Contribution ID: bb827149-6587-4c1d-94a7-88d91b0c767f
Date: 24/03/2021 10:40:38

Public consultation on strengthening the automated data exchange under the Prüm framework

Fields marked with * are mandatory.

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[1], dactyloscopic[2] and certain vehicle registration data[3]. 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 compares its data set against one or several Member States' Prüm databases. In case of a sufficient match 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. no name, date of birth, etc). In case of DNA and dactyloscopic data, if a sufficient match between two data sets in confirmed by a forensic expert, 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) 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.

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.

[1] 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)
[2] 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
[3] 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.

About you

* Language of my contribution

- ○ Bulgarian
- ○ Croatian
- ○ Czech
- ○ Danish
- ○ Dutch
- ◉ English
- ○ Estonian
- ○ Finnish
- ○ French
- ○ German
- ○ Greek
- ○ Hungarian
- ○ Irish
- ○ Italian
- ○ Latvian
- ○ Lithuanian
- ○ Maltese
- ○ Polish
- ○ Portuguese
- ○ Romanian
- ○ Slovak
- ○ Slovenian
- ○ Spanish
- ○ Swedish

* I am giving my contribution as

- ( ) Academic/research institution
- ( ) Business association
- ( ) Company/business organisation
- ( ) Consumer organisation
- ( ) EU citizen
- ( ) Environmental organisation
- ( ) Non-EU citizen
- (•) Non-governmental organisation (NGO)
- ( ) Public authority
- ( ) Trade union
- ( ) Other

* First name

Chloé

* Surname

Berthélémy

* Email (this won't be published)

chloe.berthelemy@edri.org

* Organisation name

255 character(s) maximum

European Digital Rights

* Organisation size

- ( ) Micro (1 to 9 employees)
- (•) Small (10 to 49 employees)
- ( ) Medium (50 to 249 employees)
- ( ) Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

16311905144-06

* Country of origin

Please add your country of origin, or that of your organisation.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
-
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South

	French Southern and Antarctic Lands		Sandwich Islands
Barbados	Gabon	Monaco	South Korea
Belarus	Georgia	Mongolia	South Sudan
Belgium	Germany	Montenegro	Spain
Belize	Ghana	Montserrat	Sri Lanka
Benin	Gibraltar	Morocco	Sudan
Bermuda	Greece	Mozambique	Suriname
Bhutan	Greenland	Myanmar /Burma	Svalbard and Jan Mayen
Bolivia	Grenada	Namibia	Sweden
Bonaire Saint Eustatius and Saba	Guadeloupe	Nauru	Switzerland
Bosnia and Herzegovina	Guam	Nepal	Syria
Botswana	Guatemala	Netherlands	Taiwan
Bouvet Island	Guernsey	New Caledonia	Tajikistan
Brazil	Guinea	New Zealand	Tanzania
British Indian Ocean Territory	Guinea-Bissau	Nicaragua	Thailand
British Virgin Islands	Guyana	Niger	The Gambia
Brunei	Haiti	Nigeria	Timor-Leste
Bulgaria	Heard Island and McDonald Islands	Niue	Togo
Burkina Faso	Honduras	Norfolk Island	Tokelau
Burundi	Hong Kong	Northern Mariana Islands	Tonga
Cambodia	Hungary	North Korea	Trinidad and Tobago
Cameroon	Iceland	North Macedonia	Tunisia

- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d’Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

Democratic Republic of the Congo

Saint Kitts and Nevis

Denmark

Liberia

Saint Lucia

* Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only your contribution, country of origin and the respondent type profile that you selected will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

Public

Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

I agree with the personal data protection provisions

The existing Prüm framework for the automated exchange of DNA, dactyloscopic 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.

When arguing for the expansion of an instrument like Prüm, that can lead to severe fundamental rights restrictions, it is entirely insufficient to rely on arguments that police officers find Prüm "useful" or "relevant". Yet, what we often receive is the reporting of anecdotal evidence brought by investigators.

The European Commission peremptorily assures that the Prüm framework "has helped to solve many crimes in Europe". However, there is a crucial lack of publicly available and accurate data about the impact of Prüm. In absence of such statistical analysis, it is therefore impossible whether expansion would be necessary

considering the vast restrictions possible on fundamental rights. In particular, the number of cross-border requests or hits provided by Member States does not prove the value of the instrument. Having X number of hits does not mean having X number of crimes solved. What would be useful to know is how many of these hits led to convictions. The few studies which attempted to collect that information actually found that less than 10% of hits were used in criminal proceedings and as evidence in courts of law. In this context, it is impossible to know whether Prüm is in line with the principle of necessity and proportionality as required by the EU Charter of Fundamental Rights. It might be important to recall that Prüm implies regular exchanges of potentially sensitive and private information. It is therefore very important that the benefits of the system to society and to the criminal justice systems are clarified as soon as possible.

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.

Information exchange between law enforcement authorities in EU Member States can have tremendously negative effects on the fundamental rights (notably but not restricted to data protection rights) of the individuals whose personal data is transferred to authorities in other Member States. This is why data protection authorities and human rights organisations alike have interest in monitoring the implementation of and scrutinising reforms of legislative frameworks that enable information exchange between law enforcement authorities. Their aim is to ensure those frameworks are adequately regulated with strong safeguards for people concerned, includes redress mechanisms and ensures transparency of the practices.

Currently, the Prüm framework does not meet the needs and demands of victims (whose data might be held in national DNA analysis files to which other Member States have access via Prüm), data protection authorities (see question 6.1) and human rights organisations.

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.

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. It may have reduced barriers in sharing data but compared to an approach which requires a specific warrant and reasonable suspicion, Prüm has instead further undermined due process and defense rights. It makes it easier to infringe in people’s rights without sufficient safeguards and checks and balances. We recall that even if Prüm only functions with the exchange of proxy data (hit/no hit), the data exchanged still relates to individuals and therefore amounts to personal data. Furthermore, there have been cases where Prüm hits led to the unjustified arrest or police suspicion and scrutiny of people until they were proven innocent.

5.1 What factors have prevented the effective implementation of the automated data exchange under the Prüm framework? Multiple replies are possible.

- [x] Technical reasons, e.g. compatibility with the requirements set in the Prüm Decisions;
- [x] Legal aspects, e.g. need to adapt national legislation;
- [x] Financial costs, e.g. setting up respective national databases, establishing bilateral connections with other Member States;
- [x] 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.

The Prüm Decisions adopted in 2008 have still not been fully implemented by Member States, despite the August 2011 implementation deadline. For the biometric data exchange (DNA and dactyloscopic data), only about 60% of the possible connections between Member States have been established. For the presumably simpler case of exchange of vehicle registration data, only 79% of the possible connections are operational. In itself, the extremely delayed implementation for the existing data categories makes it premature to consider extending the automated information exchange in the Prüm framework with additional data categories.

To Question "5.2 How has the Prüm framework contributed to improving the exchange of data between Member States?", we would have chosen I do not know for all the proposed statements because of the lack of publicly available data (see Question 1).

6. In your view, 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.

The European Commission’s Inception Impact Assessment argued that the “system provides a reply including no personal data, but only reference data” and later, that “the reference data does not contain any data from which the data subject can be directly identified”. This is a very dangerous misconception of how Prüm’s hits can be used in practice by law enforcement officers. When running a search across multiple databases, law enforcement officers still process data that relates to a certain individual – even if non-identifiable. Therefore it involves personal data even at this stage of the process.

Even though the automated search in Prüm only returns reference data in case of a hit, the search nonetheless involves processing of personal data in both the requesting and the requested Member State. The automated response can form the basis for intrusive measures taken against an individual in the requesting Member States, for example detention in case of a hit. A 2018 study from the European Parliament LIBE Committee showed that because some jurisdictions request, report and/or submit personal information without proper follow-up forensic and tactical work, cases were found where citizens have been arrested or undergone police suspicion and scrutiny until proven innocent. (Dr. Victor TOOM, Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision, LIBE Committee Study. The presumption of innocence, data protection principles and the respect for due process can therefore easily be undermined by this system. This data protection concerns do not seem to be addressed or foreseen in the upcoming evaluation.

This makes it absolutely critical that the personal data being processed is accurate and that there are procedural safeguards for individuals when personal data is exchanged between Member States. Whereas the Prüm framework has specific provisions on which national databases are to be made available for automated searches by other Member States, as well as the technical implementation of the automated searches, there are only very general data protection provisions in Chapter 6 of Council Decision 2008/615 /JHA.

Member States’ national law determine the criteria for inclusion in biometric (DNA and dactyloscopic) databases, the retention of personal data in biometrics databases (for suspects and convicted offenders, respectively), and the rules for searching biometric databases. The lack of proper EU-wide standards for data accuracy of biometric databases and searches becomes very problematic when national databases are made available for searches by other Member States. For example, the Prüm Decisions allow DNA matches based on six loci , which creates an unacceptable high risk of false-positive matches, especially when the search is made in a large DNA database.

Another important issue linked to the fact that the rules remain under the sole discretion of Member States is the way structural discrimination can guide national law enforcement authorities’ decisions on inclusion, retention and searches. The composition of national databases reflects the biases of law enforcement agencies and as a result, mirrors the systematic stigmatization against certain categories of people, notably racial and ethnic minority communities, migrants and other marginalised groups whose data is held in these

databases (see https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf). The rules therefore may impact the right to non-discrimination. Through digitized and networked national databases, these people undergo even more surveillance and have even more possibilities to be subject to coercive actions and abusive policing. Yet, not all national databases in the EU benefit from regulatory scrutiny.

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?

Since the adoption of the Prüm Decisions, the EU has modernised and harmonised the data protection framework for law enforcement with the Law Enforcement Directive (EU) 2016/680. One of the novelties in the Law Enforcement Directive (LED) is that biometric data for the purpose of unique identification of an individual constitutes sensitive personal data (Article 10). Such processing is only allowed where it is strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject.

The new requirements in the LED of strict necessity and appropriate safeguards should affect how Member States manage their biometric databases in terms of inclusion, data retention and searches. In practice, this depends on how Member States have transposed the LED into their national data protection law and made the necessary amendments to criminal procedure laws, police laws and specialised laws governing biometric databases. EDRi is not aware of any systematic studies, by the European Commission or other organisations, of Member States' LED transpositions in relation to biometric data and other aspects of direct relevance to the Prüm framework.

As Member States national law forms a critical part of the current Prüm framework, EDRi strongly recommends that the European Commission conducts a thorough assessment of all Member States' transpositions of the LED in connection with the upcoming evaluation of the Prüm framework. The impact of the Prüm framework on data protection and other fundamental rights of European citizens depends on the interplay between the data-exchange provisions in the Prüm Decisions and Member States' national law, in particular the data protection safeguards provided by the latter.

Since the United Kingdom remains part of the Prüm framework post-Brexit, an assessment of the level of data protection requirements provided for in the EU-UK draft adequacy decision should be carried out in connection with the foreseen evolution of Prüm.

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.

The Prüm Decisions have not been aligned with the modernised EU data protection regime in the LED. This alignment could potentially affect the existing information exchange in the Prüm framework, especially for DNA and dactyloscopic data which involve processing sensitive personal data under the LED with new requirements of strict necessity and appropriate safeguards for the rights and freedoms of the data subject.

EDRi recommends to continue with the current data categories while aligning the Prüm framework with the modernised data protection rules for law enforcement and the legislative process of the Lisbon Treaty with democratic scrutiny by the European Parliament. Additional data categories, especially those involving biometrics such as facial images (and thus facial recognition for automated search), should not be considered until the updated Prüm framework have been evaluated (after full implementation by all Member States). Even then, we do not believe that the inclusion of facial images meets the required threshold of necessity, given that their processing can lead to significant and widespread fundamental rights impacts, such as upon the right to dignity and the creation of mass surveillance infrastructures (https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf). The burden must be on the Commission to demonstrate why facial images are necessary and proportionate despite DNA and dactyloscopic data already providing for cross-border biometric identification. The next evaluation of the Prüm framework should include a thorough analysis of the data protection implications, a matter which has received very little attention in the previous evaluation by the Commission.

EDRi is strongly opposed to extending the Prüm framework with facial images in Member States' criminal investigation databases. Although this information is already available in some Member States' databases, the extension with facial images will have severe consequences. Automated searches in the Prüm framework of facial images with a hit/no-hit response can only be done with facial recognition technology, which is currently not in wide-spread use by law enforcement authorities in the EU. Addding facial images to the Prüm framework would effectively make it mandatory for all Member States to implement facial recognition technology in law enforcement in order to comply with the Prüm information exchange requirements.

Indeed, the DAPIX focus group on face recognition suggested that facial images fed to the database could

not only come from the national reference image databases for law enforcement but also public surveillance cameras. This is a clear example of function creep which is contrary to the purpose limitation principle. It risks encouraging the deployment of facial recognition technologies for mass surveillance in public spaces everywhere in the EU, which is likely to have a severe 'chilling effect' on people's ability to enjoy their rights and freedoms. Given the current lack of legal accountability and democratic vacuum in which biometric surveillance deployments are occurring across Europe, new obligations under the Prüm regime would contribute to growing unlawful mass surveillance and other fundamental rights abuses.

Moreover, facial recognition is a highly controversial technology which currently suffers from severe problems with accuracy and risks of discrimination against ethnic minorities, as mentioned above in our general remarks about facial recognition. The Commission's 2020 study on the feasibility of improving the information exchange under the Prüm Decisions presents certain test results for facial recognition technology with "good accuracy", even for the presumably typical case where the search in facial image databases is based on a low-quality image of a possible suspect captured by surveillance cameras. However, the practical experience with facial recognition by law enforcement authorities in the United States and the United Kingdom are very different from the simulated accuracy tests presented in the Commission study.

Furthermore, given the aforementioned discriminatory societal structures within which such technologies are developed, deployed, and used, even increasing the accuracy of facial recognition software will not solve the problem of its disproportionate use against already marginalised and over-policed communities. It is important for the European Commisison to acknowledge and be aware that law enforcement data embeds discriminatory policing practices and therefore expansion of them via the application of new technologies will only further this harm.

16. 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.

Facial recognition is a very intrusive and privacy-invasive form of biometric identification, in particular for the way in which it can be conducted without the subject's consent or knowledge. As cameras in public spaces, along with pictures posted on social media, have become ubiquitous, facial recognition creates an imminent risk of mass surveillance. Besides the issue of mass surveillance, facial recognition technology in its current state has significantly higher error rates for racialised minority groups. These groups are already subject to higher scrutiny in policing and risk of discrimination to the extent of the Fundamental Rights Agency (FRA) (https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf) having to produce guidelines against unlawful profiling. Introducing facial recognition technology with its greater risk of false-positive identification for minority ethnic groups can only serve to exacerbate the already serious problems of discrimination affecting these communities and potential uses against activists, human rights defenders and trade unions. However, whilst these high error rates demonstrate the discrimination that would arise if facial images were introduced in the short term, even increasingly accurate facial recognition software would only serve to more accurately target marginalised groups that are already over policed, such as activists, racialised communities, journalists and trade unionists.

In Europe and the United States, there is an ongoing substantial public discussion about the controversies of facial recognition technologies. There, we find calls for banning the technology, as some cities in the United States have done, or at least imposing a moratorium on its use. The European Data Protection Supervisor (EDPS) also publicly voiced his support for a moratorium on the deployment of biometric surveillance

technologies in the EU, “so that an informed and democratic debate can take place” (https://edps.europa.eu/sites/edp/files/publication/20-10-07_edps_biometrics_speech_en.pdf). In the White Paper on Artificial Intelligence (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN), the European Commission recognised the dangers of facial recognition for fundamental rights, and emphasised the requirements of strict necessity as well as appropriate safeguards in the LED for using facial recognition. The European Commission also highlighted the importance of a broad European debate on the circumstances, if any, which might justify the use of facial recognition. EDRi’s legal analysis has already demonstrated that uses of facial recognition that unduly restrict fundamental rights can never be necessary or proportionate.

When the Prüm Decisions were adopted in 2008, not all Member States had forensic DNA databases. The Prüm framework obliged the remaining Member States to build DNA databases, irrespective of their own assessment of the necessity and proportionality of DNA databases (or their prioritisation of financial resources allocated to policing). Currently, several Member States do not use facial recognition technology for law enforcement, but they would be forced to introduce this controversial technology if the Prüm framework were to be extended with facial images. Effectively, the Prüm framework would become the driver for pushing facial recognition technology to Member States without a meaningful democratic debate at the national level as Member States are required to implement EU law. The public consultations on the Prüm framework, unknown to most European citizens, can hardly qualify for a broad European debate, as outlined in the White Paper on AI.

EDRi urges the European Commission to refrain from imposing facial recognition through the Prüm framework. Introduction of facial recognition in law enforcement through EU-level initiatives requires a wider public debate for which the Prüm framework is ill-suited. Although the envisaged use of facial recognition technology in the Prüm framework poses somewhat different risks to live facial recognition in public or publicly-accessible spaces, there are still substantial risks for fundamental rights, in particular the clear risk of illegal discrimination based on ethnicity. Facial recognition technology could also lead to a greater interest by law enforcement in using recordings from surveillance cameras in criminal investigations since video images can be analysed automatically for possible matches against police databases of facial images. If this type of investigation is done systematically, the level of intrusiveness could potentially approach that of live facial recognition. Additionally, such an expansion of Prüm to include facial images could incentivise the expansion of facial image databases in Member States in a way which could lead to unlawful mass surveillance.

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.

Procedural rules for criminal investigations, data collection mandates and practices, as well as legal safeguards for accessing law enforcement databases vary considerably between Member States. Granting law enforcement authorities in other Member States access to information in police databases that could not be accessed in a similar domestic case can undermine important legal safeguards for those databases. With big data/predictive policing systems, law enforcement authorities are increasingly collecting personal data for intelligence purposes. This is likely to increase both the overall number of persons in police databases and the amount of information associated with each person registered in the sensitive biometric databases which are searchable through the Prüm framework.

The Prüm framework is primarily designed for automated checks of whether information about an individual exists in law enforcement databases of other Member States. The search in biometric databases of other Member States follows the legal rules of the requesting Member State, but 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.

This follow-up process introduces a very important manual assessment in the requested Member State of whether the disclosure of personal data satisfies conditions of necessity and proportionality, as well as an opportunity to review the accuracy of the personal data before it is disclosed to authorities in another Member State, where it generally will be much more difficult to assess the accuracy of the personal data. Furthermore, since there is no obligation in the Prüm Decisions to provide information other than the hit/no-hit response, the requested Member State can refuse disclosure if it would be prejudicial to the fundamental rights of the individual, or if disclosure could jeopardise ongoing investigations in the requested Member State.

17.1 What 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.

We also wanted to choose "EU should provide support and guidance to facilitate cooperation between Member States' law enforcement authorities." but the form does not allow for it.

New measures for speeding-up and streamlining the hit follow-up exchange procedure must be strictly limited to making the administrative process more efficient (for example by requiring Member States to allocate sufficient resources to cooperation with authorities in other Member States), while preserving all current legal safeguards for individuals.

The preferred option for EDRi is that the follow-up information exchange continues to follow the national law of the requested Member State and mutual legal assistance rules without a direct obligation to disclose specific information to other Member States.

In the view of EDRi, it would be highly problematic to introduce an automated procedure for exchange of additional information, as this processing would constitute automated decision-making within the meaning of Article 11 of the LED for the controller in the requested Member State, especially as the automated data exchange could be triggered by processing sensitive personal data (biometric data) which is prohibited by Article 11(2) unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

If a revised Prüm framework adopts minimum standards for the data provided in the follow-up procedure, there must be a mandatory manual review in the requested Member States, at least in order to verify the accuracy of the personal data disclosed, and there must be grounds for refusal by the requested Member State similar to Article 11 of the European Investigation Order (EIO) Directive 2014/41/EU.

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.

See answers to questions 17 and 17.1

To Question 17.2 to which we would have liked to answer, "17.2 To what extent should the process be regulated at EU level?", we would have answered:
Harmonising the deadlines to reply to a request: I do not know
Determine the law enforcement information exchange channel through which the request and the reply should be submitted: Yes
Agree on a limited data set to be first provided in “fast track”: No
Establish a designated “Prüm” IT application for submitting and receiving the requests: I do not know

Please explain in more detail why (not).
The EU could assist in facilitating the exchange of requests for follow-up information as long as this system only serve as a pass-through server to transmit messages between Member States. Emergency procedures (“fast track”) should remain regulated by the national law of the requested Member States and follow the corresponding legal safeguards.

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.

We have concerns that the creation of a communication server would serve as a first step to either the construction of a new EU-level database or the interconnexion of the database with other existing interoperable EU databases. 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.

To Question 19.1 to which we would have liked to answer, "19.1 Which of the following options would seem the most appropriate technical solution for Prüm?", we would have ticked "Network of bilateral connections between Member States’ databases
(maintaining the current solution)"

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.

As described elsewhere in this response, the inclusion of facial images entails risks to people’s rights to data protection and privacy, as well as other rights such as dignity, non-discrimination and fundamental freedoms. Because people’s faces are so strongly linked to their identity, any regulatory change that leads to unnecessary facial image collection and facial recognition should be strongly opposed. There are no safeguards that would justify the expansion of the framework to include facial images given the pre-existing biometric data categories that are already in use. Such an expansion could also undermine public trust in law enforcement procedures and poses significant risks of scope creep.

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.

If Europol were to feed the Prüm system with its database containing information received from third countries, this would amount to “data laundering” if that data is received from countries that cannot guarantee a sufficient level of fundamental rights protection.

According to Europol’s programming document 2020-2022, priority agreements on the transfer of personal data between Europol and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey are currently negotiated. All these countries have very poor records in terms of democratic standards, the rule of law and the respect of human rights, especially human rights abuses committed by law enforcement authorities. Up to now, some of them do not have any legally binding data protection instrument in place. These agreements risk undermining the quality of the protection of the personal data of European data subjects.

Therefore EDRi opposes the inclusion of Europol data into the Prüm exchange mechanism.

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.

After the entry into force of the General Data Protection Regulation and the Police Directive, it is crucial that transfers to third countries and international organisations can only take place on the basis of adequacy or a binding agreement providing adequate safeguards. A binding agreement will ensure legal certainty as well as full accountability of Europol for the transfer and should always be requirement for massive, structural and repetitive transfer of personal data. In any event of a data transfer, appropriate safeguards should exist to ensure that individuals’ rights are enforceable and effective legal remedies are available following the transfer.

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.

SIS II has an alert category for missing persons. Fingerprints can be included, and now so can DNA when fingerprints are not available. So this is unnecessary.

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.

Presumably this would require the establishment of some sort of central database in order to log all the previous queries. For that reason alone, we think this objective should not be pursued.

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?

There is very little democratic control and scrutiny over the use and development of police databases in Europe. Citizens learn every day that new technologies are being used by police forces with neither public knowledge about it nor democratic debate – let alone legal basis. In a context where law enforcement authorities are subject to legitimate criticism and questioning or their systemic abuse of power, and notably cases of racist overpolicing and disproportionate targeting of human rights defenders, journalists, trade unions and marginalised communities, the review of the Prüm framework should assess and address the issue of structural discrimination against people whose data is held in these databases. Beyond the review of the compliance of the Prüm automated data exchange mechanisms with fundamental rights and other legal requirements, the EU should also put into question the endless collection of people's data for law enforcement purposes that leads to a data-driven mass surveillance system.

We have the opportunity to hold this important debate this time. Originally, the Prüm instrument was an international convention between seven EU Member States, before its integration into the EU legal framework in 2008. Because the Lisbon Treaty did not enter into force before 2009, the European

Parliament never had the opportunity to have a say in the decision over the Prüm rules. As a result, the initiative never benefited from genuine democratic oversight and judicial control (by the Court of Justice of the European Union) and crucially lacks in democratic legitimacy. The European Commission should ensure that the European Parliament is fully included in the first phases of the evaluation process and its opinion is taken into due account when defining the future political orientations of the framework, not left with only the technical details to debate on.

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?

To Question 15.1 to which we would have liked to answer, "15.1 What do you consider to be the most appropriate means to address this shortcoming?", we would have chosen "EU should provide support and guidance to facilitate cooperation between Member States' law enforcement authorities."
The preferred option for EDRi is that the information exchange continues to follow the national law of the requested Member State and mutual legal assistance rules. The EU could assist in improving the system of assistance and especially the procedural challenges raised by the MLAT system.

To Question 15.2 to which we would have liked to answer, "15.2 What data could be exchanged under the same principles as provided by the Prüm framework?", we would have chosen:
Limited extract of police records: No
Driving Licences: No
Photos of suspects and convicted criminals: No
Ballistics: No
Other: No
See response to Question 1.
EDRi opposes the addition of new categories of data before the Prüm framework is thoroughly evaluated. Even following evaluation, we believe that introducing the category of facial images would expand the fundamental rights risks posed by the framework without sufficient justification (given that DNA and dactyloscopic data are already included) in order for such an expansion to be considered legitimate.

To complete answer to Question 16:
"Regarding extracts of police records, the introduction of a European Police Records Information System has been under discussion for years. The sharing of limited extracts from police records via the Prüm system would get a foot in the door. Whereas in 2012 the European Commission considered that the setting up of a new exchange framework for biographic data contained in national police records would be too costly and potentially overlap with other existing systems that were not used to their fullest potentiality (EIS, SIS II, SIENA), the 2020 feasibility study commissioned by the Commission now recommends to integrate that new data category in the Next Generation Prüm. However, information stored in national police records (and other operational information systems for that matter) is not always accurate. The quality of these records may suffer in various respects (spelling errors, lack of documentation, unreasonable assumptions, arbitrary categorisation resulting from hear-say, gossips, and false information etc). The data inaccuracy and arbitrariness are particularly worrying when these records contain sensitive data such as political affiliation, trade union membership and religious beliefs (See the example of France: https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-

religious-beliefs/, of the United Kingdom: https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists, Germany: https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/, and Spain: https://www.statewatch.org/news/2016/october/spain-squeezed-by-the-spooks-attempt-to-recruit-activist-as-informant-caught-on-tape/). The negative impacts on affected people's rights could be significant as there are no shared European definitions for describing and common understanding of behaviours that deserve further police scrutiny. That's notably the case for "troublemaker", for which previous attempts to create such European database on "travelling violent offenders" repeatedly failed (see Matthias Monroy, https://digit.site36.net/2019/01/23/eu-tests-crossborder-querying-of-police-files/)."

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.

The maximum file size is 1 MB
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

106b711a-efda-47a3-9c04-02431aa2eb24/2020210323_EDRiResponsePr_mIIAConsultation.pdf

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?

- None
- Very limited
- Limited
- Good
- Very good
- 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?

- None
- Very limited
- Limited
- Good
- Very good
- 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	○	○	○	○

Contact

Contact Form