EUROPEAN
COMMISSION

Brussels, 8.12.2021
SWD(2021) 379 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE 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) 378 final}

Executive Summary Sheet

Impact assessment on a proposal to strengthen the automated data exchange under the Prüm framework (revision of Council Decisions 2008/615/JHA and 2008/616/JHA).

A. Need for action

Why? What is the problem being addressed?

Criminality across Europe undermines EU citizens' security and well-being. 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 2020 EU Security Union Strategy.[1] 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 fighting crime and enhancing security.** Member States must rely on one another in these matters.

Law enforcement authorities in the EU cooperate and exchange information, notably through the framework set by the Prüm Decisions (Council Decisions 2008/615/JHA and 2008/616/JHA) for the exchange of data on DNA profiles, fingerprints and vehicle registration, but there are important shortcomings.

There are **four main issues** hampering law enforcement authorities in fighting crime through this framework, which all bear on the search and supply of information between law enforcement authorities in the EU:

1) 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;**
2) 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;
3) 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;
4) 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.

These four interrelated main issues constitute problems due to their impact on the effective fight against crime and on EU citizens' security and well-being. They raise **important policy choices** that require a detailed assessment of the problem drivers, the related objectives, available policy options and their impacts.

What is this initiative expected to achieve?

In response to pressing operational needs, and calls from the Council to consider revising the Prüm Decisions (Council Decisions 2008/615/JHA and 2008/616/JHA) with a view to broadening their scope and to updating the necessary technical and legal requirements, this initiative is expected to strenghthen the automated data exchange under the Prüm framework to help Member States' law enforcement authorities fighting crime. The

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

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.

Responding to the four major problems identified, the initiative seeks to achieve the following **objectives**:

1) Objective I: Providing a technical solution for **efficient** automated exchange of data between EU law enforcement authorities to make them **aware of relevant data** that is available in the national database of another Member State;
2) Objective II: Ensuring 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;
3) Objective III: Ensuring that **relevant data** (in terms of sources of data) from **Europol**'s database is available to law enforcement authorities;
4) Objective IV: Providing law enforcement authorities with **efficient access to the actual data** corresponding to a 'hit' that is available in the national database of another Member State or at Europol.

What is the value added of action at the EU level?

The improvement of information exchange in the European Union cannot be sufficiently achieved by the Member States in isolation, owing to the cross-border nature of crime fighting and security issues. Member States are obliged to rely on one another in these matters. Common EU level rules, standards and requirements **facilitate these information exchanges** while providing **compatibility** between different national systems. This in turn allows for a certain level of automation in information exchange workflows that release law enforcement officers from labour-intensive manual activities. Last but not least, information exchange at EU level also allows ensuring high-level **data security** and **data protection** standards.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

A number of legislative policy options have been considered. Following a pre-selection some options were quickly discarded. The other **policy options have been assessed in full detail**:

1) Policy option addressing **objective I:** *('providing a technical solution for **efficient automated exchange of data')***
    - policy option 1.1: applying a hybrid solution between a decentralised and a centralised approach without data storage at central level

2) Policy options addressing **objective II**: *('ensuring that more relevant data (in terms of **data categories**) is available to law enforcement authorities')*
    - policy option 2.1: introducing the exchange of facial images in the Prüm framework
    - policy option 2.2: introducing the exchange of police records data in the Prüm framework
    - policy option 2.3: introducing the exchange of driving licence data in the Prüm framework

3) Policy options addressing **objective III:** *('ensuring that relevant data from Europol's database is **available** to law enforcement authorities')*
    - policy option 3.1: enabling Member States to check automatically third-country sourced data at Europol as part of the Prüm framework
    - policy option 3.2: enabling Europol to check third-country sourced data against the national databases of Member States

4) Policy options addressing **objective IV**: (*providing for efficient **access to the actual data** corresponding to a 'hit' that is available in the national database of another Member State or at Europol*).
    - policy option 4.1: regulating the follow-up process at EU level with a semi-automated exchange of actual data corresponding to a 'hit'

Following a detailed assessment of the impacts of the main policy options, the **package of preferred policy options** consists of policy option 1.1, policy option 2.1 and 2.2, policy option 3.1 and 3.2 and policy option 4.1.

Who supports which option?

Stakeholders are generally supportive of the strengthening of the automated data exchange under the Prüm framework.

Member States have supported the preferred policy options explicitly in various Council fora as well as in Council conclusions ('*2018 Council Conclusions on the implementation of the "PRÜM DECISIONS" ten years after their adoption*'). At the same time, Member States are conscious of the importance of their national sovereignty in the area of law enforcement from an operational and procedural perspective.

The European Parliament is expected to verify that there is a justification for the necessity of the inclusion of any new data category in the Prüm framework, as well as the existence of strong data protection safeguards. Indeed, discussions with all stakeholders showed the importance of providing for appropriate safeguards to ensure the respect of Fundamental Rights, and in particular the right to the protection of personal data.

C. Impacts of the preferred option

What are the benefits of the preferred options (if any, otherwise main ones)?

The package of preferred policy options (policy option 1.1, policy option 2.1 and 2.2, policy option 3.1 and 3.2 and policy option 4.1.) would respond effectively to the identified problems and reinforce the current Prüm framework with **targeted and strong additional capabilities** to step up its support to Member States in reinforcing information exchange with the final objective of **preventing and investigating criminal and terrorist offences**, in full **compliance with fundamental rights**.

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

What are the costs of the preferred options (if any, otherwise main ones)?

The preferred policy options require investements at both EU and Member States' level. The sum of the investment costs at national level is 4.4 million EUR as one-off costs and 882 000 EUR in a yearly basis. At EU level, the sum of the investment costs is 17.17 million EUR as one-off costs and 4.1 million in a yearly basis. To note that these amounts are estimates, based on previous experiences with the development and implementation of IT infrastructures at the EU level. Some of the policy options are however difficult to quantify in precise terms. It is expected that the projected investments costs will be outweighed by benefits and savings, notably at the Member States' level. The creation of the central Prüm router will save costs for Member States as they would not require to create as many connections as there are Member States and data categories.

The preferred policy options are not expected to have an impact on small and medium-sized enterprises. The preferred options do not contain regulatory obligations for citizens/ consumers, and therefore do not create additional costs for these stakeholders neither.

How will businesses, SMEs and micro-enterprises be affected?

The preferred policy options are not expected to have any significant impact on businesses.

Will there be significant impacts on national budgets and administrations?

As mentioned above, the sum of the expected investment costs at national level is 4.4 million EUR as one-off costs and 882 000 EUR in a yearly basis, which will be compensated by budget savings obtained from the use of the central router instead of as many national connections for each Member State as there are Member States

and categories of data. The estimations indicate that the accumulated budget savings at national level could compensate the initial investment both at central and national level in a period of 2 years.

Will there be other significant impacts?

All preferred policy options relate to the processing of personal data. Consequently, these policy options have an impact on Fundamental Rights and in particular on the rights to the protection of personal data (Article 8 of the Charter) and to respect for private life (Article 7 of the Charter). To ensure full compliance with Fundamental Rights, the impact assessment provides for a **thorough consideration of Fundamental Rights** throughout its analysis. As a result, the preferred policy options all meet an **objective of general interest** and are **strictly limited to what is necessary and proportionate** to achieve such objective.

D. Follow up

When will the policy be reviewed?

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.