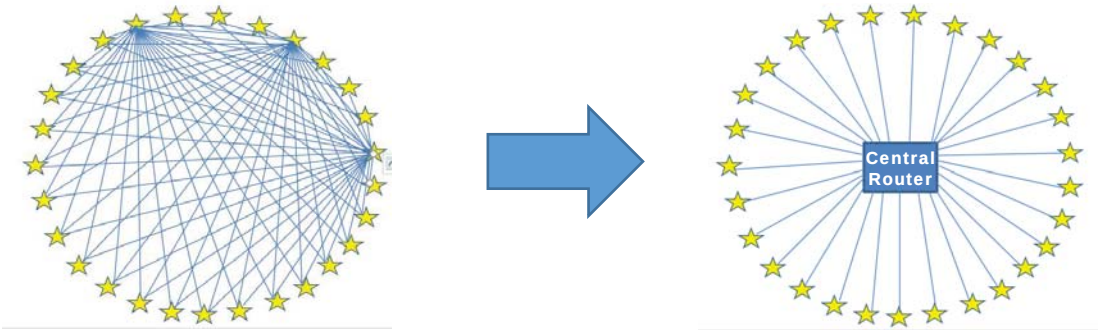


Figure 5: Evolution of the architecture of the Prüm framework

The Prüm router would make it technically possible to incorporate Europol into the Prüm framework. This results in closing one of the existing information gaps: it will allow Member States to query third country-sourced data stored at Europol and therefore allow for its exchange in the context of the Prüm framework. This is also interesting because all the current safeguards that exist regarding Europol data would also apply to its exchange in the context of the Prüm framework.

Similarly, Europol would also be able to use third country-sourced data stored in its information system to query Member States data in the context of the Prüm framework, with a view to supporting Member States law enforcement authorities in their fight against crime and terrorism.

Finally, the Prüm router would also allow to introduce a certain degree of automation in the exchange of data following a potential match. Indeed, a limited set of data could be exchanged in an automated manner following the verification of the authorities against which a match was obtained.

To conclude, the preferred policy option package includes several measures, each aiming to strengthen a particular aspect of the Prüm framework. Indeed, they are the result of years of reflections and work, which led to targeted and proportionated measures that deal with the existing information gaps and inefficiencies in the exchange of data and bring the framework up to date with new technologies. These policy options also aim to align the Prüm framework with both the EU data protection and interoperability frameworks.

8.1 Impact on citizens (++)

Very positive impact on the security of the European citizens and societies. Each of the preferred options has a positive impact on the security of citizens, therefore the combination of all of them provides an even greater positive impact. Indeed, the whole initiative aims to support law enforcement authorities in the exercise of their tasks and thus would contribute to enhancing the security and well-being of EU citizens.

Only data related to suspects and convicted criminals and terrorists would be exchanged within the scope of the preferred policy option package.

8.2 Impact on national authorities (++)

Very positive impact for national law enforcement authorities. The exchange of facial images between Member States to fight crime and terrorism is already a reality. However, there is no efficient procedure for it and it is therefore only used in ad-hoc situations and always in a bilateral way. The preferred policy option would provide a tool to ensure that Member States exchange facial images on suspects or convicted criminals and terrorists and that the data can be compared with the existing data of all Member States. Concerning the exchange of police records, this is a process that has been ongoing in the context of the ADEP/EPRIS project by some Member States. The preferred policy option extends this possibility to all Member States.

The creation of the Prüm router would result in the improvement of the architecture of the Prüm framework, regarding both its current needs as well as the needs included in the preferred policy options.

Finnaly, the proposed semi-automated exchange of data following a hit would result in an accelerated access to the most relevant information for law enforcement authorities. Its benefits include reducing both the workload with regard to eliminating possible unnecessary requests for additional information and the effort from the requested Member State's authorities to gather that data. It also brings a certain degree of harmonisation to this first step of data exchange at EU level.

8.3 Impact on fundamental rights

a. Objective of general interest (++)

Very positive impact on the security of the European citizens and societies. Each of the individual policy options aims to improve the security of the European Union in its own targeted way. As explained in section 6, each policy is narrow in its scope and provides only for what is necessary to achieve its purpose. As depicted in this impact assessment, each of the policy options aims to provide a solution to the different problems and limitations of the current Prüm framework with the final objective of strengthening the security of the European Union.

The benefit of the policy options is cumulative. Moreover, the Prüm router would contribute to render each of the other policy options more efficient, therefore further contributing to achieving their purposes.

In addition, the fact that facial images are added as a new data category in the Prüm framework would also allow for using third country-provided facial images stored in the Europol information system in this context.

The resulting policy option implies only exchanges of data linked to criminal or terrorist investigations. None of the measures provides for new access rights, and just seeks to enhance cooperation between Member States based on the principle of availability. This is all the more relevant in an area without internal borders such as the Schengen area. Therefore, we consider the policy option proportionate with its objective of general interest.

b. Impact on data protection (-)

i. Necessity

As mentioned above, each of the individual policy options aims to improve the security of the European Union in its own targeted way. This means that each new processing of data or each new improvement to existing processes is done for their own purposes as described in section 6. Therefore, the sum of the preferred policy options does not change the necessity assessment (i.e. all policy options are deemed necessary).

ii. Proportionality

While the sum of the preferred policy options does not have an impact on their necessity, it does impact their proportionality. Indeed, the creation of the router brings more added value as new data categories are added to the Prüm framework. Similarly, the need to connect Europol to the framework also reinforces the need for the creation of a central router.

On the other hand, the creation of the router contributes to the safeguards laid down for each of the other policy options. Indeed, the use of statistics and the logs kept at central level will contribute to the monitoring and improvement of the performance of each new processing of data or of each new improvement to existing processes.

Finally, except for the abovementioned contribution of the router to the other policy options, none of the other options contributes to the specific objectives of the others. Which means that there is no collusion between the policy options.

Therefore, the initiative regrouping all policy options is considered to be proportional.

8.4 Costs (++)

The following table summarizes the combined one-off and recurrent costs both at Member State level and at EU central level.

In million EUR	***Member State Administrations***		***EU central level***	
	One-off	*Recurrent*	*One-off*	*Recurrent*
Facial images	2.27	0.45	0	0
Police records	1.52	0.3 p.a.	1.66	0.33 p.a
Prüm router	0.61	0.12 p.a.	9	1.1 p.a.
Europol (including both policy options 3.1 and 3.2)	0	0	2.04	1.77 p.a.
Semi-automated exchange of additional actual data	0	0	0	0
Total		***0.87 p.a.***	***12.7***	***3.2 p.a.***

Despite the initial investments, the Prüm router would also reduce the burden of the Prüm framework from a financial perspective by reducing the costs for Member States, as they no longer would need to establish and maintain bilateral connections with all other Member States for each category of data. Indeed, the estimations indicate that the one-off costs of the preferred policy options would be compensated by the reduction in costs for Member States in two years. Moreover, setting up the exchanges of facial images and police records in the absence of a central component would cost around ten times more to the Member States.[57] All in all, the initiative has a very positive impact on costs. Despite the initial investment, the savings in costs for the Member State will bring savings in the medium and long term.

8.5 Feasibility (++)

Very positive impact on feasibility.

Regarding the technical feasibility of the preferred options, it is worth recalling the role of the Prüm router. Indeed, the described central router does not only provide for efficient automated exchange of data between Member States' law enforcement authorities. It will also allow Europol to participate in the framework. This way, both national law enforcement authorities and Europol would be made aware of relevant data available in the national database of another Member State or at Europol. The router also contributes to all the other objectives, acting as a facilitator. Once the central router is created, Member States would only require one connection to be part of the Prüm framework. This also includes the new data categories or the involvement of Europol.

[57] See Annex 3.

Concerning the **technical feasibility of the router**, as mentioned in Section 6.1, there is a common understanding among experts of the Member State and Union Agencies on the general technical feasibility of the introduction of a central router in the Prüm framework. Moreover, technical components offering similar (if not even greater) services are being implemented (e.g. the European Search Portal introduced via the interoperability Regulations). This also probes the feasibility of the Prüm router.

Regarding the political feasibility of the preferred options, we note Member States' support to dealing with the identified problems. As the measures offer solutions to these problems, we expect broad support subject to discussions. Moreover, the fact that the router would reduce Member States' costs in the medium to long term would also ensure political support.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

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. Four years after the new functionalities are put in place and operating, and every four years thereafter, Member States and 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, one year after the submission of these reports by Member States and Union Agencies, 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.

The monitoring and evaluation of the measures proposed will be notably based on the statistics which will be collected at central level thanks to the introduction of the central router, without having to ask Member States. These statistics would include for instance the number of requests per data category and responses received, including how many hits against how many Member States' databases. These statistics would allow to have a clear view of the use of the Prüm framework, per data category and per Member State. A significant use of the framework as well as the detection of matches and hits in other databases would be a strong indication of the success of the measure, as it would mean that the relevant information is at the disposal of our law enforcement authorities. Indeed, a hit indicates that information on the person for which a Member State was launching a query is found in another Member State's database. Hits may lead to solving a crime and protecting a citizen. However, the use of the hit would fall outside of the scope of the statistics that would be collected via the central router. Indeed, the use of the information would vary according to each individual case and depending on the outcome of the investigation. These statistics could be required from the Member States in a periodical exercise.

Annex 1: Procedural information

1. LEAD DG, D*e*CIDE PLANNING/CWP REFERENCES

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME) for the preparation of the initiative and the work on the evaluation and impact assessment. The agenda planning reference is PLAN/2020/6629.

2. ORGANISATION AND TIMING

The inception impact assessment was published on 11 August 2020. Within this framework, the impact assessment and the evaluation were subsequently prepared.

An Inter-Service Group was set up in August 2020 with the participation of the following Commission Directorates-General: Secretariat-General (SG); Legal Service (LS); Informatics (DIGIT); Justice and Consumers (JUST); Mobility and Transport (MOVE). The Inter-Service Group met three times, discussing (1) the stakeholder consultation and the questionnaire for the public consultation, (2) the outline for the impact assessment, the first part of the draft evaluation and the planning, and (3) the draft impact assessment and evaluation.

3. CONSULTATION OF THE RSB

On 21 June 2021, the Directorate-General for Migration and Home Affairs submitted the present impact assessment report to the Regulatory Scrutiny Board (RSB). The RSB issued an impact assessment quality checklist on 9 July 2021 with some discussion points and a number of comments. A written response to the main discussion points in this quality checklist was sent in advance to the RSB meeting on 13 July 2017. Following the meeting on 14 July 2021, the RSB issued a positive opinion without reservations on 16 July 2021, with a number of recommendations and comments that completed the previously issued quality checklist. These comments were incorporated into the final version of this document.

RSB recommendations for IA	Modification of the IA report
(1) The report should clarify how the introduction of a central router and the extension to new data categories will lead to a higher intensity of data exchanges. It should explain why the centralised model would be more successful in integrating Member States that did not make any bilateral connections in the current system. It should then explain how data protection standards will limit the impact on data	Wording has been added in Sections 7.1 and 7.2 on the introduction of the central router and the new data categories, and on the higher intensity of data exchanges and how this higher intensity is counter-balanced by the benefit brought to the fight against serious crime and terrorism.

protection and how the more intense data exchanges will be counterbalanced by the benefits for fighting crime.	
(2) The report should define the operational (and time bound) objectives that allow measuring the success or failure of the initiative. It should not only plan the monitoring and evaluation of the results of the initiative, but also indicate how to remedy the lack of data at EU and Member State level. This should include data collected at the level of the new central router, and any other new (survey) data collection needed to evaluate the effectiveness and usefulness of the framework for the fight against crime in the future.	Wording has been added in Section 5.2.1 and in Section 9 on the monitoring and evaluation, based on statistics, which would allow to measure the use of the Prüm framework and its success.
(3) The report could better demonstrate the need for rapid data exchanges, of both the current and the new data categories, between police services to fight crime. It should present the (systematic or anecdotal) evidence that shows that the automated exchange of data via Prum provides police forces with means that are more effective and efficient than other ways of acquiring and exchanging information.	Wording has been added in Section 5.2.2 under policy options 2.1 and 2.2.
(4) The report should clarify the content of some policy options. It should explain where the central router will be situated and managed and what national law will govern the router and the data requests following a 'hit'. It should also point out practical issues, such as how the exchange of facial images will take place. It should explain why the options foresee that police records would be exchanged solely on a voluntary basis and why for driving licences there is only a 'hit/no-hit' option.	Wording has been added in Section 5.2.1 on where the router would be hosted and in Sections 6.1.1, 6.2.1 and 6.2.2 on the applicable legislation for data protection. Wording has been added in Section 5.2.2 under policy option 2.1 on the exchange of facial images. Wording has been added in Section 5.2.2 under policy option 2.2 on why police records would be exchanged on a voluntary basis.
(5) A dedicated section should present the discarded policy options and the annexes	The description of the discarded options was moved to Section 5.3 Options

could further explain them in detail. The impact analysis should focus on the retained policy options.	discarded at an early stage.
(6) The views of the various stakeholder groups should be reflected throughout the report.	The views of the various stakeholder groups have been described in more detail in Annex 2 and references have been added throughout the report (Sections 5.2.2, 5.2.4, 6.1.1, 6.3.1, 6.3.2).

4. EVIDENCE, SOURCES AND QUALITY

The impact assessment is notably based on the stakeholder consultation (see Annex 2). The Commission applied a variety of methods and forms of consultation, ranging from consultation on the Inception Impact Assessment, which sought views from all interested parties, to targeted stakeholders' consultation by way of questionnaires, experts' interviews and targeted thematic technical workshops, which focused on subject matter experts, including practitioners at national level.

In this context, the Commission also took into account the findings of the 'Study on the Feasibility of Improving Information Exchange under the Prüm Decisions',[58] which was commissioned by DG HOME and developed by the contractor based on desk research and the following stakeholder consultation methods: surveys, interviews with subject matter experts, questionnaires, and three expert workshops.

[58] See the Final Report (https://op.europa.eu/en/publication-detail/-/publication/6c877a2a-9ef7-11ea-9d2d-01aa75ed71a1/language-en/format-PDF/source-search), the Advanced Technical Report (https://eur-lex.europa.eu/eli/reg/2016/679/oj), and the Cost-Benefits Analysis (https://op.europa.eu/en/publication-detail/-/publication/503f1551-9efc-11ea-9d2d-01aa75ed71a1/language-en).

Annex 2: Stakeholder consultation

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

1. CONSULTATION STRATEGY

The objective of the consultation activities was to gather data and stakeholders' views in the context of preparations for the revision of the Prüm Decisions, back-to-back with the evaluation of the Prüm Decisions, for the review of automated exchange of data under the Prüm Decisions. More specifically, the consultations sought to:

- Gather data for assessing the effectiveness, efficiency, relevance, coherence, and EU-added value of the Prüm Decisions;
- Update the information and gather data on challenges and shortcomings, but also best practices of the existing Prüm framework;
- Identify any new and update existing information about the needs of stakeholders;
- Gather stakeholders' views on the different policy options and their respective impacts;
- Fill any data gaps in the evidence base.

In the past years, several processes have contributed to establishing a sound knowledge about the benefits and shortcomings of the existing Prüm framework.

1) Implementation Report of the Prüm Decisions, European Commission (2012);[59]
2) Several projects aiming to improve the implementations of the Prüm Decisions;
3) Regular discussions on law enforcement information exchange and specifically on the Prüm Decisions, in the Council Working Party DAPIX/IXIM;[60]
4) High Level Expert Group on Information Systems and Interoperability;[61]
5) Expert discussions in the context of four focus groups addressing topical improvement opportunities of the Prüm Decisions;[62]

[59] See the report here.
[60] 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).
[61] See the final report here.
[62] Council documents 11264/19, 13356/19, 13511/19 and 13556/19 (not publicly available).

6) Study on the feasibility of improving the exchange of information under the Prüm Decisions, including 3 workshops with the end-users from Member States and other stakeholders;[63]

7) Various studies, e.g. Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision.[64]

The consultation activities carried out built on the data collected and the work already done, in order to minimise the administrative burden of already-consulted stakeholders. At the same time, the intention was to extend the consultation activities to a wider group of stakeholders, in order to achieve a more balanced and comprehensive assessment of the policy options and their impacts. A re-consultation with some stakeholders, especially the end-users of the system who have shared their views already in the context of the activities listed above, was still needed and was therefore carried out.

1.1 Mapping of stakeholders

In preparing the initiative, Commission services carried out an initial **mapping of stakeholders**. Two main categories of stakeholders that may have an interest in the strengthening of the automated exchange of data under the Prüm framework were identified.

1.1.1 Current and potential new end-users or other directly related stakeholders of the Prüm framework

The main stakeholders in this group are Member States' authorities using the Prüm automated data exchange and database custodians. Depending on the national legal and administrative system, one or more of the roles listed below could belong to the same authority:

- Law enforcement and judicial authorities responsible for the prevention and investigation of criminal offences;
- National vehicle registration authorities;
- National authorities responsible for issuing driving licences;
- National databases' custodians responsible for the national databases interconnected by the Prüm framework;
- Forensic laboratories/institutes responsible for the forensic assessment of the results of automated matching of biometric data;

As potential new end-users, two EU agencies can be listed:

[63] See the final report here.
[64] See the study here.

- The European Union Agency for Law Enforcement Cooperation (Europol), as a potential new participant in the Prüm framework;
- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), as a potential host of the possible new architectural options for the Prüm framework.

1.1.2 Other important stakeholders

The second group of stakeholders includes various EU bodies, organisations and networks, who have relevant expertise and interests related to the initiative:

- National data protection authorities (via European Data Protection Board).
- EU bodies and institutions
  - European Data Protection Supervisor (EDPS);
  - European Union Agency for Fundamental Rights (FRA);
  - European Parliament, notably the Committee of Civil Liberties, Justice and Home Affairs (LIBE Committee);
  - General Secretariat of the Council;
  - European Commission internal stakeholders from different Directorates-General (especially DG Justice and Consumers and DG Informatics) and services.
- Non-governmental organisations
  - European Digital Rights (EDRi)
- Intergovernmental organisations
  - European car and driving licence Information System (EUCARIS)
- Persons (wider public) with interest in the initiative.

1.2 Methods and forms of consultation

In view of the crisis due to the coronavirus, it was difficult to interact with stakeholders in physical meetings. Therefore, the consultation activities focused on alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

The consultation activities were launched with the publication of the **Inception Impact Assessment**.[65] Due to the COVID-19 pandemic, the consultation period was extended from four to eight weeks, from 11 August until 6 October 2020.

A public consultation was launched for 14 weeks,[66] in order to give the possibility to the wider public to share their views on the functioning of the existing automated exchange of data under the Prüm framework and on the planned initiative. The questionnaire for public consultation was available in English, French and German. However, respondents could reply in any of the official EU languages.[67]

Targeted consultation activities were aimed to build on the consultation activities that took place in the course of a feasibility study undertaken in 2018-2020,[68] especially concerning the Member States' authorities, relevant EU agencies and EUCARIS. **Four technical workshops** were organised with Member States' authorities and EU agencies to discuss the options, which were being envisaged as part of the revision from a technical perspective.

Meetings were carried out with some Member States, with EU agencies and other stakeholders.

With the exception of the public consultation, the consultation activities were conducted in English and French.

2. CONSULTATION ACTIVITIES

2.1. The Inception Impact Assessment

The Inception Impact Assessment[69] was published for feedback by all interested parties on the Commission's 'Have your say' portal. Respondents were invited to provide online comments and, where appropriate, submit short position papers to provide more background to their views. Due to the COVID-19 pandemic, the consultation period was extended from four to eight weeks, from 11 August until 6 October 2020.

A total of six contributions were submitted over the 8-week feedback period. Of these, two were provided by a public authority,[70] one by a non-governmental organization (NGO),[71] one from a company/business organization,[72] one from a trade union[73] and one

[65] The Inception Impact Assessment consultation is available here.
[66] 12 weeks extended by 2 weeks due to the Christmas break.
[67] https://europa.eu/european-union/about-eu/eu-languages_en
[68] See the final report here, the advanced technical report here and the cost benefits analysis here.
[69] The Inception Impact Assessment consultation is available here. All contributions received are publically available.
[70] EE, FR.
[71] BE.
[72] FR.
[73] LU.

from an EU citizen.[74] The limited number of contributions received is most likely due to the technical nature of the instrument. In general, respondents supported the Commission's initiative to strengthen the automated exchange of data under the Prüm framework with the identified objectives and expressed their preference for certain policy options.

The majority of respondents recognized the need to speed up and streamline the hit-follow-up exchange process and supported the inclusion of one or several additional categories of data. Concerns were raised on the importance of a mandatory manual review by the requested Member State before any data is sent to the requesting Member State. The contributions from public authorities and one EU citizen highlighted the benefits of the introduction of a central router to facilitate the implementation, use and maintenance of the information system. Support was expressed by two public authorities and one company/business organization for the participation of Europol in the Prüm data exchange mechanism for the purpose of crosschecking data received from third countries. One NGO opposed the inclusion of Europol data into the Prüm exchange system. Concerns were raised on the need to take data protection safeguards into account.

2.2. The Public Consultation

The European Commission launched a public consultation on 16 December 2020, which aimed to gather feedback and collect opinions on the effectiveness of the current legislative and policy framework and on existing problems and possible options for future initiatives. The consultation closed after 14 weeks[75] on 24 March 2021.

The public consultation was conducted through an online questionnaire published on the internet in all EU official languages. It was advertised on the European Commission's website,[76] through the Council Working Party IXIM, and at all relevant meetings (as listed below). The questionnaire consisted of a series of 34 mainly closed questions, along with a limited number of open questions to allow for clarifying remarks and/or remarks of a more general nature.[77] While the questionnaire itself was only available in English, French and German, respondents were free to complete the 'open' elements of the questionnaire using any recognised EU language.

Thirteen practitioners and two members of the general public replied to the questionnaire of the public consultation. One practitioner provided additional input through a written contribution. The limited number of contributions received is most likely due to the technical nature of the instrument. Practitioners included:

- national public authorities (e.g. law enforcement authorities) (9);
- companies/business organisations (1);

[74] ES.
[75] 12 weeks extended by two weeks due to the Christmas break.
[76] See DG HOME website.
[77] See Annex 6 for the public consultation questionnaire.

- non-governmental organisations or networks (1).

The members of the general public contributed from IT and EL. Based on the country which they specified, practitioners from 12 Member States/Schengen associated countries contributed.[78]

Results

Questions relating to the existing Prüm framework for the automated exchange of DNA, dactyloscopic and vehicle registration data

In reply the public consultation, almost all stakeholders indicated that cooperation and the exchange of information between Member States' law enforcement authorities for the prevention and investigation of criminal offences is **very relevant**. One stakeholder stressed the lack of publicly available and accurate data about the impact of the Prüm framework. Being able to search and compare DNA, fingerprint and vehicle registration data in other Member States' databases for the prevention and investigation of criminal offences was highlighted by most stakeholders as **very relevant**.

It was also found by most stakeholders that the Prüm framework is **effective**. Almost all respondents clearly stated that the Prüm framework has improved the exchange of data between Member States, specifying that increased and faster access to the data has facilitated law enforcement authorities' work. One stakeholder added however that the integration of the technical requirements into Decision 2008/616 has been an impediment to making the necessary amendments and updates to the Prüm system. One stakeholder disagreed and specified that from the perspective of fundamental rights protection, the Prüm framework has not improved the exchange of data between Member States' authorities responsible for the prevention and investigation of criminal offences.

The replies to the public consultation further indicated that 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. Some stakeholders specified that the efficiency gains regarding the costs and the staff are smaller or difficult to ascertain. However, most replies indicated that the costs (administrative, budgetary, in terms of personnel, etc.) related to the implementation of the Prüm framework have been proportionate to its contribution in terms of the improvements in law enforcement information exchange.

The Prüm framework was also found to be **coherent**. Indeed, stakeholders agreed that it complements other EU and international action in the area of law enforcement information exchange.

[78] Based on the country specified, replies for all respondents were received from FR (3), CH (1), Spain (1), SK (1), NL (1), LV (1), IT (1), EL (1), DE (1), FI (1), EE (1), BE (1) and AT (1).

When asked to what extent has the Prüm framework provided **added value** compared to what Member States could achieve in the field of law enforcement information exchange in the absence of the Prüm framework, stakeholders agreed, with several highlighting that law enforcement information exchange has been facilitated and has become faster.

Questions relating to the strengthening of the automated data exchange under the Prüm framework

Most respondents agreed that the fact that **additional data categories**, which are not covered by the current Prüm framework, are exchanged by sending manual queries, often time-consuming, to other law enforcement authorities, is a shortcoming in the law enforcement information exchange and that EU legislation should be established to standardise and automate the exchange of additional data categories. The majority of contributions to the public consultation expressed support for the inclusion of new data categories such as facial images, police records and driving licences in the Prüm framework. One respondent opposed the extension of the Prüm framework to include facial images and expressed concerns in terms of the use of facial recognition technology. Five respondents expressed doubts or reservations on the inclusion of police records, one stating that they are still studying the possible added value of adding these data categories instead of making better use of the current possibilities. Concerning the possible inclusion of ballistic data, replies were more mixed.

In reply to the public consultation, most respondents agreed that the fact that the exchange of further personal data after a hit has been confirmed is not governed by the Prüm Decisions is a shortcoming of the existing Prüm framework and almost all agreed that EU legislation should be established to streamline the **hit follow-up exchange of further personal and case-related data**. One respondent highlighted that any information exchange in addition to the automated hit/no-hit response ("supply of further personal data") must take place in accordance with the national law of the requested Member State.

Most respondents agreed that the fact that the existing Prüm framework is a decentralised network of bilateral connections between Member States' national databases is a shortcoming of the existing Prüm framework. When asked what they consider to be the most appropriate means to address this shortcoming, most replied establishing an **EU central router** for transferring messages between Member States with limited functions at a central level such as technical/operational system monitoring and collection of statistics. Some others replied establishing an EU automated biometric identification system (ABIS) that would allow matching biometric templates by a centrally managed technical solution. One respondent highlighted in particular that if a "central router" were to be put in place it should only serve as a pass-through server to transmit messages between Member States, and the collection of statistical data.

2.3. Stakeholder events

In the course of the consultation and in the context of the preparation of the initiative and the impact assessment, the Commission organised four technical workshops which were held on 17 March, 26 March, 20 April and 4 May 2021, respectively, to which representatives of the Member States, of the Schengen associated countries as well as EU agencies and the General Secretariat of the Council were invited. 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.

2.3.1 Technical workshop 1 – The IT architecture of Prüm and the follow-up process (17 March 2021)

This first workshop focused on (1) the IT architecture of the Prüm framework with the possible introduction of a central router and on (2) options to regulate the follow-up process (the so-called 'second step', i.e. the exchange of case-related personal data after a hit). 26 Member States, 2 Schengen associated countries, EU agencies (Europol,[79] eu-LISA,[80] FRA)[81] the General Secretariat of the Council and Commission Directorates-Generals (DG HOME and DG JUST) participated.

In the discussion on the possible introduction of a central router, it seemed like there was a rather broad consensus among experts on the feasibility of the introduction of a central router in the Prüm framework. From the discussion on the options to regulate the second step exchange of data, a rather broad consensus on the necessity to speed up the exchange of data following a hit appeared. Several experts underlined the importance of a human intervention before sending back data to the requesting Member State.

In the context of this first technical workshop, a targeted questionnaire was circulated to Member States and Schengen associated countries in order to support and/or further develop the discussions which took place in the workshop. 19 Member States and one Schengen associated country replied.

2.3.2 Technical workshop 2 – Links between Prüm and interoperability and the participation of Europol in the Prüm framework (26 March 2021)

This second workshop focused on (1) Possibilities of linking Prüm to the interoperability framework with the querying of the Common Identity Repository via the Prüm router and European Search Portal, and on (2) The participation of Europol in the Prüm framework. 27 Member States, 2 Schengen associated countries, EU agencies (Europol, eu-LISA, FRA) the General Secretariat of the Council and Commission Directorates-Generals (DG HOME and DG JUST) participated.

[79] European Union's law enforcement agency.
[80] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
[81] Fundamental Rights Agency.

In both discussions, support was expressed for the linking of the Prüm framework to the interoperability framework and for the participation of Europol in the Prüm framework. Several experts stressed the great benefit of Europol's involvement and expressed their support therefore. However, it appeared clearly that there are different options possible for this involvement, which would need to be considered.

2.3.3 Technical workshop 3 – The introduction of new data categories in the Prüm framework (20 April 2021)

This third workshop focused on the introduction of new data categories in the Prüm framework with the possible inclusion of the exchange of (1) facial images, (2) (pseudonymised) biographical data [police records], (3) driving licences, and (4) data on unidentified human remains and missing persons. 27 Member States, 3 Schengen associated countries, EU agencies (Europol, eu-LISA, FRA, EBCGA),[82] the General Secretariat of the Council and Commission Directorates-Generals (DG HOME and DG JUST) participated.

Both on the topics of facial images and of biographical data, there seemed to be a common understanding among experts that it would make a lot of sense to include these data categories into the new Prüm framework. On the possible inclusion of driving licence data, the necessity to automate these exchanges and include them in the Prüm framework did not appear so clearly. Finally, on the possibility to search for missing persons and unidentified human remains under Prüm, support was expressed to harmonise the legal scope and allow these searches under Prüm.

In the context of this third technical workshop, a targeted questionnaire was circulated to Member States and Schengen associated countries in order to support and/or further develop the discussions which took place in the workshop. 18 Member States and two Schengen associated countries replied.

2.3.4 Technical workshop 4 – Options to step up the information exchange on firearms and ballistics (4 May 2021)

This fourth workshop focused on (1) Including the exchange of firearms-related data in the Prüm framework, and on (2) Including the exchange of ballistics-related data in the Prüm framework. 23 Member States, 2 Schengen associated countries, EU agencies (Europol, eu-LISA), the General Secretariat of the Council and Commission Directorates-Generals (DG HOME and DG JUST) participated.

From the discussions, there seemed to be a shared agreement on the need to streamline and improve law enforcement cooperation and the exchange of firearm-related data between Member States but whether or not this exchange should be automated (i.e. included in the Prüm framework) was not clear and the necessity of the automation of these exchanges still remained to be demonstrated. From the discussion on the exchange

[82] European Border and Coast Guard Agency ('Frontex').

of ballistic data, it appeared that it is too early and premature at this stage to capture these exchanges under the automated framework of Prüm.

In the context of this fourth technical workshop, a targeted questionnaire was circulated to Member States and Schengen associated countries in order to support and/or further develop the discussions which took place in the workshop. 17 Member States and two Schengen associated countries replied.

Annex 3: Who is affected and how?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

The practical implications are given by stakeholder group.

1.1 EU citizens

All the policy options aim to support law enforcement officers in the exercise of their tasks by ensuring all available data is used and that it is used in the most efficient manner possible in the context of criminal investigations. Therefore, the initiative would contribute to enhancing the security and well-being of EU citizens.

1.2 National authorities

a. Law enforcement officers

The initiative aims to provide law enforcement officers with more tools to help them in the context of criminal investigations. These tools include:

- querying and accessing, via the Prüm framework, facial images and police records;
- allowing Europol to further support their tasks;
- creating a central router acting as a single-search interface to query and access Prüm data; and
- providing for the semi-automated exchange of additional actual data following hits against Member States' databases.

b. IT organization in Member States

An initial investment would be needed to implement the Prüm router. However, this would save costs for Member States, as only one connection would be required rather than one connection per pair of Member States and per data category. Once done, further changes to any national system would require less changes to all other national systems, as the connection would be done centrally via the Prüm router and it would absorb most necessary changes.

2. SUMMARY OF COSTS AND BENEFITS

The overview of costs of the preferred policy options is indicated below.

I. Overview of costs – Preferred option						
	Citizens/Consumers		Member State Administrations		Union Agencies	
	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Direct costs						
Facial images	0	0	€2.27m	€0.45m	0	0
Police records	0	0	€1.52m	€0.3m p.a.	€1.66m	€0.33m p.a
Prüm router	0	0	€0.61m	€0.12m p.a.	€9m	€1.1m p.a.
Europol (including both policy options 3.1 and 3.2)	0	0	0	0	€2.04m	€1.77m p.a.
Semi-automated exchange of additional actual data	0	0	0	0	0	0
Total	***0***	***0***	***€4.4m***	***€0.87m p.a.***	***€12.7m***	***€3.2m p.a.***
Indirect costs						
None						

All one-off and recurrent costs are implementation costs. No regulatory charges, hassle costs, administrative costs, or indirect costs were identified and therefore are not quantified. These are all provisional estimates that would need to be confirmed, including how the costs are split between the relevant Union Agencies. As a result the confidence margin of cost estimates cannot be better than 20-25% at this early stage in a project. What is stable is how the costs of the various measures compare with each other.

As can be concluded from the above table, the one-off total costs amount to €17.1 million and recurrent costs to €4.07 million *per annum*.

II. Overview of Benefits– Preferred Option

Description	*Amount*	*Comments*
Direct benefits		
Reduced costs of connecting each Member State's national database with each other due to the router[83] One-off costs	€32.9m as one-off	Member States' IT departments and law enforcement authorities
Reduced costs of connecting each Member State national database with each other due to the router[84] Recurrent costs	€12.96m recurrent	Member States' IT departments and law enforcement authorities
Indirect benefits		
None identified		

All benefits are reduced implementation costs and are based on very cautious estimates, which for instance do not consider economies of scale in the context of the bilateral connections. The benefits include reduced costs due to the central router for the Member States. These reduced costs include a reduction of the costs for maintaining the existing bilateral connections (fingerprints and DNA). Indeed, these include a reduction of the costs due to changes to national applications when any other national database or connection is modified. Moreover, there are also reduced costs for the Member States of setting up and maintaining bilateral connections for the new categories of data: facial images and police records. The one-off benefits could be larger as some bilateral connections for fingerprints and DNA do not exist today. But as these should exist we did not take them into account. We did however consider the benefits on the maintenance costs of existing connections.

The rationale for the calculation of the reduced one-off costs was to use the one-off cost of connecting to the central router and multiplying it by the number of Member States (27)[85] times the number of new data categories (2).[86]

[83] Only considering new connections. There would be additional added value for current connections which were not made at the time of the start of operations of the Prüm router.
[84] Considering both the new connections (facial images and police records) and the existing bilateral connections (fingerprints and DNA).
[85] 27 Member States minus the one establishing the connection plus the UK.
[86] Facial images and police records.

The rationale for the calculation of the reduced recurrent costs was to use the one-off cost of connecting to the central router and multiplying it by the number of Member States (27) times the number of data categories (4).[87]

As can be concluded from the above table, the one-off total benefits amount to €32.9 million (exceeding the accumulated costs of the preferred option which are 17.1 million) and recurrent benefits €12.96 million per *annum* (exceeding the accumulated costs of the preferred option which are €4.07 million *per annum*).

Taking the above into consideration, just with the savings for Member States in recurrent costs (12.96 – 4.07 = €8.89 million), the costs of setting up the preferred policy option would be compensated in two years.

- Savings for Member States in operating costs in two year time = 8.89 x 2 = **€17.78 million**
- Total one-off costs of the preferred policy option = **€17.1 million**

However, the most important benefit — the contribution to fighting crime and terrorism — is not monetized in the above calculation.

[87] Fingerprints, DNA, facial images and police records.

Annex 4: Evaluation of the existing policy and legislative framework

1. INTRODUCTION

Purpose and scope of the evaluation

The main objective of this evaluation is to provide an understanding of whether Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,[88] and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA[89] (hereinafter referred to as the 'Prüm Decisions' or the 'Decisions' or the 'Prüm framework') are still "fit-for-purpose" 13 years after their adoption in 2008. In line with the "evaluate first" principle, this evaluation supports the preparation of a new initiative to strengthen the automated exchange of data by law enforcement authorities for preventing and investigating criminal offences.[90]

The Prüm Decisions aim to support and step up cross-border cooperation in matters covered by Title VI of the Treaty (now Part III, Title V, Chapters 1, 4 and 5 of the Treaty on the Functioning of the EU), namely in police and judicial cooperation in criminal matters, particularly the **exchange of information between authorities responsible for the prevention and investigation of criminal offences**. To this end, the Prüm legal framework contains rules in the following areas:

(a) provisions on the conditions and procedures for mutual on-line access to national databases for automated search and supply of DNA profiles, dactyloscopic data and certain national vehicle registration data. Thanks to the Prüm Decisions, law enforcement authorities in one Member State are able to search and compare DNA, fingerprints and vehicle registration data in other Member States, which helps them in their investigations.

The Prüm Decisions also cover provisions on operational police cooperation, which are not covered by this evaluation and are instead addressed in the study supporting the preparation of the forthcoming Police Cooperation Code (PCC) initiative:[91]

(b) provisions on the conditions for the supply of non-personal and personal data in connection with major events with a cross-border dimension. Those provisions help Member States to exchange data

[88] Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210 of 6.8.2008, p. 1.
[89] Council Decision 2008/616/JHA 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 of 6.8.2008, p. 12.
[90] See the inception impact assessment: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12563-Strengthening-the-automated-data-exchange-under-the-Pr-m-framework.
[91] The Inception Impact Assessment is available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12614-EU-police-cooperation. It should be noted that the provisions on the automated exchange of data and the provisions on operational police cooperation have no operational or technical link and function autonomously. The reason why they were included in the same instrument – namely the 2008 Prüm Decisions – is a historical one. Indeed, as will be explained further below in this evaluation, the Prüm Decisions incorporated the substance of the 2005 Prüm Convention, an intergovernmental treaty that was concluded between a small number of EU Member States, into the EU legal framework. For the purpose of operational and legal clarity, it was decided to revise the Prüm Decisions' operational cooperation provisions in the context of the future Police Cooperation Code.

for the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings.

(c) provisions on the conditions for the supply of information in order to prevent terrorist offences. Those provisions help Member States to exchange data when there are reasons to believe that criminal offences will be committed.

(d) provisions on the conditions and procedure for stepping up cross-border police cooperation through various measures. Those provisions help Member States to set up joint operations and provide each other with mutual assistance in connection with mass gatherings, in maintaining public order and security and in preventing criminal offences.

The focus of this report is to **evaluate the functioning of the automated exchange of data pursuant to the Prüm Decisions** (only letter a) as indicated above) and the level of implementation and application in each EU Member State since the adoption of the instruments in 2008, according to the five evaluation criteria set out in the Commission's Better Regulation Guidelines:[92]

1) *Relevance*: whether the tools provided by the Prüm Decisions for the automated exchange of data correspond to the current operational needs;

2) *Effectiveness*: whether the original objectives of the Prüm Decisions have been achieved as regards the automated exchange of data;

3) *Efficiency*: assessing the functioning of the Prüm Decisions as regards the automated exchange of data from a simplification and burden reduction perspective;

4) *Coherence*: examining how the Prüm Decisions work together with other relevant EU instruments in the field of data exchange;[93] and

5) *EU added value* of the Prüm Decisions as regards the automated exchange of data.

This evaluation has been carried out against the background of considerable developments and changes in terms of EU legal framework, operational needs, technical and forensic possibilities, and data protection requirements that have materialized since 2008. It aims at identifying best practices and possible key problems and obstacles that hamper the effective use of the Prüm Decisions.

The scope of the evaluation is the following:

- *Material scope*: the evaluation covers the current state of implementation of the Prüm Decisions and their functioning to the extent that they establish a decentralised system for the automated exchange of DNA, dactyloscopic data and vehicle registration data.
- *Geographical scope*: the evaluation covers all EU Member States and participating third countries.[94] Since the United Kingdom left the European Union as of 1 February 2020 and

[92] SWD(2017) 350 final.
[93] A non-exhaustive list of examples of EU instruments that have been introduced in the years since the adoption of the Decisions in 2008 and that are relevant in a cross-border law enforcement cooperation context include: the Entry/Exit System (EES), the Eurodac system, the Interoperability Regulations, etc.

the reference period for this evaluation is 2011-2020, this evaluation includes information on the United Kingdom.

- *Temporal scope*: the reference period for this evaluation runs from 2011 (implementation deadline for Chapter 2 of Council Decision 2008/615/JHA and Decision 2008/616/JHA) to 2020.

The implementation of the Prüm Decisions has been discussed in various fora over the past years, namely in the Commission report of 2012 on the implementation of the Prüm Decisions,[95] regular discussions in the Council Working Party DAPIX/IXIM,[96] several implementation projects at EU level such as the 'Mobile Competence Team' (MCT) project or establishment of a 'Prüm helpdesk' by Europol,[97] discussions in the High Level Expert Group on Information Systems and Interoperability,[98] the reports of four focus groups composed of Member States experts,[99] and the Commission study on the feasibility of improving information exchange under the Prüm Decisions.[100] This has allowed the establishment of a solid understanding of the benefits and of the difficulties and shortcomings encountered by law enforcement authorities when using the Prüm Decisions, pointing at a need to revise the EU legal framework. Moreover, the data protection framework has changed considerably. For that reason, it was decided to conduct the evaluation in parallel to the impact assessment ("back-to-back").

This evaluation assists in determining the level of EU intervention necessary for the efficient and effective exchange of data between law enforcement authorities when fighting crime and terrorism. The findings of this evaluation serve as one relevant input to the impact assessment.

---

[94] The EU has concluded an agreement on the application of certain provisions of the Prüm Decisions with Norway and Iceland (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D1023&from=EN), and is in the process of concluding a similar agreement with Switzerland and Liechtenstein. Even though the agreement entered into force between the EU and Norway on 1 December 2020, Norway is not yet operational for the exchange of data under any data category. The agreement between the EU and Iceland is not yet in force.

[95] COM(2012) 732 final.

[96] 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).

[97] 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. Where appropriate, informal expert groups were set up, which focussed on drafting best practice guides on implementation issues.
Europol established a 'helpdesk' as a permanent structure as of 2012 to support Prüm operational Member States for their daily operations regarding DNA and fingerprint data exchange. Furthermore, the helpdesk established a Europol Platform for Experts (EPE) in order to facilitate the sharing of relevant knowledge. The helpdesk closely aligned its activities with the MCT and the Commission.

[98] High Level Expert Group on Information Systems and Interoperability Final Report (May 2017), https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3435.

[99] Council documents 11264/19, 13356/19, 13511/19 and 13556/19 (not publicly available).

[100] Deloitte, Study on the Feasibility of Improving Information Exchange under the Prüm Decisions (May 2020).

2. BACKGROUND TO THE INTERVENTION

2.1. The context of the intervention

The Prüm Decisions (henceforth the 'Decisions') built on the **Prüm Treaty** (or Prüm Convention) on stepping up cross-border cooperation in combating terrorism, cross-border crime and illegal migration,[101] which was concluded by seven EU Member States in 2005, outside of the scope of the European Union legal framework. The Prüm Treaty left participation in such cooperation open to all other EU Member States and sought, as provided for by its article 1(4), to have its provisions brought within the legal framework of the Union three years after its entry into force. While a number of EU Member States acceded to the Prüm Treaty by 2008, not all Member States became contracting parties.[102] With the adoption of the Prüm Decisions by the Council in 2008, the substance of the provisions of the Prüm Treaty was incorporated into the legal framework of the European Union.[103]

The Prüm Treaty aimed to **improve data exchange between the contracting parties' law enforcement authorities**, in particular for the search and comparison of DNA, fingerprints and vehicle registration data, by means of direct online access to the databases of the State storing those data. When a law enforcement authority of a contracting party searches DNA or fingerprints data in another contracting party's databases, the reply received is a "hit" or a "no hit", depending on whether there is a match with data in the databases searched or not. This first step is based on reference data only, which does not contain any data from which the data subject can be directly identified. In case of a hit, the investigative authority may ask the State holding the data, in a second step, for further corresponding personal information. The supply of such follow-up information is governed by national law and national legal assistance of the supplying State.

The Prüm Treaty was drafted in line with the **Hague Programme** on strengthening freedom, security and justice in the European Union,[104] a multi-annual programme adopted by the European Council in 2005, which focused in particular on the improvement of police and judicial cooperation to fight organised cross-border crime and to repress the threat of terrorism. The Hague Programme emphasized the importance of the exchange of information as an operational prerequisite for internal security, and highlighted that such exchange of information should be governed by the **principle of availability**.[105] In the Hague Programme, the European Council underlined the need

[101] Prüm Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. Available here: https://data.consilium.europa.eu/doc/document/ST-10900-2005-INIT/en/pdf.

[102] The fourteen contracting parties were Belgium (Treaty in force since 06.05.2007), Bulgaria (23.08.2009) Germany (23.11.2006), Estonia (22.12.2008), Finland (17.06.2007), France (31.12.2007), Luxembourg (09.05.2007), the Netherlands (20.05.2008), Austria (01.11.2006), Romania (03.03.2009), Slovakia (28.05.2009), Slovenia (08.08.2007), Spain (01.11.2006) and Hungary (14.01.2008).

[103] Preamble of Council Decision 2008/615/JHA.

[104] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53 of 3.3.2005 p. 1.

[105] The principle of availability requires that throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties is entitled to obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated

for an innovative approach to the cross-border exchange of law enforcement information to strengthen freedom, security and justice. Subsequently, the Council and Commission Action Plan implementing the Hague Programme[106] announced the implementation of the principle of availability in the areas of DNA, fingerprints, ballistics, telephone numbers, vehicle registrations and civil registers. Finally, the Hague programme and the principle of availability were referred to explicitly in the preamble of Council Decision 2008/615/JHA.

In emphasizing the need for an innovative approach, the Hague Programme took into consideration the 2004 Communication from the Commission towards enhancing access to information by law enforcement agencies, which stated that "[a]t *present, law enforcement authorities can search databases that are nationally accessible. However, accessing information held by law enforcement services from other Member States poses challenges that amount to making them inaccessible in practice.*"[107]

Another relevant instrument in the field of law enforcement cooperation with regard to the principle of availability is Council Framework Decision 2006/960/JHA of 18 December 2006 (also known as the **Swedish Framework Decision** ('SFD') or the Swedish Initiative),[108] which aims at simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union and of the Schengen associated countries. At the moment of its adoption in 2006, it described the situation as follows: "[c]*urrently, effective and expeditious exchange of information and intelligence between law enforcement authorities is seriously hampered by formal procedures, administrative structures and legal obstacles laid down in Member States' legislation; such a state of affairs is unacceptable to the citizens of the European Union and it therefore calls for greater security and more efficient law enforcement while protecting human rights*."[109] To mitigate that situation and in developing the Schengen acquis, the Framework Decision aimed at simplifying the exchange of information and intelligence between law enforcement authorities of the Member States and of the Schengen associated countries. In implementing the principle of availability, it laid down the rules regarding time limits and standard forms for the exchange, on prior request or spontaneously, of information and/or intelligence, i.e.:

– any type of information or data which is held by law enforcement authorities; and

– any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures.[110]

---

purpose, taking into account the requirements of ongoing investigations in that State. If the information requested is available, it must be provided and the grounds for declining to do so are rather limited. The principle should be respected as of 1 January 2008. The principle was transposed into EU legislation by Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386 of 29.12.2006 p. 89.

[106] Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union, OJ C 198/1 of 12.8.2005 p.1.

[107] COM(2004) 429 final p. 7.

[108] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29.12.2006, corrected by Corrigendum, OJ L 75/26, 15.3.2007.

[109] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29.12.2006, corrected by Corrigendum, OJ L 75/26, 15.3.2007 (recital 6).

[110] Council Framework Decision 2006/960/JHA, article 2.

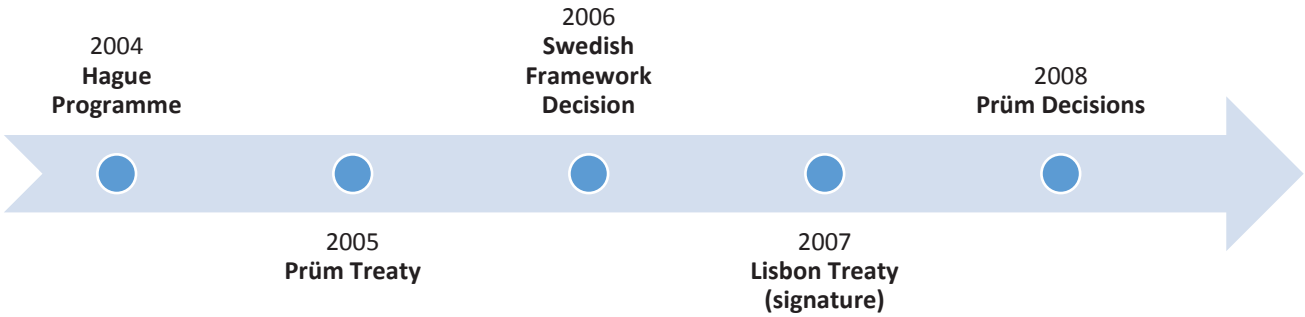


Figure 1: Timeline of the context of the Prüm Decisions

	YEAR	MS	SCOPE	CONTEXT
Prüm Treaty	2005	7 EU Member States[111]	Outside of the scope of the EU legal framework	Cross-border cooperation and automated exchange of DNA, fingerprints and VRD
Swedish Framework Decision	2006	27 EU Member States[112]	Part of scope of EU legal framework	Cross-border cooperation and information exchange between law enforcement authorities
Prüm Decisions	2008	27 EU Member States[113]	art of scope of EU legal framework	Automated exchange of DNA, fingerprints and VRD

Table 1 Main characteristics of legal instruments in the context of the Prüm Decisions

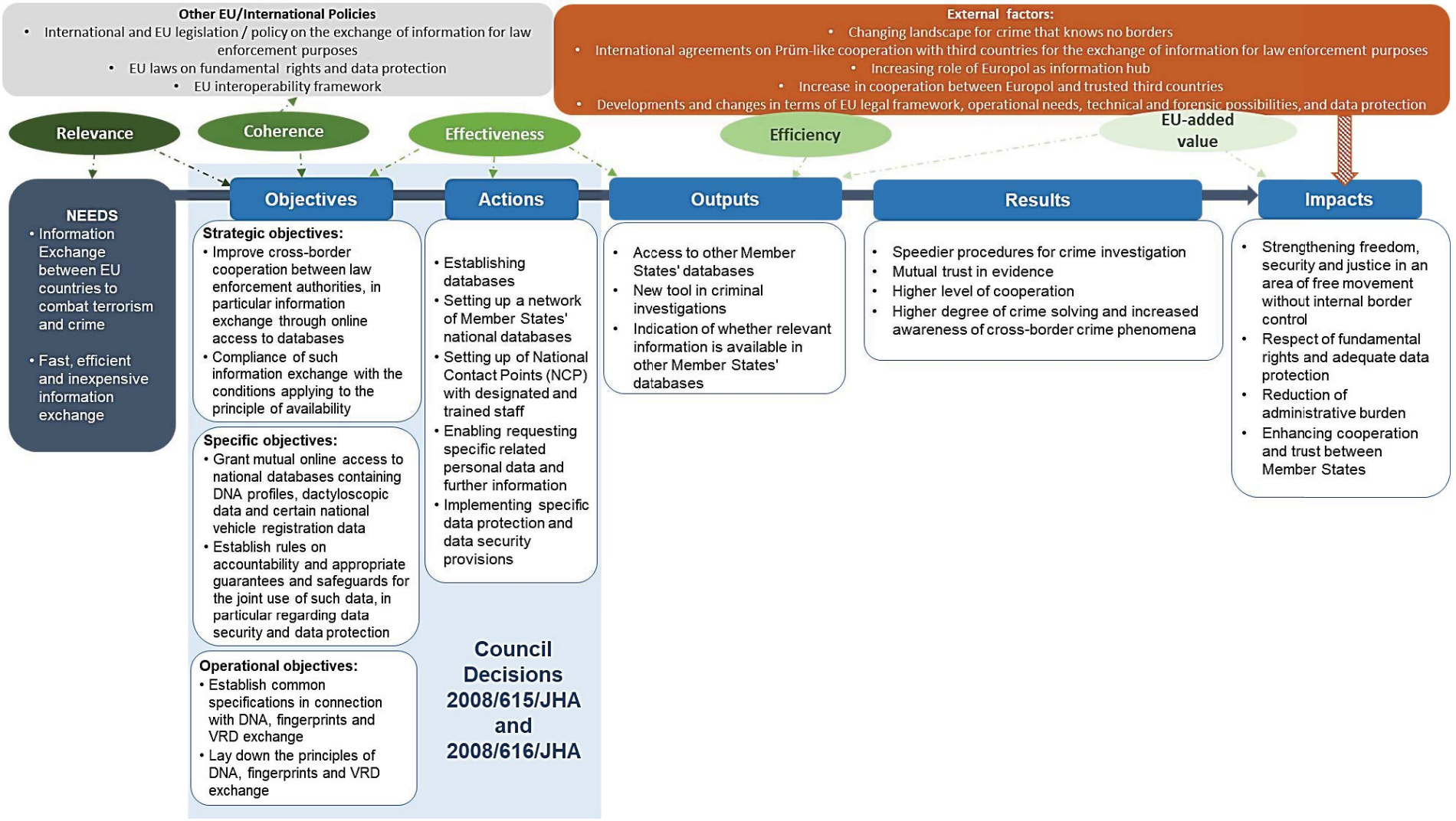
The proposal for the Prüm Decisions was put forward at the initiative of Belgium, Bulgaria, Germany, Spain, France, Luxembourg, the Netherlands, Austria, Slovenia, Slovakia, Italy, Finland, Portugal, Romania and Sweden, entitled to do so by the right of initiative shared between the Commission and the Member States under the third pillar of the Treaty on European Union. This led to the adoption of the Prüm Decisions in 2008. The rather broad scope of the Prüm Treaty was reduced as its incorporation into Union law focused on the substance of the Prüm Treaty referring to data exchange, data protection and police cooperation. Provisions on cooperation on illegal immigration were not incorporated into the Prüm Decisions.

2.2. The intervention logic of the Prüm Decisions

The adoption of the Prüm Decisions was not based on a prior impact assessment. There was also no prior evaluation of the application of the Prüm Treaty. Therefore, the intervention logic set out

[111] BE, DE, ES, FR, LU, NL and AT.
[112] BE, BG, CZ, DK, DE, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE.
[113] BE, BG, CZ, DK, DE, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE.

below is based on the adopted legal texts of the Prüm Decisions and the operational and legal circumstances at the time of their adoption in 2008.



The starting point for the negotiations of the Prüm regime was the **need for a fast, efficient and cost-effective means of law enforcement information exchange to combat terrorism and crime**. Plurality of national administrative, legal and judicial systems, lack of common standards and procedures resulted in difficulties in law enforcement information exchange. At the same time, access to the right information in a timely and efficient manner is key in any criminal investigation, and even more so in the area of free movement of goods, services and persons.

The intervention logic therefore identified as a general, strategic objective the streamlining of police cross-border cooperation and, to that end, brought it in line with state-of-the-art communication technologies. The focus was set on measures enhancing the collection, storage, processing, analysis and exchange of law enforcement information based on the principle of availability. Member States agreed to follow an innovative approach in this area aiming at:

- establishing a mesh network of Member States' national databases with mutual access rights. This preference for a decentralised structure was based on the understanding that no new centralised European database should be created unless their added value has been duly proven;[114] and

- defining specific measures both with regard to security and protection of personal data and with regard to the data subjects' rights, in order to respect fundamental freedoms and due to the lack of a Union legal basis regarding the protection of personal data processed by law enforcement authorities.[115]

To achieve the ambitious objectives and to frame this cooperation, the legislator foresaw:

- national databases for DNA and dactyloscopic data files to be established and kept for the investigation of criminal offences, and for certain vehicle registration data, for the purpose of search and comparison of these data;

[114] See the Hague Programme for strengthening freedom, security and justice p. 8 and the preamble of Council Decision 2008/615/JHA recital 7.

[115] Council Framework Decision 2008/977/JHA (OJ L 350/60, 30.12.2008), which provides for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, was adopted later than the Prüm Decisions, namely on 27 November 2008, and set 27 November 2010 as the deadline by which Member States had to take the necessary measures to comply with that Decision. The Framework Decision was repealed by Directive (EU) 2016/680 (OJ L 119/89, 4.5.2016) 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 (the 'Law Enforcement Directive'). However, in accordance with article 60 of the Law Enforcement Directive, the specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, remain unaffected. According to article 60 (6) of the Directive, the Commission is tasked to assess the need to align the said legal acts with the Directive and to make, where appropriate, the necessary proposals to amend them to ensure a consistent approach to the protection of personal data within the scope of the Directive. This assessment was conducted in the context of the 2020 Communication on the way forward on aligning the former third pillar acquis with data protection rules; see COM(2020) 262 final.

- mutual cross-border access rights to these databases; and

- rules on accountability and appropriate guarantees and safeguards for the joint use of such data, in particular with regard to both security and protection of personal data.

Accordingly, Decision 2008/615/JHA

- lays down general rules on the conditions and the procedure for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data (chapter 2), and

- defines the general framework on data protection for the processing of personal data in line with the purposes of the Decision (chapter 6),

while Decision 2008/616/JHA

- provides in particular for the necessary measures for the implementation of the provisions of chapter 2 of Decision 2008/615/JHA, which were to be based on the Implementing Agreement of 5 December 2006 concerning the administrative and technical implementation and application of the Prüm Treaty;

- establishes the common normative provisions for the administrative and technical specifications necessary for implementing the envisaged data exchange pursuant to chapter 2 of Decision 2008/615/JHA; and

- sets out the technical implementing provisions in its Annex, in particular the evaluation procedure to be followed as a prerequisite before the launch of the automated exchange of each data category can be initiated.

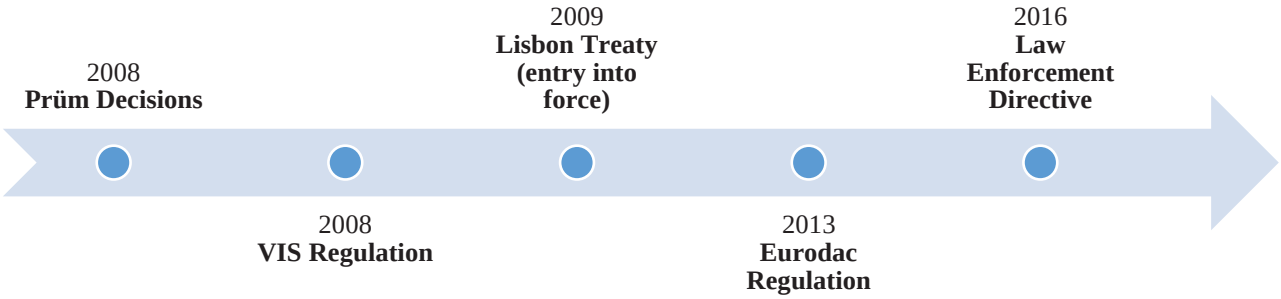
As a consequence, Member States had to provide for appropriate national legislation to comply with the provisions of the Decisions. They had to establish, if not already established before or under the Prüm Treaty, national databases and national contact points (NCPs) for the search and comparison and for the supply of data respectively. NCPs were to be designated for incoming and outgoing requests relating to information exchange in each data category. For the automated exchange of DNA, fingerprint data and VRD, the Trans European Services for Telematics between Administrations (TESTA II) communications network was chosen and Member States were to ensure the automated searching or comparison of those data 24 hours a day and seven days a week. For the exchange of VRD, it was decided to make use of the European Vehicle and Driving Licence Information System (EUCARIS), a system established for the exchange of data on vehicle registration, driving licences and the accompanying personal data, connecting national registration authorities. A specific application was developed within this system, for the exchange of VRD under the Prüm Decisions.[116]

[116] Council Decision 2008/616/JHA, article 15.

The facilitation of the cross-border data exchange under the Prüm Decisions was expected to speed up the existing procedures enabling a Member State to find out whether any other Member State, and if so, which, has the information it needs, and to open up a new dimension in crime fighting by cross-border data comparison.[117] Cooperation between law enforcement authorities would grow together with increased trust in evidence received from other Member States due to the use of common forensic standards. Finally, the technical and procedural set-up of the system guarantees the respect of fundamental rights, in particular the right to respect for privacy and to protection of personal data.

2.3. Evolution of the context

Considerable developments and changes in terms of the EU legal framework, operational needs, technical and forensic possibilities,[118] and data protection requirements have materialized since 2008.



[117] Council Decision 2008/615/JHA (recitals 11 and 12).

[118] Council Decision 2008/616/JHA obliges Member States to use existing standards for DNA data exchange, such as the European Standard Set (ESS). Council Resolution (2009/C 296/01) of 30 November 2009 on the exchange of DNA analysis results, taking account of the results in the DNA Working Group of the European Network of Forensic Institutes (ENFSI) on the harmonisation of the DNA markers and DNA technology, encouraged Member States to implement as soon as practically possible the extended ESS, as annexed to that Resolution. Accordingly, Member States upgraded the Prüm software by the extended ESS in 2012.
Council Framework Decision 2009/905/JHA on accreditation of forensic service providers carrying out laboratory activities, applies to laboratory activities, in particular forensic service providers relating to such sensitive personal data as DNA profiles and dactyloscopic data. Pursuant to Article 7(4) of Council Decision 2008/616/JHA), Member States shall take the necessary measures to guarantee the integrity of DNA profiles made available or sent for comparison to other Member States and to ensure that these measures comply with international standards, such as EN ISO/IEC 17025. The purpose of the Framework Decision is to ensure that the results of laboratory activities carried out by accredited forensic service providers in one Member State are recognised by the authorities responsible for the prevention, detection and investigation of criminal offences as being equally reliable as the results of laboratory activities carried out by forensic service providers accredited to EN ISO/IEC 17025 within any other Member State. The application of EN ISO/IEC 17025 was part of the evaluation visits prior to the adoption of a Council Decision to launch DNA or dactyloscopic data exchange.

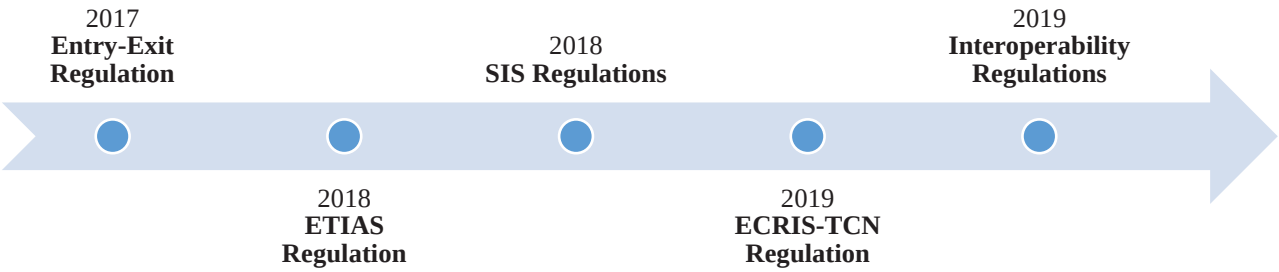


Figure 2: Timeline of the evolution of the context of the Prüm Decisions

The Justice and Home Affairs (JHA) information exchange legal framework has undergone significant change over the past 13 years, with the strengthening and the maximisation of the benefits of existing information systems and the establishment of new information systems. Indeed, on the one hand, in November 2018, the further reinforcement of the existing Schengen Information System (SIS)[119] improved the sharing of information between Member States by introducing new types of alerts and the use of biometrics. It also enhanced the use of SIS in the context of counter-terrorism, vulnerable people and irregular migration, and the access to SIS for EU agencies. Additionally, negotiations are ongoing on the revised legal basis for the EU asylum fingerprint database (Eurodac)[120] and for the Visa Information System (VIS),[121] including law enforcement access to these systems.

On the other hand, additional information systems have been established to address identified gaps in the EU's data management architecture: the Entry/Exit System (EES)[122] and the European Travel Information and Authorisation System (ETIAS)[123] to strengthen security checks on visa-free

[119] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312, 7.12.2018; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018; 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.

[120] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29.6.2013.

[121] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008.

[122] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017.

[123] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19.9.2018.

travellers by enabling advance irregular migration and security vetting. The European Criminal Record Information System for third-country nationals (ECRIS-TCN)[124] is under development to address the identified gap in the exchange of information between Member States on convicted non-EU nationals.

In June 2016, the Commission set up a high-level expert group on information systems and interoperability in order to elaborate on the legal, technical and operational aspects of options to achieve interoperability between EU information systems for borders, migration and security.[125] The high-level expert group identified shortcomings and potential information gaps caused by the complexity and fragmentation of information systems, and made a number of recommendations to address these. This work resulted in the adoption of the Interoperability Regulations establishing a framework for interoperability between EU information systems in the area of justice and home affairs.[126] Easier information sharing will considerably improve security in the EU, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration while safeguarding fundamental rights.

These developments have widened law enforcement access to data in the EU central systems in the area of Justice and Home Affairs, have enhanced the use of biometrics for the purpose of identification and verification of identity and have changed the roles of the EU bodies acting in the JHA area. These developments need to be taken into account when evaluating the fitness of the Prüm Decisions in the current law enforcement information management landscape.

The architecture of Justice and Home Affairs (JHA) cooperation also changed considerably with the adoption of the **Treaty of Lisbon**, which not only formally abolished the Pillar structure, but also transferred the supervision of compliance with and implementation of EU law on police and judicial cooperation in criminal matters from Member States' domestic authorities to the European Parliament, the Commission and the European Court of Justice (CJEU).[127] This shift implied transnational legal, judicial and democratic accountability of national laws and practices meant to implement EU law, and, in particular, of the extent to which EU legislation is timely and duly observed by national authorities.

However, while paving the way for that shift, the Lisbon Treaty introduced transitional provisions. They limited for a period of five years (1 December 2009 to 1 December 2014) the enforcement powers of the Commission and the CJEU's scrutiny over legislative measures adopted before the entry into force of the Lisbon Treaty under the then 'third pillar' (Title VI of the former version of

[124] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019.
[125] See the Final report of the High-level expert group on information systems and interoperability, available here: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600.
[126] 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.
[127] Treaty of Lisbon (2007), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT.

the Treaty on the European Union). Furthermore, Article 10(1) to (3) of Protocol 39 on Transitional Provisions stated that the legal effects of pre-Lisbon 'common positions', 'framework decisions' and 'decisions' as defined in Article 34 of the former TEU would be preserved until such acts are amended or replaced (or, indeed, repealed or annulled).

It follows from this and from the judgement of the CJEU of 22 September 2016 that the provisions of the Prüm Decisions would stay in force as adopted in 2008.[128] In this same judgment, the Court refused the attribution of co-decision powers to the European Parliament in the evaluation procedure to be followed by Member States before they can start exchanging data (see below, Section 2.4). The European Parliament is, however, to be consulted before the decision on the launch of automated data exchange in a Member State is taken by the Council.[129]

Considerable developments of the EU data protection framework have materialized since 2008, with the adoption of the **General Data Protection Regulation ('GDPR')**[130] and of the **Law Enforcement Directive ('LED')**[131] in 2016. Only the LED is relevant in this context as competent law enforcement authorities under the Prüm framework process and transfer natural persons' sensitive personal data (e.g. biometric data) for the prevention, investigation, detection or prosecution of criminal offences. In the absence of an EU data protection legal framework at the adoption of the Prüm Decisions, specific provisions were included in the Decisions. According to these provisions, Member States were to guarantee, in their national law and as regards the processing of personal data supplied pursuant to the Prüm Decisions, a level of protection that is at least equal to that resulting from the Council of Europe Convention taken as a reference in the Prüm Decisions.[132] As set out in the June 2020 Communication on the way forward on aligning the former third pillar acquis with the data protection rules, there is a need to ensure that a revised Prüm legislation is fully aligned with the Law Enforcement Directive, especially as regards the data protection safeguards.[133]

[128] Judgment of the Court of Justice of 22 September 2016, European Parliament v Council of the European Union, C- 14/15 and C- 116/15, ECLI:EU:C:2016:715, paragraph 43: '...a provision of an act duly adopted on the basis of the EU Treaty before the entry into force of the Treaty of Lisbon, which lays down detailed rules for the adoption of other measures, continues to produce its legal effects until it is repealed, annulled or amended...'.

[129] The Council Decisions dating from before that judgement and vitiated by a procedural defect were subsequently replaced by Council Implementing Decision (EU) 2017/945, (EU) 2017/946 and (EU) 2017/947, OJ L 142, 2.6.2017.

[130] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[131] 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.

[132] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001. Article 25 of Council Decision 2008/615/JHA.

[133] COM(2020) 262 final.

2.4. Key elements of the automated exchange of data in the Prüm Decisions

The core of the Prüm Decisions lies in the automated exchange of three categories of data: DNA, dactyloscopic data ('fingerprints') and vehicle registration data. For that purpose, each Member State has to grant the other Member States access to its national databases so that each Member State can check its reference data against the reference data in other Member States' databases. The reference data does not contain any data from which the data subject can be directly identified.

When Member States search DNA or dactyloscopic data in other Member States' databases, the reply they receive is a "hit"- or a "no hit"-message, depending on whether there is a match with reference data in the databases searched or not. When the comparison results in a "hit", the searching Member State receives an automated message specifying only the reference data of the corresponding profiles in the respective databases. A forensic expert of the requesting Member State then verifies whether the match is sufficiently relevant and reliable, and reports it to the relevant law enforcement or judicial authority (depending on the national administrative and legal system). Only after this forensic verification has taken place can further personal and case-related data corresponding to the hit be requested. This request and the subsequent exchange of follow-up data is not governed by the Prüm Decisions, but by the national law, including the legal assistance rules, of the requested Member States.

For vehicle registration data, the search needs to be conducted with a full chassis number or a full licence plate number. Should data searched for relating to the owner/operator or to the vehicle be available in the consulted databases, the data are provided immediately, without a request for further personal or case-related data having to be introduced separately in a second step.

Before a Member State can start exchanging data, it needs to undergo an evaluation procedure in accordance with article 25 of Decision 2008/615/JHA and article 20 of Decision 2008/616/JHA.[134] This procedure aims to verify whether the Member State concerned has implemented the general provisions on data protection (Chapter 6 of Decision 2008/615/JHA) into its national law. It is up to the Council to decide whether this implementation condition has been met and subsequently to authorise the launch of the automated exchange of data pursuant to the Prüm Decisions by the Member State concerned.[135]

Once a Member State has taken the necessary measures to comply with the Decisions and believes it fulfils the prerequisites for sharing data, it notifies the General Secretariat of the Council and the Commission thereof and submits the declarations foreseen and the replies to the questionnaires on data protection and on the data category concerned by the evaluation to the relevant Council Working Party.[136] Upon endorsement of these replies, a pilot run and an evaluation visit related to the data category in question is carried out by experts from supporting Member States, which are

[134] This is without prejudice to article 25(3) of Decision 2008/615/JHA, according to which this evaluation procedure shall not be necessary for those Member States that had already started exchanging data under the Prüm Treaty. These Member States were Belgium, (VRD), Germany (DNA, fingerprints, VRD), Spain (DNA, fingerprints, VRD), France (DNA, VRD), Luxembourg (DNA, fingerprints, VRD), the Netherlands (DNA, VRD), Austria (DNA, fingerprints, VRD), Romania (DNA, FP), Slovenia (DNA, fingerprints, VRD), Finland (DNA).

[135] It should be noted that at the moment of drafting this evaluation, some Member States still have not completed the evaluation and hence have not yet started to exchange data under the Prüm Decisions.

[136] The relevant Council Working Party here is DAPIX – and as from 1 January 2020, IXIM.

already operational and sharing data. A report on the outcome of the evaluation visit is to be produced by the evaluation team while consulting the Member State concerned and to be endorsed by the relevant Council Working Party.

On that basis, the Council proceeds to the adoption of Council Conclusions on the fulfilment of data protection requirements, and subsequently to the adoption of the Council Implementing Decision on the launch of automated exchange of the respective data for the Member State concerned. The Council Implementing Decision, which specifies the date from which the Member State concerned can start exchanging data, is adopted by the Council after having consulted the European Parliament.

Once the evaluation procedure is complete and the Member State concerned has been authorised to exchange data in the relevant category pursuant to article 25(2) and, in particular, article 33 of Decision 615/2008/JHA, it can set up the required bilateral connections for DNA and fingerprints, and start cooperating with already operational Member States.

The situation with regard to vehicle registration data exchange is slightly different. Indeed, once the Member State has undergone the required evaluation with respect to VRD and has been duly authorised by the Council, it connects to the EUCARIS application and is thereby automatically connected to all other operational Member States. Member States do not need to establish bilateral connections separately with each other.

2.5. Automated searching and comparison of DNA data

To assess the likelihood of the involvement of a suspect in a crime, forensic scientists compare DNA found at a crime scene to DNA reference samples taken from this suspect and analysed to establish the individual's DNA profile. If there is no match, the suspect may be ruled out. If, however, there is a match, further information may be requested.

DNA profiling in the criminal justice system started in 1986. Since then, thanks to forensic and technical developments, highly accurate testing procedures have been developed. DNA profiling has a high level of accuracy and can provide strong evidence when linking or exonerating a suspect to or from a crime. However, DNA profiling, despite being very accurate, remains only one element in the overall investigation.

In order to build up the Prüm network for DNA data exchange, Member States first had to establish and to keep national DNA analysis files for the investigation of criminal offences. Secondly, Member States had to make available data from their databases as reference data for automated search and comparison within the Prüm framework. Finally, Member States granted each other direct cross-border access to each other's national DNA analysis files for the purpose of investigating criminal offences in individual cases.[137] Dedicated national contact points act as agencies competent for sending and receiving requests relating to information exchange.

[137] The analysis files open for cross-border access and the conditions for automated searching are laid down in Declarations. They are referred to in the Manual setting out factual information on the implementation of the Decisions to be submitted to the General Secretariat of the Council and kept up to date by it. See, for the latest available version of

The DNA search and comparison under the Prüm Decisions is done on the basis of, according to the Prüm terminology, 'anonymous profiles', i.e. on the basis of reference data from the national DNA analysis files. This reference data does not allow the direct identification of the data subject. Two types of profiles are to be distinguished: the 'reference DNA profile', which refers to an identified person, and the 'unidentified DNA profile', which refers to traces found on a crime scene and not yet attributed to a known person.

'Full matches' or 'near matches' are defined in detail in the Prüm Decisions.[138] In case a search is performed under the Prüm framework, both instances of full or near matches and 'no hits' are reported in an automated way to the requesting and to the requested national contact point.

In case of a match between supplied data and data stored in the searched file, the searching Member State receives the reference data with which the match has been found and no data immediately revealing the data subject. Once the match has been confirmed by the requesting Member State according to the rules of the Prüm Decisions, this Member State may request further personal data and other information relating to the reference data that is the subject of the match. The exchange of this follow-up data is conducted outside the scope of the Prüm Decisions, subject to the national rules of the requested Member State. Annual Figures on the dimension of national DNA databases and sent DNA profiles as well as on national match statistics are compiled on the basis of a model agreed upon by the relevant Council Working Party. The General Secretariat of the Council produces an annual summary overview on the basis of these statistics submitted by the Member States.[139]

2.6. Automated searching and comparison of dactyloscopic data

Fingerprints provide the police with physical evidence that links suspects to evidence or crime scenes. Dactyloscopic analysis is based on the principle that each individual has distinguishing biometric features, in this case fingerprints, which are recognizable and verifiable. Computer processing of fingerprints began in the early 1960s with the introduction of computer hardware that could reasonably process these prints. Since then, the introduction of Automated Fingerprint Identification Systems (AFIS) replacing laborious and time-consuming manual processing of fingerprints by automated processing has remarkably improved crime solving performance. These systems process and store digitised fingerprint images (reference data) and enable the comparison of this reference data to crime scene traces.

In order to build up the Prüm network, Member States had to establish national automated fingerprint identification systems for the prevention and investigation of criminal offences and make their reference data available for automated search and comparison across borders. Dedicated national contact points act as agencies competent for sending and receiving requests relating to information exchange.

---

the state of implementation (16 April 2021): https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.

[138] Council Decision 2008/616/JHA, p. 21.

[139] See, for the latest available version (19 April 2021), Council document 5729/21 (not publicly available).

Dactyloscopic search and comparison under the Prüm Decisions is done on the basis of, according to the Prüm technology, 'anonymous profiles', i.e. on the basis of reference data from the national AFIS. This reference data does not allow to identify directly the data subject. Two types of profiles are to be distinguished: tenprints and latents. While the former refer to fingerprints taken from a known individual under well-defined technical conditions, the latter are recovered from a crime scene or physical evidence and not yet attributed to a known person. Latents are often only partial or highly fragmented and therefore less reliable. In case of a search with a latent in other Member States' AFIS, several potential matches might be retrieved, which require further analysis and interpretation by forensic experts to verify the reliability of these matches. The confirmation of a potential match and the request for further personal data in a second step take place in the same way as with DNA (see above).

In order to allow for the calibration of the national AFIS connected with each other in the Prüm network, Member States define in line with the principle of reciprocity maximum daily search capacities. The search capacities for data of identified persons and for data of not yet identified persons are set out in the Manual kept up to date by the General Secretariat of the Council. Figures on outgoing requests and verified hits are compiled in accordance with a model agreed upon by the relevant Council Working Party. The General Secretariat of the Council produces an annual summary overview on the basis of these statistics submitted by the Member States.[140]

2.7. Automated searching of vehicle registration data

Access to vehicle registration data under the Prüm Decisions should provide law enforcement authorities with useful information in three different scenarios:

- in the prevention and investigation of criminal offences;
- in dealing with other offences coming within the jurisdiction of the courts of the public prosecution service in the searching Member States; and
- in maintaining public security.

For these purposes, Member States grant each other on-line access to a specified set of national vehicle registration data, which may be consulted across the border: data relating to the owners or operators and data relating to vehicles. Such automated searching is to be carried out in compliance with the searching Member State's national law and is restricted to individual cases, that is to a single investigation or prosecution file. The search can be launched either with the chassis number (vehicle identification number) or with the licence plate. While in the former case, the search can be carried out in one or all of the participating Member States, in the latter case, the search can only be performed in one participating Member State.

To carry out such searches, Member States use a dedicated version of the European Vehicle and Driving License Information System (EUCARIS) software application, and where necessary, amended versions of that software. The application connects all participating Member States in a mesh network where each Member State communicates directly to another Member State. There is

[140] See, for the latest available version (19 April 2021), Council document 5729/21 (not publicly available).

no central component needed for the communication to be established.[141] Dedicated national contact points act as agencies competent for sending and receiving requests relating to the exchange of VRD.

An overview of the license plates/vehicle types for which the Member State will make VRD available in the framework of Council Decision 2008/615/JHA is set out in the manual, comprising factual information provided for the Member States, prepared and kept up to date by the General Secretariat of the Council.[142] Annual statistics on VRD searches are prepared by the EUCARIS secretariat, referring to the total annual amount of EUCARIS/Prüm inquiries and responses. They are set out in the annual summary overview produced by the General Secretariat of the Council.[143]

[141] Council Decision 2008/616/JHA, p. 66.
[142] See, for the latest available version (16 April 2021) of the state of implementation: https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.
[143] See, for the latest available version (19 April 2021), Council document 5729/21 (not publicly available).

3. IMPLEMENTATION / STATE OF PLAY

3.1. Baseline and points of comparison

The information available on the baseline situation prior to the adoption of the Prüm Decisions and to the conclusion of the Prüm Treaty is very limited and no quantitative data that could provide a point of comparison was identified. There are no statistics available on the pre-Prüm regime cross-border data exchange between Member States at EU level. Therefore, this evaluation focused on descriptions of the pre-Prüm situation, as set out in a report to the JHA Council of 1/2 December 2005,[144] using qualitative data where possible. At the time of drafting this report:

- The majority of Member States had DNA databases with the capability to compare DNA profiles from other Member State with the profiles contained in their own databases. However, much international data exchange continued to take place within the EU via the classic "police-to-police" approach of indirect access to information upon request or through using mutual legal assistance (MLA) channels. Various channels of communication for such indirect exchanges existed, including via the national Interpol, Europol or SIRENE national units or bureaux, or via the bilateral liaison officers network. Procedures in place for exchanging DNA data were deemed to be time consuming and resource intensive;
- Fingerprints were exchanged on a regular basis upon request between Member States, mostly via the Interpol National Central Bureaux, though in certain Member States mutual legal assistance was required. Law enforcement authorities also noted that the procedures for exchanging fingerprint data could be time consuming, subject to error and resource intensive;
- VRD was exchanged between Member States via three principal channels. First, through informal, reciprocal, arrangements which existed between registration authorities. Second, through ad hoc requests transmitted via existing law enforcement communication channels such as via the Interpol, Europol or Sirene bureaux. Third, through the EUCARIS platform which, however, at that time had not yet been formally established.

At the time of the adoption of the Prüm Decisions, the cross-border exchange of information between police authorities was governed, on the one hand, at central level by the Schengen acquis and the use of the Schengen Information System and, on the other hand, at decentralised level by intergovernmental bilateral and multilateral agreements.

At political level, the European Council set forth, in the Hague Programme of November 2004, its conviction that an innovative approach to the cross-border exchange of law enforcement

[144] The 'Report of the Friends of the Presidency on the technical modalities available for implementing the principle of availability' (13558/1/05) was presented to the JHA Council of 1/2 December 2005. The report focussed on six areas of information: DNA; fingerprints; ballistics; vehicle registrations; telephone numbers; and minimum data for the identification of persons [contained in civil registers]. The report had been prepared against the backdrop of a series of initiatives, forthcoming or under way, that were seeking to implement the principle of availability, i.e. the Commission and Council Action Plan to implement the Hague Programme and the Prüm Treaty. It summarised the situation regarding DNA, fingerprint data and VRD exchange. See https://data.consilium.europa.eu/doc/document/ST-13558-2005-REV-1/en/pdf (partially publicly available).

information was needed. In line with the requirements of the Hague Programme, the Prüm Treaty was concluded between a small number of EU Member States.

As examined in Section 2.1, the Swedish Framework Decision described at the moment of its adoption in 2006 the situation of cross-border law enforcement cooperation as follows (recital 6): "[c]*urrently, effective and expeditious exchange of information and intelligence between law enforcement authorities is seriously hampered by formal procedures, administrative structures and legal obstacles laid down in Member States' legislation; such a state of affairs is unacceptable to the citizens of the European Union and it therefore calls for greater security and more efficient law enforcement while protecting human rights.*" The SFD has a wide scope and broadly covers the exchange of information between law enforcement authorities while the automated Prüm exchange process for certain data categories (DNA, dactyloscopic data and VRD) is deemed in this context to be a sub-set of information exchange.

In order to meet the substantive requirements of the Hague Programme and to make applicable the substance of the essential parts of the Prüm Treaty to all Member States, its relevant parts with regard to police cooperation were brought into the EU legal framework by the adoption, on 23 June 2008, of the Prüm Decisions.

3.2. Description of the current situation and state of play of implementation of the Prüm Decisions

The Decisions were adopted on 23 June 2008, and entered into force on 26 August 2008. Member States were given until 26 August 2011 to implement Chapter 2 of Decision 2008/615/JHA and the relevant provisions of Decision 2008/616/JHA into national law.[145] An overview on the state of play of the general implementation and in particular, of the degree of bilateral connectivity is set out in the Manual kept by the GSC.[146]

According to article 36(4) of Decision 2008/615/JHA, the Commission was to submit a report to the Council by 28 July 2012 on the implementation of Decision 2008/615/JHA. In the 2012 Report on the Implementation of Council Decision 2008/615/JHA (hereinafter the '2012 Report'),[147] the Commission noted considerable delays in the implementation process. On 31 October 2012, the state of play of the implementation was as follows:

- DNA: 18 Member States were operational
- Fingerprints: 14 Member States were operational
- VRD: 13 Member States were operational

In order to support the implementation of the Prüm Decisions, the Commission has made funding available through the Prevention of and Fight against Crime programme (ISEC) and the Internal Security Fund-Police.[148] Besides funding, several initiatives (e.g. the Mobile Competence Team

[145] Article 36(1) of Council Decision 2008/615/JHA and article 23 of Council Decision 2008/616/JHA.
[146] See, for the latest available version of the state of implementation (16 April 2021): https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.
[147] COM(2012) 732 final.
[148] SWD(2017) 278 final.

(MCT) and the Prüm helpdesk at Europol) were also put in place to support Member States in their efforts. A number of operational Member States with considerable experience in running the Prüm instrument could be consulted for advice.

According to the 2012 report, the main reasons for implementation delays were technical in nature and caused by a lack of human and financial resources in the Member States. The 2012 report also stated that bearing in mind the indicated technical problems and scarce resources, it was surprising that non-operational Member States had been reluctant to request support from the assistance tools put in place. Indeed, in reply to a questionnaire circulated to Member States in the context of the preparation of the final report of the Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, only 3 Member States reported that their implementation process had been supported by a MCT or the Europol helpdesk. The report concluded that "*given the various possibilities to obtain support and the long period of time that has elapsed since the adoption of the two Prüm Decisions, it is hard to see any reasons which could justify lack of implementation. What is needed above all seems to be political will and appropriate prioritisation to overcome barriers at national level.*"

The Commission repeatedly invited the Member States to take necessary action (e.g. in the 2012 report, in the European Information Exchange Model (EIXM) communication[149] and in the 2015 European Agenda on Security)[150] to complete the implementation of the Prüm Decisions.

Decision 2008/616/JHA only outlined the evaluation procedure and called upon the relevant Council Working Party to define the details. That evaluation procedure was only set out in 2010 with the final approval of the data exchange questionnaires, the reply to which serves as a pre-requisite for any evaluation of a Member State's legal and technical readiness to start Prüm data exchange. Additionally, the peer-to-peer evaluation procedure itself requests a lot of coordination between numerous stakeholders as to pilot runs, evaluation visits and drafting of reports. The procedure became heavily bureaucratic, cumbersome, more time consuming than expected and turned out to be a complex issue in its own. Finally, the adoption[151] of the Council Decision up to its publication in the Official Journal to enter into force also takes time. These elements may partially explain the slow implementation of the Prüm Decisions in the EU Member States. Other elements will be analysed in Section 5 (see notably 5.2, Q5).

Therefore, the deadline 3 years after the adoption of the Decisions, probably was too ambitious for the implementation of chapter 2 of Decision 2008/615/JHA, not to mention the establishment of all bilateral connections necessary for the completion of the entire Prüm network. However, nearly ten years after the deadline for the implementation of the Decisions expired, the fact that this deadline was perhaps a bit too ambitious cannot explain why some Member States have still not completed the implementation.

[149] COM(2012) 735 final.
[150] COM(2015) 185 final.
[151] The European Parliament is entitled to be consulted prior to the adoption of a Council Implementing Decision on the launch of automated data exchange. In line with the Inter-institutional Agreement, the European Parliament may requests three up to four months for a consultation period. However, consultation had no impact on the failure to comply with the initial deadline because consultation was systematically applied only subsequent to the ECJ judgement of 22 September 2016 in Joined Cases C-14/15 and C-116/15.

Following the expiry of the transitional period under Article 10(3) of Protocol 36 to the Treaties ceasing five years after entry into force of the Treaty of Lisbon, i.e. on 1 December 2014, the limitations to the judicial control by the Court of Justice of the EU and to the Commission's enforcement powers regarding former third pillar instruments which have not been repealed, annulled or amended after the entry into force of the Lisbon Treaty, have been lifted. Since that date, the Commission can, under Article 258 TFEU, monitor the complete and correct transposition and implementation of these instruments. This includes the possibility of launching infringement proceedings where appropriate. Using these new possibilities, on 29 September 2016 the European Commission addressed letters of formal notice to Croatia, Greece, Ireland, Italy and Portugal for failing to comply with the Prüm Decisions. These Member States had not yet ensured automated data exchanges in at least two of the three data categories of DNA, fingerprints and national vehicle registration data. As of December 2020, two of these infringement cases were still open, against Italy and Greece.

In addition to the launch of infringement proceedings, the Commission organised a workshop, which took place on 19 January 2017 with Member States on the implementation of the Prüm Decisions, designed primarily for the benefit of practitioners to allow them to learn from one another and build even stronger cooperation.[152] Experienced, operational Member States shared their experiences of using the system, including what lessons they have learned and how they have addressed various challenges that they faced over the years. Member States concurred in highlighting the benefits that they have obtained by using Prüm – with large numbers of 'matches' providing assistance in criminal investigations.

By 16 April 2021, the state of play of the implementation of the Prüm Decisions was the following:[153]

- 26 Member States and the United Kingdom[154] had been authorised by the Council to exchange DNA profiles;[155]
- 26 Member States and the United Kingdom had been authorised by the Council to exchange dactyloscopic data;[156]
- 25 Member States had been authorised by the Council to exchange vehicle registration data.[157]

However, it has to be noted that in the case of DNA and fingerprints, the number of Member States authorised to start exchanging data under the Prüm Decisions does not show if the Member State actually exchanges data with other Member States. Indeed, the formal authorisation to start

[152] SWD(2017) 278 final.
[153] See, for the latest available version of the state of implementation (16 April 2021): https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.
[154] Under the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, EU law on law enforcement information exchange, including data exchange in accordance with the Prüm Decisions applied to and in the United Kingdom until the end of the transition period. The EU-UK Trade and Cooperation Agreement (TCA) includes a title on the exchange of DNA, fingerprints and vehicle registration data, which mirrors the current Prüm legislation. Subject to certain conditions to be met by the UK, the Council may take Decisions with regard to each data category in order for the UK to continue participating in the Prüm framework, under the TCA.
[155] All EU Member States except IT.
[156] All EU Member States except IT.
[157] All EU Member States except EL and IT. The UK had not received the authorisation to exchange VRD either.

exchanging data granted by the Council (as explained above, see Section 2.4) means that the Member State in question has successfully passed the evaluation procedure and is therefore operational for the data category in question. It does not, however, mean that it is exchanging data (DNA or fingerprints) as this Member State needs to establish bilateral connections with each other Member State before it can actually start exchanging DNA or fingerprint data. For VRD, as examined above, the situation is slightly different as the Member State connects to the EUCARIS application and is thereby automatically connected to all other Member States, without having to establish bilateral connections.

As of 16 April 2021, 26 Member States (+ UK) had been authorised to exchange DNA or fingerprint data, and 25 Member States had been authorised to exchange VRD.[158] However, some Member States had not established any bilateral connections (i.e. are not exchanging any DNA or fingerprints) despite the fact that by the respective Council Implementing Decisions they have been authorised to do so.[159] Indeed, full implementation of the Prüm automated data exchange system requires that all of the 378 possible connections in the respective data categories have been established between Member States (+ the UK). As 16 April 2021, of all possible bilateral connections between Member States (and the UK), 72 % had been established in the case of DNA, 71 % in the case of fingerprints, and 88,4 % in the case of VRD.[160]

Data category	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
DNA	11	13	18	21	22	22	22	24	26	27	26 + UK
FP	6	9	14	16	18	21	22	24	26	26	26 + UK
VRD	8	10	12	15	19	20	20	23	24	25	25

Table 2 Evolution of the number of Member States authorised to exchange data

The below tables[161] visualize the degree of connectivity in each data category. A grey box shows that a bilateral connection exists, a white box that it still needs to be established.

[158] See, for the latest available version of the state of implementation (16 April 2021): https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.
[159] EL (DNA and dactyloscopic data), HR (dactyloscopic data).
[160] See, for the latest available version of the state of implementation (16 April 2021): https://data.consilium.europa.eu/doc/document/ST-5383-2021-REV-1/en/pdf.
[161] See, for the latest available version (19 April 2021), Council document 5729/21 (not publicly available).

	DNA operational data exchange																												
	BE	**BG**	**CZ**	**DK**	**DE**	**EE**	**EL**	**ES**	**FR**	**HR**	**IE**	**IT**	**CY**	**LV**	**LT**	**LU**	**HU**	**MT**	**NL**	**AT**	**PL**	**PT**	**RO**	**SI**	**SK**	**FI**	**SE**	**UK**	
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	

Table 3 State of play on the operational exchange of DNA as of 31 December 2020

	Fingerprints operational data exchange																												
	BE	**BG**	**CZ**	**DK**	**DE**	**EE**	**EL**	**ES**	**FR**	**HR**	**IE**	**IT**	**CY**	**LV**	**LT**	**LU**	**HU**	**MT**	**NL**	**AT**	**PL**	**PT**	**RO**	**SI**	**SK**	**FI**	**SE**	**UK**	
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	

Table 4 State of play on the operational exchange of dactyloscopic data as of 31 December 2020

	VRD operational data exchange																												
	BE	**BG**	**CZ**	**DK**	**DE**	**EE**	**EL**	**ES**	**FR**	**HR**	**IE**	**IT**	**CY**	**LV**	**LT**	**LU**	**HU**	**MT**	**NL**	**AT**	**PL**	**PT**	**RO**	**SI**	**SK**	**FI**	**SE**	**UK**	
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	

Table 5 State of play on the operational exchange of VRD as of 31 December 2020

Both the dimension of cross-border crime and the extent to which the Prüm data exchange network stepped up cross-border criminal investigation to cope with that phenomenon is shown in annual statistics. While each operational Member State compiles, in accordance with a model defined by the relevant Council Working Party, quantitative statistics on the direct access to national DNA and dactyloscopic data in other Member States' databases, VRD statistics are compiled by the EUCARIS Secretariat.

The figures for each elapsed year are set out in the summary overviews produced by the General Secretariat of the Council since 2012.[162] With more Member States becoming operational and the number of established bilateral connections growing, the total number of Prüm cross-border consultation and matches has overall increased over time. The figures demonstrate, indeed, that law enforcement authorities effectively make use of the automated consultation of each other's databases and of the instrument. However, the figures do not provide any case-specific indication as to the sort of crime or offence that has been investigated at national level nor do they indicate whether a match has been followed-up at all, and hence, whether a match has been decisive for an investigation. Since the follow-up to Prüm data exchange is covered by the respective national legislation, such information could be part of national accountability regarding law enforcement activities.

Data category	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
DNA – total matches	20 686	26 264	24 457	38 268	37 313	40 376	35 316	49 050	60 635	62 944
FP – total verified matches	2 568	3 874	4 594	5 855	5 826	8 146	9 499	10 131	10 080	9 933
VRD – total responses with information found	260 253	695 624	1 498 663	2 038 618	2 176 172	2 758 120	3 422 180	4 479 207	4 756 849	4 680 496

Table 6 Evolution of the number of matches per data category[163]

One reply to the public consultation gave the following as an illustration of how the Prüm automated data exchange has helped to fight crime and terrorism from a Member State's perspective:

The Prüm automated data exchange with regard to fingerprints was used over 14.000

[162] Member States provide the General Secretariat of the Council with annual statistics on the results of automated data exchange, in accordance with the model defined by the relevant Council Working Party. These statistics have been used in this evaluation, based on the summary overviews produced by the General Secretariat of the Council since 2012: 11367/1/12 REV 1; 7146/2/13 REV 2; 5968/3/14 REV 3; 5503/2/15 REV 2; 5129/1/16 REV 1; 6126/17; 5509/18; 5323/19; 5199/20; 5729/21. However, this information is not publicly available.

[163] The imbalances between these figures do not reflect the overall importance of the individual data types but the fact that different data types are used in differing ways in police practice.

times in 2020. In 620 cases, this resulted in information from another EU country that was relevant for the investigation.

Moreover, recently adopted Regulations further reinforce the importance of the Prüm Decisions. This is the case for example of the Entry-Exit System (EES) Regulation,[164] where it is established that access to the EES for the purposes of identifying unknown suspects, perpetrators or victims of terrorist offences or other serious criminal offences should be allowed only on the condition that searches in the national databases of the Member State have been carried out and the search with the automated fingerprinting identification systems of all other Member States under the Prüm Decisions has been fully conducted, or the search has not been fully conducted within two days of being launched.

[164] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

4. METHOD

4.1 Short description of methodology

The evaluation aimed to analyse the implementation and application of the Prüm Decisions in each EU Member State according to the five evaluation criteria set out in the Commission's Better Regulation Guidelines (relevance, coherence, effectiveness, efficiency and EU added value).[165] The evaluation covered all operational EU Member States and their implementation of the Decisions from their adoption in 2008 until the end of 2020.

The implementation of the Prüm Decisions has been discussed in various fora over the past years, namely in the Commission report of 2012 on the implementation of the Prüm Decisions,[166] regular discussions in the Council Working Party DAPIX/IXIM, several implementation projects at EU level, discussions in the High Level Expert Group on Information Systems and Interoperability,[167] the reports of four focus groups composed of Member States experts,[168] and the Commission study on the feasibility of improving information exchange under the Prüm Decisions.[169] This has allowed the establishment of a solid understanding of the benefits and of the difficulties and shortcomings encountered by law enforcement authorities when using the Prüm Decisions, pointing at a need to revise the EU legal framework. Moreover, the data protection framework has changed considerably. For that reason, it was decided to conduct the evaluation in parallel to the impact assessment ("back-to-back").

The evaluation relied on:

- the reconstruction of the intervention logic of the Prüm Decisions, showing the objectives of the intervention and the chain of expected effects (outputs, outcomes and impacts);
- desk research on EU and national information and previously compiled data in various projects and reports;
- field research, including interviews, workshops and questionnaires targeted to law enforcement agenciesfield research, including interviews, workshops and questionnaires targeted to law enforcement agencies;[170]
- the results of the public consultation that the European Commission launched in December 2020 to collect opinions on the effectiveness of the current legislative and policy framework and on existing problems and possible options for future

[165] SWD(2017) 350 final.
[166] COM(2012) 732 final.
[167] High Level Expert Group on Information Systems and Interoperability Final Report (May 2017).
[168] Council documents 11264/19, 13356/19, 13511/19 and 13556/19 (not publicly available).
[169] Deloitte, Study on the Feasibility of Improving Information Exchange under the Prüm Decisions (May 2020).
[170] Please see Annex 2 for more information on the consultation strategy.

initiatives. Please see Annex 2 for more information on the results of the consultation.[171]

4.2 Limitations and robustness of findings

- One of the main limitations of this evaluation is a general lack of statistics and quantitative data at EU and Member States' level on the functioning of the Prüm Decisions. According to article 21 of Decision 2008/616/JHA, statistics should support the evaluation of the administrative, technical and financial application of operational automated data exchange. In 2011, discussions in the Council Working Party DAPIX on Prüm statistics led to a common agreement between Member States on how to compile statistics on the results of the automated data exchange. According to that agreement, Member States compile statistics on DNA and dactyloscopic matches with connected Member States. These statistics were designed in a way to justify, in quantitative terms, Prüm data exchanges by putting in relation the number of requests and the number of matches following a request. As stated in the 2012 report, *"[i]n many Member States, the authority recording Prüm matches is not the same as that using the data for investigations. And often only a third authority, such as the prosecutor's office, is able to assess the value of a certain piece of information originating in the Prüm exchange.* (…) *Due to* [these] *administrative difficulties, the majority of Member States have opted for a statistical model focusing on the number of matches between data sets.*" Since the Prüm Decisions do not define the scope of application in qualitative terms, i.e. the type of crime investigated, there are no statistics on the type of crime investigated and no statistics on whether a hit was followed up on and eventually led to the solving of a criminal case.
- Despite this common agreement on the statistical model reached in 2011, discrepancies continue to exist to a certain degree between figures submitted by each Member State on DNA matches. It is difficult to explain and understand these discrepancies as a match is always reported to the NCPs of both the requesting and the requested Member State and there should therefore be a certain concordance. In stakeholder consultations, it was pointed out that more precise Prüm related statistics are also missing at Member State level. Thus, conclusions regarding these statistics are to be met with some reservations. Therefore, where quantitative data was not available, qualitative evidence was provided in the analysis.

  Over the years, the implementation of the Prüm Decisions, the evaluations of Member States and projects aiming to improve the implementation of the Prüm Decisions have been thoroughly discussed in the Council Working Group DAPIX, which is meeting approximately six times a year. In stakeholder discussions with Member States, "a questionnaire fatigue" was noticed, especially related to re-stating the obvious benefits and hurdles of implementing the Prüm Decisions. As a result, in

[171] The questions of the public consultation served as a basis for the evaluation questions which sought to address the five evaluation criteria. Please see Annex 6 for the list of the evaluation questions.

order to reduce Member States' (administrative) burden in carrying out this evaluation, existing information was used as much as possible.[172]

- The baseline situation before 2008 was not fully known. Indeed, as examined above in Section 3, the information available on the baseline situation prior to the adoption of the Prüm Decisions is very limited and no quantitative data that could provide a point of comparison was identified.

[172] Such as the 2012 report, the EIXM communication, the results of the public consultation, the HLEG report.

5. ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS

5.1. Relevance

To what extent are the Prüm Decisions relevant in view of current and future needs/challenges?

Main findings:

- The Prüm Decisions are 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 Prüm Decisions meet the needs of criminal investigators, of victims of crime, of forensic specialists, of database custodians and of legal practitioners.
- Council Decision 2008/616/JHA contains detailed inclusion and matching rules, technical specifications, security measures, etc. that have not been updated since its adoption. Some of these rules are outdated or no longer relevant as forensic science and information technology have significantly developed since 2008.

Q1. To what extent are the Prüm Decisions relevant in view of current and future needs/challenges related to security and more precisely criminal investigations?

The starting point to assess the relevance of the Prüm Decisions is related to the need to exchange data between Member States' law enforcement authorities in order to prevent and investigate criminal offences. Data from EU SOCTA 2017 and 2021 clearly states that criminals act across borders.[173] In an area without internal borders, it is important to remove borders and obstacles when it comes to data exchange between law enforcement authorities, which lead to blind spots and loopholes for numerous criminals and terrorists that act in more than one Member State. Given the cross-border nature of crime fighting and security issues, Member States alone cannot close the information gap and have to rely on one another to effectively prevent and investigate criminal offences.

[173] European Union Serious and Organised Crime Threat Assessment, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

For a growing group of Member States, Prüm has become a routine tool in investigating crime with a potential cross-border dimension. The ability to conduct automated comparisons of data found at crime scenes against comparable data held in other Member States remains a significant tool for law enforcement.[174] As shown in table 6 on the evolution of the number of matches per data category, the total number of Prüm cross-border matches has increased overall over time. These matches show that the Prüm framework is used in practice. The fact that data comparison results in hits in various Member States proves that criminals do act across borders.

The following example from Germany illustrates the value of Prüm in a cross-border context:

In the late summer of 2011 a man was found stabbed to death in a north-western German city. On the crime scene, police experts discovered a fingerprint on a door frame in the apartment where the man had been found. Although there was no obvious link to another country, an automated Prüm search led to a hit in the Bulgarian AFIS database. The follow-up information requested from Bulgaria the following day was sent within three hours and was immediately entered into the Schengen Information System. Already the next day the individual concerned was arrested in Austria.[175]

In their contributions to the public consultation, **stakeholders highlighted that cooperation and the exchange of information between Member States' law enforcement authorities for the prevention and investigation of criminal offences is very relevant**. Being able to search and compare DNA, fingerprint and vehicle registration data in other Member States' databases for the prevention and investigation of criminal offences has also been highlighted as very relevant. Cooperation and exchange of information between Member States' law enforcement authorities are deemed by stakeholders to be of paramount importance for safeguarding the internal security of the EU and the safety of its citizens.

In reply to the public consultation, it was also specified that the direct access to vehicle registration data for law enforcement on the street has contributed to policing in the areas of prevention, emergency assistance and criminal investigations. Before the adoption of the Prüm Decisions, vehicle registration data was only available after a lengthy procedure and often therefore not useful (especially not for public order policing). It was highlighted in the public consultation that the hit-no hit search in databases for DNA and fingerprints has contributed to a decrease in time-consuming processes with multiple Member States, as it enables law enforcement to quickly identify links across the EU and provides essential information for criminal investigation and prosecution of criminals. One stakeholder pointed out that its use of the Prüm mechanism for the exchange of information has increased considerably over the years, as its number of matches across countries was multiplied by thirty between 2011 and 2019.

[174] SWD(2017) 278 final.
[175] COM(2012) 735 final.

The following examples were given by respondents to the public consultation to show the relevance of the Prüm Decisions in view of current and future needs/challenges related to security and more precisely criminal investigations:

A number of events took place in spring 2019 where unidentified criminals were able to sweep ATM cash in different small towns in Estonia. Estonian forensics managed to collect DNA data from the scenes, which had not been entered in Estonian registers. Through the exchange of Prüm DNA data, the authorities managed to identify these individuals as DNA profiles were available in several Member States. This made it possible to dismantle a criminal group and arrest individuals.

In the context of the knife attack in The Hague on 29 November 2019, the perpetrator fled after having injured three bystanders in the crowd. The knife used, which had been found on the scene of the attack, bore traces of DNA. A query of the automated databases of national DNA profiles revealed a match with a DNA profile in the French database.

According to Estonia, to the extent that a very large number of countries collect and share VRD data, the possibility to search for VRD via Prüm brings a high added value to investigating and combatting cross-border crime. It makes it possible to determine the history of the vehicle as well as to provide investigators with preliminary information on the possible owners (users) of the vehicle, which in turn allows further enquiries to be carried out if necessary (for example via Interpol or requests for legal assistance to Member States).

The theft of luxury vehicles is often linked to organised crime. In such cases, it is common practice for stolen vehicles to use falsified VRD data. The Prüm query makes it possible to identify the previous vehicle life history and/or Vehicle Identification Number code and thereby to carry out the necessary investigations.

Estonian law enforcement authorities have also benefited from the exchange of insurance data. In the last few years, the authorities have had a number of cases of falsified insurance policies presented to them at the border. Prüm made it possible to quickly verify the vehicle's insurance.

Q2. To what extent do the Prüm Decisions correspond to the needs/interests of the stakeholders?

Investigators need to have fast and seamless access to all the information they need and which they are legally entitled to in order to perform their tasks to successfully prevent and investigate crime. This need has been repeatedly emphasised in DAPIX/COSI[176] discussions and Council Conclusions.[177] **Stakeholders broadly**

[176] Standing Committee on Operational Cooperation on Internal Security.
[177] See the Council Conclusions on Internal Security and European Police Partnership as the most recent example, 13083/1/20REV 1 (24 November 2020).

confirmed in the contributions received to the public consultation **that the Prüm Decisions correspond to the needs of criminal investigators**.

The results of the public consultation also highlighted that the Prüm Decisions correspond to the needs of victims of crime and address the needs/interests of forensic specialists. Additionally, stakeholders stated that the Prüm Decisions correspond to the needs/interests of database custodians, and to the needs/interests of legal practitioners.

Regarding the needs/interests of data protection authorities, it was highlighted that the Prüm Decisions were adopted in 2008 (before the adoption of the Law Enforcement Directive). Thus, there is a need to assess the Prüm Decisions in view of the relevant data protection framework. Information exchange between law enforcement authorities in EU Member States may affect the fundamental right to privacy and to the protection of personal data of the individuals whose personal data is transferred to authorities in other Member States. This is why specific data protection provisions were included in the Prüm Decisions. However, the data protection legal framework has considerably developed since the adoption of the Prüm Decisions, as pointed out in Section 2.3, requiring examination to ensure that all relevant safeguards are in place.

According to a questionnaire circulated by the Commission in preparation of the 2012 report and to which 25 Member States (all except MT and PT) replied, more than half of the competent authorities in Member States see an important added value in the areas of VRD and DNA data exchange for the prevention and investigation of criminal offences.[178] For fingerprints, about 40 % of respondents attach a considerable value to the instrument while more than 50 % consider it to add at least some value.

However, concerns about the fact that the follow-up to Prüm hits takes place outside the scope of the Prüm framework (see Section 2.1) have been raised as hindering the functioning of the Prüm system in various occasions from the beginning. Already in 2012, in reply to the same questionnaire, 18 out of 24 Member States generally pointed to the need to improve the follow-up to Prüm hits, one third focusing on national structures while a majority saw a need for action primarily at EU level.[179]

As highlighted by stakeholders in the stakeholder consultations, one of the key success factors for the Prüm framework is the possibility to search and compare data in an automated manner in other Member States' databases. However, this possibility currently covers only a few categories of data: DNA, dactyloscopic and vehicle registration data. There are some other categories of data in Member States' databases that are often the subject of cross-border information requests for the purpose of criminal investigations, but which are exchanged in an inefficient way. The need to examine the possibility to extend the scope of the Prüm Decisions to include data categories such as facial images, police records, driving licences and ballistic data has been highlighted by many stakeholders in their replies to the public consultation.

[178] COM(2012) 732 final.
[179] COM(2012) 732 final.

Q3. Are there any aspects of the Prüm Decisions that might be considered obsolete? (e.g. technical, security, forensic)

Council Decision 2008/616/JHA contains detailed inclusion and matching rules, technical specifications of queries, security measures, communication etc. that have not been changed since the adoption of the Prüm Decisions. **Some of these rules are outdated as forensic science and information technology have significantly developed since 2008**. Some examples of the outdated features of the Prüm legal framework include the protocols and standards for encryption, the need for upgrades to the latest forensic biometric standards used (ANSI/NIST-ITL latest versions) and for updates related to the alignment with the European Standard Set for DNA loci and the detailed matching rules on rare loci details, etc.

The rapid development of technology and of forensic tools and the outdated legal text in this regard raise the question of whether the current type of instrument is appropriate for such types of common technical specifications. As the case of the Prüm Decisions show, for these specifications, a more flexible legal instrument would be needed, such as implementing act(s). Such an instrument would allow for more flexibility in updating the purely technical specifications to ensure the highest level of quality and security for cross-border exchanges of data.

5.2. Effectiveness

To what extent have the Prüm Decisions been effective in delivering the intended results?

Main findings:

- The Prüm Decisions have improved the exchange of data between the Member States to the extent that they partially automated the process, thereby making it faster and less burdensome for law enforcement authorities.
- However, the implementation of the Prüm Decisions has been slow. Indeed, nearly ten years after the implementation deadline on 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 may decrease the possibility that criminals are identified, and cross-border links between crimes are detected, hindering 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 hindering the functioning of the Prüm system. Indeed, due to differences in national rules and procedures, the exchange of hit follow-up data is very fragmented, to the extent that it sometimes takes weeks or even months to receive the relevant information behind a hit.

Q4. Have the Prüm Decisions improved the exchange of data between Member States? If so, how?

As explained in Section 3.1, in 2005, some Member States had DNA databases with the capability to compare DNA profiles from other Member State with the profiles contained in their own databases. Fingerprints were exchanged on a regular basis upon request between Member States and VRD was exchanged between Member States. However, the procedures in place for exchanging those categories of data were deemed to be time consuming, subject to error and resource intensive.

The objective of the Prüm decisions is to step up cross-border cooperation, particularly the exchange of information between authorities responsible for the prevention and investigation of criminal offences. It did so by automating certain steps in the information exchange process, by harmonising data, and by introducing an obligation to establish DNA analysis files (national DNA databases for criminal investigations).

In their replies to the public consultation, almost all respondents clearly stated that the Prüm framework has improved the exchange of data between Member States, specifying that increased and faster access to the data has facilitated law enforcement authorities' work. One stakeholder highlighted that its main benefits are the provision of IT interfaces to query other Member States and standardized format of requests. Prüm allows for automated searching without the intervention of the country surveyed. It also makes it possible to avoid passing through judicial cooperation channels and to be obliged to identify the correct interlocutor in each of the countries concerned. In addition, procedures and formalism are simplified through the use of single forms. As regards forensic work, Prüm has significantly reduced the administrative burden in order to compare data. However, the workload for the National Contact Point (NCP/Single Point of Contact (SPOC)) did not decrease as the exchange of information following correspondence has increased.

Q5. If not, what has prevented the effective implementation?

As examined in Section 3 above, **the implementation of the Prüm Decisions has been slow**. Indeed, nearly ten years after the implementation deadline on 26 August 2011, all Member States have not yet completed the evaluation procedure and a number of

bilateral connections have not been established. Several factors may explain the slow implementation or lack thereof in some Member States. However, it is difficult to assess as there are little statistics available, as examined under Section 4.

One major factor can nonetheless be identified following consultations with stakeholders: the need to establish bilateral connections with each other Member State for each data category. **Some Member States have explained that setting up all the connections and maintaining them is technically complex and requires considerable financial and human resources**. For these reasons, they have decided to focus on establishing connections with prioritised Member States. As a consequence, queries cannot be checked against the data in some Member States if the relevant bilateral connection has not been established. This may decrease the possibility that criminals are identified, and cross-border links between crimes are detected.

As stated in the 2012 report, other aspects hampering the use of Prüm relate to a number of specifications for the automated data exchange laid down in the Prüm Decisions. In reply to the public consultation, it was stressed that the integration of the technical requirements from Decision 2008/616/JHA has been an obstacle to make the necessary amendments and updates to the Prüm system at technical level and has made it less adaptable to national needs.

A considerable number of Member States consider that the matching rules, in particular for DNA data, are not fully satisfactory and should be re-designed so as to avoid matches that lead to "false positive" results and are identified as false upon subsequent verification.[180]

Another problem commonly raised by experts relates to the specifications concerning the interface control document (ICD) for fingerprint exchange, which leaves too much room for interpretation in its current version and thus can lead to technical incompatibilities between different uses of this ICD.[181]

Moreover, some Member States pointed to the ceilings agreed bilaterally between Member States, defining the maximum daily search capacities of a requested Member State. More efficient use of these limited search capacities in the area of fingerprint data is suggested by some Member States to ease the danger of overloading national systems. These Member States suggested that the capacities not used by one Member State should be available for use by others, whereby the Member State receiving the request should itself indicate when the limit of its search capacity has been reached.[182]

A few Member States have expressed concerns regarding the national capacities for verifying transmitted potential matches (candidates) after a request with fingerprint data.[183] Indeed, upon sending a query with fingerprint data, a candidate list with potential

[180] COM(2012) 732 final.
[181] COM(2012) 732 final.
[182] COM(2012) 732 final.
[183] COM(2012) 732 final.

matches (‘hits’) for this fingerprint data is returned to the Member State. The requested Member State then needs to verify these hits before requesting personal data related to these hits. The more Member States become operational in this area, the more staff resources need to be available for this required manual verification of hits to avoid a situation where this requirement constitutes a limitation on fingerprint data exchange.[184] In reply to the public consultation and regarding legal aspects, it was noted that the changes in national legislation were hard to manage for some of the Member States, which led to long delays in national implementation.

As concluded in the 2012 Report, improved functioning of the system would create an even stronger incentive for swift implementation.

Q6. What are the main obstacles for smooth information exchange under the Prüm Decisions?

The fact that some bilateral connections have not yet been established due to the technical complexity and the important financial and human resources entailed (see Q5) constitutes a major obstacle for smooth information exchange. As stated in the 2017 Comprehensive Assessment of EU Security Policy, **there is an implementation gap in some Member States which reduces the overall potential of the Prüm Decisions**.[185] Indeed, if a bilateral connection has not been established between 2 Member States, these Member States’ law enforcement authorities will not be able to find out if relevant data is available in the other Member State, preventing any information exchange from taking place.

As stemmed out from consultations with stakeholders, another obstacle is the **lack of standardisation for follow-up on hits**, which hinders the information exchange according to Member States. Automated searches in Member States’ DNA and fingerprints databases under the Prüm Decisions are based on reference data only. This reference data does not contain any data from which the data subject can be directly identified. Further personal and other case related data is exchanged only when a hit has been confirmed by a forensic expert. This exchange of “hit follow-up data”, however, is not governed by the Prüm Decisions, but by national law.[186] Due to differences in national rules and procedures, the exchange of hit follow-up data is very fragmented: Member States use different law enforcement cooperation channels, different procedures, different data sets and different time limits when requesting and submitting follow-up data. Consequently, the processes are so cumbersome and time-consuming that in some cases, it takes weeks or even months to receive the relevant information behind a hit.[187]

[184] COM(2012) 732 final.
[185] SWD(2017) 278 final.
[186] Articles 5 and 10 of Council Decision 2008/615/JHA.
[187] COM(2012) 732 final.

Some experts particularly criticised the **lack of standardisation of the channel used for follow-up requests of information**.[188] For managing follow-up requests, roughly equal use is made of the Europol (SIENA) and Interpol (i-24/7) channels[189] while only a few Member States prefer the SIRENE bureaux or bilateral liaison officers. In some Member States, the choice depends on the type of data; in others, it depends on the type of crime. In any event, it is a rather heterogeneous picture, which according to experts sometimes leads to delays.

Finally, bilaterally-agreed ceilings between Member States define the maximum daily search capacities of a requested Member State. Although these ceilings are necessary to prevent a national system from collapsing due to too many requests, they can prevent certain – potentially urgent and important – requests from being received and treated, thereby also hampering information exchange.

Member States have tried to take action to address the shortcomings of Prüm. For instance, through a project led by Finland, Member States analyzed the national procedures applied following a hit. The final report of this project[190] recommended a series of non-mandatory good practices to streamline the post-hit information exchange throughout the EU. 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.[191] It is, however, not known to what extent National Contact Points use these forms. Despite all these actions, the shortcomings remained the same as the ones that were described in the 2012 report.

5.3. Efficiency

To what extent have the Prüm Decisions achieved the intended results in the most efficient manner?

Main findings:

- 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 was found that these benefits outweigh the investment required for the

[188] COM(2012) 732 final.
[189] In reply to a questionnaire circulated to Member States in the context of the preparation of the final report of the Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, 3 Member States reported using SIENA, ten Member States reported using Interpol and 4 Member States reported using both SIENA and Interpol.
[190] See document 14310/2/16 REV2 for more information.
[191] See document 9383/13 for more information.

implementation of the Prüm framework.

- Moreover, the automated Prüm system provides substantial savings in working time.
- However, it was stressed that there is still an administrative burden with regards to hit verification and reporting, and also to receipt/transmission of second step information.

Q7. To what extent has the automated data exchange under the Prüm Decisions brought any efficiency gains in the law enforcement information exchange?

It stems from consultations with stakeholders that one of the key success factors for the Prüm framework is **the possibility to search and compare data in an automated way in other Member States' databases**. This possibility **brought efficiency gains in the law enforcement information exchange to the extent that it simplified and sped up the process, reducing the administrative burden on Member States' law enforcement authorities**. Indeed, law enforcement authorities no longer have to manually search their national databases upon reception of a query from another Member State, as this part of the process has been automated. Moreover, law enforcement authorities are now able to find out very quickly if information relevant to their cases is available in another Member State and if so, where.

Most stakeholders reported in their replies to the public consultation that the automated data exchange under the Prüm framework has brought efficiency gains in the law enforcement information exchange to a large extent regarding the speed of exchanges. Regarding the administrative burden, the costs and the staff, the replies were more diverse. However, all stakeholders reported efficiency gains regarding these three aspects to a certain extent.

By preventing the need to query each Member State bilaterally, the automated data exchange under the Prüm framework improves the speed of exchanges and the administrative burden in particular. The automated Prüm system provides substantial savings in working time. However, it was stressed that there is still an administrative burden with regards to hit verification and reporting, and also to receipt/transmission of second step information (the level of administrative burden depending on the internal procedures of relevant institutions).

One stakeholder highlighted that the exact impact regarding costs and staff is difficult to ascertain and that they do not keep such specific data on efficiency gains (for example the change in waiting time for the responses, the change in the number of queries per official that the law enforcement authorities are capable of serving, the change in the costs of respective information systems/ICT developments, etc). Another stakeholder replied that this mechanism may sometimes involve additional treatment of sources, but it is the price to be paid for having more sources. The French National Contact Point (NCP/SPOC) is not in a position to provide statistical data on the evolution of response

time. As regards step 1 of the exchange of dactyloscopic data, the time saving is considerable (a few hours instead of days). In terms of profiles identified, almost all transactions are managed during the day. In traces, quotas affect the speed of processing for cases containing several traces.

When asked whether the costs (administrative, budgetary, in terms of personnel, etc.) related to the implementation of the Prüm framework have been proportionate to its contribution in terms of the improvements in law enforcement information exchange, stakeholders replied completely or to a certain extent (large or some) for each of the three categories of data covered under the Prüm Decisions. It was specified that the benefits (speed of exchanges, administrative burden) outweigh the investment required for the implementation of the Prüm framework and that the costs for the VRD/National Contact Point are low in any case.

According to Estonia, the highest efficiency of the Prüm data exchange lies in the speed of the data exchange. The information reaches the investigators without delay, thereby making the way forward and the efficient conduct of the procedure effective.

5.4. Coherence

To what extent are the Prüm Decisions coherent and complementary to other relevant interventions at EU and international level?

Main findings:

- Regarding data protection, even though specific data protection provisions were included in the Prüm Decisions, the data protection legal framework has considerably developed since 2008, requiring that any revision of the legal instrument ensures that all relevant safeguards are in place.
- 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, such as the Entry-Exit System (EES).
- Potential synergies can be identified regarding Europol and the interoperability

framework.

Q8. Are there any overlaps/contradictions/complementarities/synergies/gaps between the Prüm Decisions and any other relevant EU/international legislation?

Over time, several EU and international initiatives and systems aiming at facilitating the exchange of information between law enforcement authorities have been developed, such as the **Europol Information system** (EIS), **Interpol's information systems** and the **Schengen Information System** (SIS). When asked to what extent do you agree/disagree that the Prüm framework complements other EU and international action in the area of law enforcement information exchange, stakeholders either fully agreed or tended to agree.

One stakeholder specified that the Prüm mechanism automates the principle of availability of information implemented by the SFD. The Prüm mechanism is also complementary to the SIS as it does not only concern wanted persons. The SIS targets wanted or alerted persons, while Prüm gives access to individuals implicated and/or convicted in their State. In addition, Prüm allows automated batch comparison of DNA data in other Member States' national files. Conversely, for States not participating in Prüm (third States and non-operational Member States in Prüm), consultations can only be carried out on a case-by-case basis in the context of secure institutional channels for police cooperation. Batch searches are possible in the Interpol DNA database, but the number of data available is very limited compared to national genetic files. The exchange of data in the framework of Prüm, although subject to improvement, has become essential in the fight against terrorism and cross-border crime.

Another stakeholder wrote that the Prüm framework complements the existing exchange of information between law enforcement authorities because it allows for an access to the complete databases of the exchanging party. In the case of Interpol, SIS and Europol, Member States chose the information they want to contribute to these databases, so they can be deemed less complete than the national ones.

Therefore, based on the evidence presented above, it can be said that **there are mostly complementarities between the Prüm Decisions and other relevant EU/international legislation**. Firstly, the Prüm framework applies to EU Member States when the Interpol's information systems include other countries as well. Secondly, the SFD has a wide scope and broadly covers the exchange of information between law enforcement authorities while the automated Prüm exchange process for certain data categories (DNA, dactyloscopic data and VRD) is deemed in this context to be a sub-set of information exchange. Thirdly, the Prüm framework is used in individual investigation cases for the prevention and investigation of criminal offences (particularly cross-border crime and terrorism) while the second generation Schengen Information System ('SIS II') is used for controls at external borders and searches by law enforcement officials for wanted persons and crime-related objects. As stated in the 2017 Comprehensive Assessment of EU Security Policy, "*Prüm is primarily a tool to assist in the investigation of serious*

criminal offences. It is mainly used as a way to identify the originator of a crime stain (biological material of latent fingerprint), generating an important element in criminal investigations, potentially leading to an arrest or even to the conviction of the individual. As such, it contains a very high verification threshold in order to ensure that the correct individuals are arrested and eventually convicted. Prüm is not designed as an identity checking tool for border guards or to give immediate answers or an on the spot instruction to a police officer or a border guard to take action. This presents an essential difference compared to databases like the SIS, which functionality it is to allow for such checking and specific follow-up instructions. As such, the use of the Prüm system serves a different purpose compared to SIS. These systems are complementary rather than in competition to each other."[192]

There are also complementarities with some of the EU central information systems that serve different purposes than investigations for law enforcement purposes. However, Prüm comes into play in the context of access to those systems for the purposes of preventing and fighting serious crime and terrorism. This is the case for example of the Entry-Exit System (EES) Regulation,[193] where the search with the automated fingerprinting identification systems of all other Prüm operational Member States under the Prüm Decisions is a pre-condition for querying the system for law enforcement purposes.

Potential synergies can be identified regarding Europol and the interoperability framework. Indeed, the interoperability framework provides synergies between information systems to contribute to the purposes of these systems. This includes providing competent authorities and end-users of the EU information systems with fast, seamless, systematic and controlled access to the information they need to perform their tasks, when and where they need it. Thanks to interoperability, this can be done without enlarging access rights or extending data retention periods. The interoperability framework also provides for a tool for police authorities in the territory of the Member States to identify persons whose data is recorded in the EU central information systems. It also provides a solution to detect multiple identities, with the dual purpose of ensuring the correct identification of bona fide persons and combating identity fraud. Additionally, involving Europol as the law enforcement agency and criminal information hub in the Prüm framework in order to perform searches on data received from third countries would bring added value for law enforcement purposes.

Regarding **overlaps**, only three stakeholders identified some, in reply to the public consultation, with other law enforcement information exchange tools/instruments at EU or international level while six stakeholders identified none. One stakeholder wrote that

[192] SWD(2017) 278 final.

[193] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

there is some overlap with the Interpol systems AFIS and SMV,[194] which are still used for international alerts by the police. However, the Prüm hit-no hit system is more advanced and the Interpol database contains only a limited number of persons and traces. There is also some overlap with the Europol Information System (EIS) and the Schengen Information System (SIS), but this pertains only to a limited set of data insofar as the information is shared with these central systems in line with their legal framework. The size and scope of these central systems does not compare to the size and scope of the national databases of all Member States because not all information from those databases is included in the EIS or in the SIS. As stated in the 2017 Comprehensive Assessment of EU Security Policy, "*while there are centralised databases that contain some elements of similar data to those existing in Prüm (e.g. fingerprints stored* [in the] *SIS, the EIS, or Interpol), they contain very limited amounts of data in comparison with that which is accessible under the Prüm Decisions*."[195]

Another stakeholder stressed that the Interpol data exchange and SIENA are overlapping in the EU. However, these are two channels used for the exchange of information, chosen by different Member States for reasons of their own. One result of Member States having a free choice of channel is that they use different channels to different extents.[196] In reply to a questionnaire circulated to Member States in the context of the preparation of the final report of the Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, three Member States reported using SIENA, ten Member States reported using Interpol and four Member States reported using both SIENA and Interpol.

Q9. What developments in the EU acquis have had an impact on the Prüm Decisions since 2008?

Considerable developments of the EU data protection framework have materialized since 2008, with the adoption of the General Data Protection Regulation ('GDPR') and of the Law Enforcement Directive ('LED') in 2016. As set out in the June 2020 Communication on the way forward on aligning the former third pillar acquis with the data protection rules, there is a need to ensure that a new Prüm legislation is fully aligned with the Law Enforcement Directive, especially as regards the data protection safeguards:

- Alignment of the data subject rights and rules regarding liability for personal data processing, and remedies;
- Ensure that the logging requirements are fully aligned with the LED;
- Align rules on transfer of personal data to a third country or international organisation;

[194] This database contains extensive identification details from all types of motor vehicles (cars, trucks, trailers, heavy machinery, motorbikes) and identifiable spare parts reported as stolen. See https://www.interpol.int/How-we-work/Databases/Our-18-databases.
[195] SWD(2017) 278 final.
[196] COM(2012) 735 final.

- Consider the interplay between the Article 9(3) LED and the system established by the Prüm Decisions.[197]

As mentioned in the reply to the previous question, Prüm comes into play in the context of law enforcement access to those systems for the purposes of preventing and fighting serious crime and terrorism (e.g. EES Regulation). Searches of national databases under the Prüm framework are preconditions for allowing searches of non-law enforcement systems for law enforcement purposes.

On 11 June 2019, the Interoperability Regulations[198] entered into force. The Regulations are designed to upgrade the EU information systems for security, border and migration management and make them work together in a smarter and more efficient way. The interoperability between EU information systems was established with a view to improve the effectiveness and efficiency of checks at the external borders, to contribute to the prevention of illegal immigration and to contribute to a high level of security within the area of freedom, security and justice of the Union. It also aims to improve the implementation of the common visa policy, to assist in the examination of applications for international protection, to contribute to the prevention, detection and investigation of terrorist offences and other serious criminal offences and to facilitate the identification of unknown persons. Interoperability between EU information systems was established in order for these systems and their data to supplement each other while respecting the fundamental rights of individuals, in particular the right to protection of personal data. Interoperability should also be explored in the context of the Prüm information exchange: what technical components can be used to address potential information gaps and provide for better access to end-users without enlarging access rights or extending data retention periods?

Currently, three EU central information systems are in operation: the Schengen Information System (SIS), the Visa Information System (VIS) and the Eurodac system. In addition, three other systems are currently in 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).

[197] COM(2020) 262 final.

[198] 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.

5.5. EU added value

To what extent have the Prüm Decisions brought EU added value compared to what could be achieved at either national or international level?

Main findings:

- The improvement of information exchange in the European Union cannot be sufficiently achieved by Member States in isolation, owing to the cross-border nature of crime fighting and security issues so that Member States have to rely on one another in these matters. Cross-border crime can only be tackled by effective cross-border police cooperation, especially by exchanging information.
- Common EU level rules, standards and requirements facilitate these exchanges, provide compatibility between different national systems, and help to ensure high-level security and data protection standards. Moreover, common standards enhance trust between Member States.
- There is no instrument at international level that can provide the same added value as the Prüm framework.

Q10. What is the added value resulting from the EU intervention compared to what could be achieved by Member State action only?

In reply to the public consultation, when asked to what extent has the Prüm framework provided added value compared to what Member States could achieve in the field of law enforcement information exchange in the absence of the Prüm framework, stakeholders either fully agreed or tended to agree, with several highlighting that law enforcement information exchange has been facilitated and has become faster. One stakeholder specified that in the light of technological progress, the increase and diversification of police cooperation, it is not appropriate to compare the number of exchanges on DNA and dactyloscopic data before the Prüm Treaty of 2005 and now. According to this same stakeholder, statistical data prior to 2005 are of little significance. DNA techniques have evolved considerably as well as the volume of analyses.

The improvement of information exchange in the European Union cannot be sufficiently achieved by Member States in isolation, owing to the cross-border nature of crime fighting and security issues. Hence, Member States have to rely on one another in these matters. Cross-border crime can only be tackled by effective cross-border police cooperation, especially by exchanging information. As mentioned in the EU Security Union Strategy, cooperation and information sharing are the most powerful means to combat crime and pursue justice.[199]

[199] COM(2020) 605 final (24.7.2020).

Member States also exchange information under national laws and bilateral/multilateral agreements. These different agreements imply the use of different standards. In the case of the Prüm Decisions, common EU level rules, standards and requirements facilitate these exchanges, provide compatibility between different national systems, and help to ensure high-level security and data protection standards. Moreover, common standards enhance trust between Member States. It follows therefore that the added value of the instrument lies in the harmonisation and standardisation provided. Additionally, as the experience with the current Prüm framework shows, common standards allow for a certain level of automation in information exchange workflows which release law enforcement officers from certain labour-intensive manual activities.

Q11. What is the added value resulting from the EU intervention compared to what could be achieved at international level?

Member States are all members of Interpol, through which information can be exchanged with countries across the world either through Interpol notices and databases (e.g. Stolen and Lost Travel Documents) or bilaterally using the Interpol communication channel I-24/7.[200]

Interpol collects some data from participating countries into Interpol databases whereas Prüm connects national databases. As examined under Q8, these are different instruments and there are mainly complementarities between the exchange of information under Prüm and under the Interpol systems. Basically, there is no instrument at international level that can provide the same added value as the Prüm framework. Moreover, working with an EU instrument also provides for strong guarantees regarding the respect of the EU data protection framework.

6. CONCLUSIONS AND LESSONS LEARNT

The overall objective of this evaluation was to evaluate the functioning of the automated exchange of data pursuant to the Prüm Decisions and the level of implementation and application in each EU Member State since the adoption of the instruments in 2008. The evaluation used the five evaluation criteria: relevance, effectiveness, efficiency, coherence and EU added value. In line with the "evaluate first" principle, this evaluation identifies areas where the instrument can be improved or updated in order to support the preparation of a new initiative to strengthen and modernize the automated exchange of data between law enforcement authorities for preventing and investigating criminal offences.

As described in Section 4, the evaluation of the Prüm Decisions and of the policy context has limitations in terms of a general lack of statistics and quantitative data at EU and Member States' level on the functioning of the Prüm Decisions. This is indeed one of the

[200] For more information, see https://www.interpol.int/How-we-work/Databases.

areas where the instrument could be improved in the future, as the current situation does not allow for the sufficient quantification of the effects (regarding the improvement of information exchange, the costs, the administrative burden, etc.) of the Prüm Decisions. Therefore, where quantitative data was not available, qualitative evidence was provided in the analysis. The evaluation concluded 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 Prüm Decisions meet the needs of criminal investigators, of victims of crime, of forensic specialists, of database custodians and of legal practitioners.

- 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 was 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, it was stressed that there is still an administrative burden with regards to hit verification and reporting, and also to receipt/transmission of second step information.

- Regarding data protection, even though specific data protection provisions were included in the Prüm Decisions, the data protection legal framework has considerably developed since 2008, requiring that any revision of the legal instrument ensures that all relevant safeguards are in place.

- 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.[201] There are mostly complementarities between the Prüm Decisions and other relevant EU/international legislation, including the interoperability framework.[202] There are also complementarities with some of the EU

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

[202] 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;

central information systems that have different purposes.[203] Potential synergies can be identified regarding Europol and the interoperability framework.

- Council Decision 2008/616/JHA contains detailed inclusion and matching rules, technical specifications of queries, security measures, communication etc. that have not been changed since the adoption of the Prüm Decisions. Some of these rules are outdated as forensic science and information technology have significantly developed since 2008.

- The Prüm Decisions have improved the exchange of data between the Member States to the extent that they partially automated the process, thereby making it faster and less burdensome for law enforcement authorities.

- However, the implementation of the Prüm Decisions has been slow. Indeed, nearly ten years after the implementation deadline on 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 may decrease the possibility that criminals are identified, and cross-border links between crimes are detected, hindering 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 hindering the functioning of the Prüm system. Indeed, due to differences in national rules and procedures, the exchange of hit follow-up data is very fragmented, to the extent that it sometimes takes weeks or even months to receive the relevant information behind a hit.

This evaluation demonstrated that the improvement of information exchange in the European Union cannot be sufficiently achieved by the Member States in isolation. Indeed, due to the cross-border nature of crime fighting and security issues, which can only be tackled by effective cross-border police cooperation, exchanging information at EU level is key. This evaluation also allowed to identify areas for further improving the information exchange. The Prüm Decisions provide added value to the extent that they introduce common EU level rules, standards and requirements facilitate these exchanges, provide compatibility between different national systems, and help to ensure high-level security and data protection standards.

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.

[203] Such as the Entry-Exit System (EES).

Annex 5: Evaluation criteria and questions

In accordance with the Commission's Better Regulation Guidelines, the evaluation's overall objective was to assess the relevance, effectiveness, efficiency, coherence and EU added value of the Prüm Decisions. In order to assess each of these criteria, a number of specific evaluation questions were developed on the basis of the definition of each of the Better Regulation's criteria and on the questions asked in the Public Consultation.

Relevance: *To what extent are the Prüm Decisions relevant in view of current and future needs/challenges?*

Q1. To what extent are the Prüm Decisions relevant in view of current and future needs/challenges related to security and more precisely criminal investigations?

Q2. To what extent do the Prüm Decisions correspond to the needs/interests of the stakeholders?

Q3. Are there any aspects of the Prüm Decisions that might be considered obsolete? (e.g. technical, security, forensic)

Effectiveness: *To what extent have the Prüm Decisions been effective in delivering the intended results?*

Q4. Have the Prüm Decisions improved the exchange of data between Member States? If so, how?

Q5. If not, what has prevented the effective implementation?

Q6. What are the main obstacles for smooth information exchange under the Prüm Decisions?

Efficiency: *To what extent have the Prüm Decisions achieved the intended results in the most efficient manner?*

Q7. To what extent has the automated data exchange under the Prüm Decisions brought any efficiency gains in the law enforcement information exchange?

Coherence: *To what extent are the Prüm Decisions coherent and complementary to other relevant interventions at EU and international level?*

Q8. Are there any overlaps/contradictions/complementarities/synergies/gaps between the Prüm Decisions and any other relevant EU/international legislation?

Q9. What developments in the EU acquis have had an impact on the Prüm Decisions since 2008?

EU added value: *To what extent have the Prüm Decisions brought EU added value compared to what could be achieved at either national or international level?*

Q10. What is the added value resulting from the EU intervention compared to what could be achieved by Member State action only?

Q11. What is the added value resulting from the EU intervention compared to what could be achieved at international level?

Annex 6: Public consultation questionnaire

Introduction

Serious and organised crime in Europe knows no borders. Fighting national and cross-border crime requires daily operational cooperation and information exchange between Member States' law enforcement authorities.

At EU level, the so-called Prüm Decisions (Council Decisions 2008/615/JHA and 2008/616/JHA of 23 June 2008) are one of the key instruments for supporting cooperation between law enforcement authorities to fight cross-border crime. Automated exchange of data under the Prüm framework allows national law enforcement authorities responsible for the prevention and investigation of criminal offences to search and compare DNA,[204] dactyloscopic[205] and certain vehicle registration data.[206] Member States give each other access to an extraction of their national DNA, dactyloscopic databases established for the purpose of criminal investigations, and to certain data from national vehicle registration databases. In the first step, an inquiring Member State searches and compares its data set against one or several Member States Prüm databases. In case of sufficient matches between two sets of data, "a hit" is reported back. The query and the reply includes only reference data that does not contain any data from which the data subject can be directly identified (e.g. name, date of birth, place of birth, etc). In case of DNA and dactyloscopic data, the hits are verified by forensic experts. If a sufficient match between two data sets in confirmed, a request to receive personal and case related data should be sent to the Member State where the hit occurred. This subsequent exchange of personal data is called step 2 and it takes place under national law. In case of vehicle registration data, the additional data is provided immediately upon "a hit".

Prüm automated exchange of data has allowed to solve many serious crimes in Europe. For example, Prüm framework can be used in a case when comparing a partial fingerprint example (so-called latent print) that was found on a crime scene against the national criminal fingerprint database brings no results, i.e. the suspect remains unidentified. Checking the same latent fingerprint data also against other Member State's criminal fingerprint databases could show that the same person had been convicted for a criminal offence in another Member State. As a result, after the exchange of additional data between the two Member States, the suspect can be identified and the criminal investigation can lead to the prosecution and conviction of a criminal.

---

[204] 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, i.e. the particular molecular structure at the various DNA locations (loci)

[205] Dactyloscopic data mean 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

[206] Query is launched based on chassis number or licence plate number. Data set returned is described in Chapter 3 of the Annex of Council Decision 2008/616/JHA.

The objective of this consultation is to gather stakeholders' feedback on the Prüm framework for automated data exchange. The consultation looks at the effectiveness, efficiency, relevance, coherence, and European added value of the Prüm framework. It also aims to collect information on the shortcomings of the existing Prüm framework and on the possible ways to address these.

Questionnaire

The existing Prüm framework for automated exchange of DNA, fingerprint and vehicle registration data

1. **In your view, how relevant is cooperation and the exchange of information between Member States' law enforcement authorities for the prevention and investigation of criminal offences?**

   ✓ Not at all

   ✓ To a small extent

   ✓ To some extent

   ✓ To a large extent

   ✓ Very relevant

   ✓ I do not know

Please explain in more detail.

2. **How relevant it is to be able to search and compare DNA, fingerprint and vehicle registration data (the Prüm framework) in other Member States' databases for the prevention and investigation of criminal and terrorist offences?**

	Not at all	To a small extent	To some extent	To a large extent	Very relevant	I do not know
DNA						
Dactyloscopic data						
Vehicle registration data						

Please explain in more detail.

3. To what extent does the Prüm framework correspond to the needs/interests of different stakeholders?

	Not at all	To a small extent	To some extent	To a large extent	Completely	I do not know
Victims of crime						
Criminal investigators						
Data protection authorities						
Forensic specialists						
Database custodians						
Legal practitioners						
Human Rights organisations						
Other (please describe below)						

Please explain in more detail. If you replied "other", please describe it here.

4. Please provide any examples or (statistical) data how, if any, Prüm automated data exchange has helped to fight crime and terrorism.

5. The purpose of the Prüm automated exchange of data is to step up cross-border cooperation, particularly the exchange of information between authorities responsible for the prevention and investigation of criminal offences. In your view, has the Prüm framework improved the exchange of data between Member States?

- ✓ No
- ✓ To some extent
- ✓ Yes
- ✓ I do not know

Please explain in more detail.

5.1 What factors have prevented the effective implementation of the automated data exchange under the Prüm framework? Multiple replies are possible.

- □ Technical reasons, e.g. compatibility with the requirements set in the Prüm Decisions;
- □ Legal aspects, e.g. need to adapt national legislation;
- □ Financial costs, e.g. setting up respective national databases, establishing bilateral connections with other Member States;
- □ Operational reasons, e.g. lack of efficient and effective work processes;
- □ Gaps or lack of clarity in the Prüm Decisions;
- □ Other (please describe below);
- □ I do not know

Please explain in more detail. If you replied "other", please describe it here.

5.2 How has the Prüm framework contributed to improving the exchange of data between Member States?

	I do not agree at all	I tend to disagree	I neither disagree nor agree	I tend to agree	I fully agree	I do not know
Harmonised rules allow more efficient data comparison between the police.						

Less administrative burden for the police, as a part of the data exchange process is automated.						
Faster access of the police to the relevant information						
Other (please describe below)						
I do not know						

Please explain in more detail. If you replied "other", please describe it here.

6. In your opinion, has the automated exchange of DNA, dactyloscopic and vehicle registration data resulted in any negative consequences?

- ✓ No
- ✓ To some extent
- ✓ Yes
- ✓ I do not know

6.1 What are the main negative consequences of the Prüm framework?

	I do not agree at all	I tend to disagree	I neither disagree nor agree	I tend to agree	I fully agree	I do not know
Undermining data security in national systems and when transferring data between national authorities						
Limiting of the right of data protection and privacy for the individual concerned (data subject)						
Limiting of other fundamental rights for the individual concerned (data subject)						
Other (please describe below)						

I do not know						

Please explain in more detail. If you replied “other”, please describe it here.

7. In your view, to what extent has the Prüm framework provided added value compared to what Member States could achieve in the field of law enforcement information exchange in the absence of the Prüm framework?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

8. Over the time, several EU and international initiatives aim at facilitating the exchange of information between law enforcement authorities, such as Europol information systems, Interpol information systems, Schengen Information System, Council Framework Decision 2006/960/JHA. To what extent do you agree/disagree that the Prüm framework complements other EU and international action in the area of law enforcement information exchange?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

9. Are you aware of any overlaps with other law enforcement information exchange tools/instruments at EU or international level?

- ✓ No
- ✓ Yes
- ✓ I do not know

Please explain in more detail.

10. Is there anything else you would like to comment on with relation to the current EU policy on automated cross-border exchange of data between law enforcement authorities?

11. In your view, to what extent has the automated data exchange under the Prüm framework brought any efficiency gains in the law enforcement information exchange?

	Not at all	To a small extent	To some extent	To a large extent	I do not know
Speed of exchanges					
Administrative burden					
Costs					
Staff					
Other (please describe below)					

Please explain in more detail. If you replied "other", please describe it here.

12. Please provide any examples or (statistical) data how, if any, Prüm automated data exchange improved the efficiency of law enforcement information exchange (for example the change in waiting time for the responses, change in the number of queries per official that the law enforcement authorities are capable of serving, change in the costs of respective information systems/ICT developments, etc)

13. In your view, have the costs (administrative, budgetary, in terms of personnel, etc.) related to the implementation of the Prüm framework been proportionate to its contribution in terms of the improvements in law enforcement information exchange?

	Not at all	To a small extent	To some extent	To a large extent	Completely	I do not know
DNA						
Dactyloscopic data						
Vehicle registration data						

14. Please explain in more detail why you deem the costs related to the implementation of the Prüm framework to be proportionate/disproportionate in relation to the efficiency gains.

Strengthening the automated data exchange under the Prüm framework

The following questions target the shortcomings identified by the Commission and the possibilities if and how to address these shortcomings.

15. The existing Prüm framework allows the exchange of DNA, fingerprint and vehicle registration data. There are other data in Member States' databases that are often the subject of cross-border information requests in criminal investigations. These are exchanged by sending manual queries to other law

enforcement authorities that require human resources and that can take time. To what extent do you agree/disagree that this is a shortcoming in the law enforcement information exchange?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

15.1What do you consider to be the most appropriate means to address this shortcoming?

- ✓ No changes are needed.
- ✓ Member States should address it in bilateral/multilateral agreements with other Member States
- ✓ EU should provide support and guidance to facilitate cooperation between Member States' law enforcement authorities.
- ✓ EU legislation should be established to standardise and automate the exchange of additional data categories.
- ✓ Other (please describe below)
- ✓ I do not know

Please explain in more detail why (not). If you replied "other", please describe it here.

15.2What data could be exchanged under the same principles as provided by the Prüm framework?

	No	Yes	I do not know
Limited extract of police records			

Driving licences			
Photos of suspects and convicted criminals			
Ballistics			
Other (please describe below)			

Please explain in more detail why (not). If you replied "other", please describe it here.

16 In your view, can the inclusion in Prüm framework of any data listed above entail risks (data security, data protection, other rights and freedoms)? Please describe any safeguards (procedural, technical, data protection, etc), if any, that you would consider necessary for this change in the Prüm framework.

17 In case of DNA and dactyloscopic queries, the exchange of personal data after a hit has been confirmed (step 2) is not governed by the Prüm Decisions, but by national law. Differences in administrative, legal, judicial systems lead to sometimes long waiting times and diverse practices in defining the data to be handed over. To what extent do you agree/disagree that this is a shortcoming of the existing Prüm framework?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

17.1What do you consider the most appropriate means to address this shortcoming?

- ✓ No changes are needed.
- ✓ Member States should address it individually in their national legislation/procedures
- ✓ EU should provide support and guidance to facilitate cooperation between Member States' law enforcement authorities.
- ✓ EU legislation should be established to streamline the hit follow-up exchange of personal and case related data.
- ✓ Other (please describe below)
- ✓ I do not know

Please explain in more detail why (not). If you replied "other", please describe it here.

17.2To what extent should the process be regulated at EU level?

	Yes	No	I do not know
Harmonising the deadlines to reply to a request			
Determine the law enforcement information exchange channel through which the request and the reply should be submitted			
Agree on a limited data set to be first provided in "fast track"			
Establish a designated "Prüm" IT application for submitting and receiving the requests			
Other (please describe below)			
I do not know			

Please explain in more detail. If you replied "other", please describe it here.

18 In your view, can the inclusion of any data listed above in the Prüm framework entail risks (data security, data protection, other rights and freedoms)? Please describe any safeguards (procedural, technical, data protection, etc), if any, that you would consider necessary for this change in the Prüm framework.

19 The existing Prüm framework is a decentralised network of bilateral connections between the national databases of Member States without any EU level central components. Not all Member States have established connections with all other Member States for various reasons. This could result in some queries not being checked against the data in some countries and may increase the possibility that some criminals are not identified, and some cross-border links between crimes are not detected. To what extent do you agree/disagree that this is a shortcoming of the existing Prüm framework?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

19.1Which of the following options would seem the most appropriate technical solution for Prüm?

- ✓ Network of bilateral connections between Member States' databases (maintaining the current solution)
- ✓ Establishing an EU central router for transferring messages between Member States (so-called hub and spoke model) with limited functions at central level such as technical/operational system monitoring, collection of statistics.
- ✓ Establishing an EU automated biometric identification system (ABIS) that would allow matching biometric templates by a centrally managed technical solution.
- ✓ Other (please describe below)
- ✓ I do not know

Please explain in more detail why (not). If you replied "other", please describe it here.

20 In your view, can the inclusion of any data listed above in the Prüm framework entail risks (data security, data protection, other rights and freedoms)? Please describe any safeguards (procedural, technical, data protection, etc), if any, that you would consider necessary for this change in the Prüm framework.

21 Europol is the EU Agency for Law Enforcement Cooperation. Europol is not part of the Prüm framework, however Europol databases contain relevant data from 3rd countries about serious criminals and terrorists. This data is currently not compared against Member States criminal databases in a structured manner. To what extent do you agree/disagree that this is a shortcoming of the existing Prüm framework?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

22 Which of the following options would seem the most appropriate participation of Europol in the Prüm framework?

- ✓ No changes are needed.
- ✓ Europol could improve the availability of relevant data through existing Europol information systems.
- ✓ EU legislation should be established to allow Europol to exchange data in the Prüm framework.
- ✓ Other (please describe below)
- ✓ I do not know

Please explain in more detail why (not). If you replied "other", please describe it here.

23 In your view, can the inclusion of any data listed above in the Prüm framework entail risks (data security, data protection, other rights and freedoms)? Please describe any safeguards (procedural, technical, data protection, etc), if any, that you would consider necessary for this change in the Prüm framework.

24 In several Member States Prüm biometric data exchanges cannot be used for searching missing people and unidentified human remains as this is not a criminal investigation according to national legislation. To what extent do you agree/disagree that this is a shortcoming?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

The experts have proposed a number of possible changes in the existing vehicle registration data queries.

25 In order to further improve the criminal investigations, especially regarding stolen vehicles, it might be useful to have additional data provided in the reply to a query on vehicle registration data, such as mileage or vehicle colour. To what extent you agree/disagree that this new data should be added in the reply to a query on vehicle registration data?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree

- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

26 In criminal investigations it might be useful to have knowledge of all vehicles registered in the name of a certain natural person or legal entity. To what extent you agree/disagree that this query should be allowed under Prüm framework as a follow-up request to the existing query on vehicle registration data?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

27 In criminal investigation, it might be useful to know if any other Member State has previously made queries regarding the same vehicle. To what extent you agree/disagree that this information could be flagged in the reply to a query concerning vehicle registration data?

- ✓ I do not agree at all
- ✓ I tend to disagree
- ✓ I neither disagree nor agree
- ✓ I tend to agree
- ✓ I fully agree
- ✓ I do not know

Please explain in more detail.

28 In your view, can any of these options listed above regarding the improvements in vehicle registration data queries entail risks (data security, data protection, other rights and freedoms)? Please describe any safeguards (procedural, technical, data protection, etc), if any, that you would consider necessary for this change in the Prüm framework.

29 Are there any other shortcomings in the current Prüm framework that should be addressed? If yes, how would you suggest addressing these?

30 In your view, are there any aspects of the existing Prüm automated exchange of data that should not be changed?

31 Do you have any other comments that you wish to make on the Prüm automated exchange of data?

If you wish, you may upload a concise document, such as position paper. This is an optional complement to your responses to this questionnaire and will serve as additional background reading to better understand your position. If you prefer, you may email this to HOME-PRUM@ec.europa.eu.

Your experience with the Prüm framework

32 How would you rate your knowledge and understanding of EU policies in the area of cross-border exchange of data between law enforcement authorities?

- ✓ Very good
- ✓ Good
- ✓ Limited

- ✓ very limited
- ✓ none
- ✓ I do not know

33 How would you rate your knowledge and understanding of the legal framework and the functioning of the Prüm automated exchange of DNA, dactyloscopic and vehicle registration data?

- ✓ Very good
- ✓ Good
- ✓ Limited
- ✓ very limited
- ✓ none
- ✓ I do not know

34 Have you used Prüm automated data exchange in your work since its establishment in 2008?

	never	in very rare occasions (one to four times per year)	regularly (on a monthly basis)	frequently (on a weekly basis)
as a criminal investigator				
as a forensic expert				
as an officer responsible for the international police cooperation				
As a judicial authority				

Annex 7: Overview of EU information systems

As mentioned in the introduction of the impact assessment, the landscape of the large-scale EU information systems has developed substantially in recent years. This includes the revision of the three EU central information systems that are in operation: the Schengen Information System (SIS),[207] the Visa Information System (VIS)[208] and the Eurodac system.[209]

The **SIS** is the most widely used and largest information sharing system for security and border management in Europe. It assists competent authorities in Europe to preserve internal security in the absence of internal border checks through three different areas of cooperation:

- Border control cooperation: SIS enables border guards, as well as visa issuing and migration authorities, to enter and consult alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area.
- Law enforcement cooperation: SIS supports police and judicial cooperation by allowing competent authorities to create and consult alerts on missing persons and on persons or objects related to criminal offences.
- Cooperation on vehicle registration: Vehicle registration services may consult SIS in order to check the legal status of the vehicles presented to them for registration. They only have access to SIS alerts on vehicles, registration certificates and number plates.

SIS enables competent national authorities, such as the police and border guards, to enter and consult alerts on persons or objects. A SIS alert does not only contain information about a particular person or object but also instructions for the authorities on what to do when the person or object has been found. The specialised national SIRENE Bureaus located in each Member State serve as single points of contact for the exchange of supplementary information and coordination of activities related to SIS alerts.

The **VIS** allows Schengen States to exchange visa data. It consists of a central IT system and of a communication infrastructure that links this central system to national systems. VIS connects consulates in non-EU countries and all external border crossing points of Schengen States. It processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. The purposes of VIS are the following:

[207] Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862. For more information, see https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/schengen-information-system_en.
[208] Regulation (EC) No 767/2008. For more information, see https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-information-system_en.
[209] Regulation (EU) No 603/2013.

- Facilitating checks and the issuance of visas: VIS enables border guards to verify that a person presenting a visa is its rightful holder and to identify persons found on the Schengen territory with no or fraudulent documents. Using biometric data to confirm a visa holder's identity allows for faster, more accurate and more secure checks. The system also facilitates the visa issuance process, particularly for frequent travellers.
- Fighting abuses: While the very large majority of visa holders follow the rules, abuses can also take place. For instance, VIS will help in fighting and preventing fraudulent behaviours, such as "visa shopping" (i.e. the practice of making further visa applications to other EU States when a first application has been rejected).
- Protecting travellers: Biometric technology enables the detection of travellers using another person's travel documents and protects travellers from identity theft.
- Helping with asylum applications: VIS makes it easier to determine which EU State is responsible for examining an asylum application and to examine such applications.
- Enhancing security: VIS assists in preventing, detecting and investigating terrorist offences and other serious criminal offences.

The **Eurodac** system establishes an EU asylum 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.

In addition, three new systems are currently in development phase: the Entry/Exit System (EES),[210] the European Travel Information and Authorisation System (ETIAS)[211] and the centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN system).[212]

The **EES** and **ETIAS** will strengthen security checks on visa-free travellers by enabling advance irregular migration and security vetting.

The **EES** will be an automated IT system for registering travellers from third-countries, both short-stay visa holders and visa exempt travellers, each time they cross an EU external border. The system will register the person's name, type of the travel document, biometric data (fingerprints and captured facial images) and the date and place of entry and exit, in full respect of fundamental rights and data protection.

It will also record refusals of entry. EES will replace the current system of manual stamping of passports, which is time consuming, does not provide reliable data on border crossings and does not allow a systematic detection of over-stayers (travellers who have exceeded the maximum duration of their authorised stay).

[210] Regulation (EU) 2017/2226. For more information, see https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en.
[211] Regulation (EU) 2018/1240.
[212] Regulation (EU) 2019/816. For more information, see https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/european-travel-information-authorisation-system_en.

EES will contribute to prevent irregular migration and help protect the security of European citizens. The new system will also help bona fide third-country nationals to travel more easily while also identifying more efficiently over-stayers as well as cases of document and identity fraud. In addition to this, the system will enable to make a wider use of automated border control checks and self-service systems, which are quicker and more comfortable for the traveller.

ETIAS will be a largely automated IT system created to identify security, irregular migration or high epidemic risks posed by visa-exempt visitors travelling to the Schengen States, whilst at the same time facilitate crossing borders for the vast majority of travellers who do not pose such risks. Non-EU nationals who do not need a visa to travel to the Schengen area will have to apply for a travel authorisation through the ETIAS system prior to their trip. The information gathered via ETIAS will allow, in full respect of fundamental rights and data protection principles, for advance verification of potential security, irregular migration of high epidemic risks.

After filling in an online application form, the system will conduct checks against EU information systems for borders and security and, in the vast majority of cases, issue a travel authorisation within minutes. In limited cases, where further checks on the traveller are needed, the issuing of the travel authorisation could take up to 30 days. The ETIAS travel authorisation will be a mandatory pre-condition for entry to the Schengen States. It will be checked together with the travel documents by the border guards when crossing the EU border. This prior verification of visa exempt non-EU citizens will facilitate border checks; avoid bureaucracy and delays for travellers when presenting themselves at the borders; ensure a coordinated and harmonised risk assessment of third-country nationals; and substantially reduce the number of refusals of entry at border crossing points.

Thanks to ETIAS authorities will receive vital information necessary to assess potential risks with individuals travelling to the EU and, if required, a travel authorisation could be denied. Schengen participating States will be able to manage their external borders more effectively and improve internal security. Travellers will have early indication of their admissibility to the Schengen States, making legal travel across Schengen borders easier.

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) is responsible for developing the system. ETIAS is expected to be operational by the end of 2022. The ETIAS Regulation provides for transitional measures to ensure a smooth roll out of the system.

The **ECRIS-TCN** system will address the identified gap in the exchange of information between Member States on convicted non-EU nationals.

All these above-mentioned, current and future, systems are linked through the **interoperability framework for the EU information systems**[213] for security, border and migration management, adopted in 2019, and which is currently being put in place.

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