Respecting fundamental rights in the cross-border investigation of serious crimes

A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")

7 September 2022

This paper has been co-authored by EDRi members: Access Now, Digital Society (Switzerland), Državljan D (Citizen D, Slovenia), the European Center for Not-for-profit Law (ECNL), the IT-Political Association of Denmark (IT-Pol) and Statewatch.
We are extremely grateful for their support and expertise.


Table of Contents

Executive summary of our analysis and recommendations

The Prüm framework is a set of European Union (EU) laws which regulate the automated sharing of certain personal data between Member States for investigating purportedly serious crimes. Whilst the framework is long overdue for reform, we argue that any reform should focus on tackling structural issues with the (mis)use of national police databases; on establishing the necessity and proportionality of the Prüm framework; and on aligning data protection safeguards to the standards of the Law Enforcement Directive. The EU's new proposal, Prüm II, fails to make these improvements, and creates additional serious risks to fundamental rights.

Having entered into force before both the Lisbon Treaty (2009) and the Law Enforcement Directive (LED) (2018), the Prüm framework is arguably no longer fit for purpose. A modernisation of the 2008 Prüm Decisions is thus much-needed. Unfortunately, the analysis undertaken by the EDRi network finds that this is not achieved by the European Commission's proposal for Prüm II.

The proposed Regulation fails to align itself sufficiently to the LED, instead lowering the protection of personal data and procedural rights – in contradiction to its own legal basis. Furthermore, the proposal fails to meet vital obligations under the Charter of Fundamental Rights of the European Union ("the Charter"), which require any limitation on fundamental rights to be necessary, proportionate and with adequate safeguards.

We argue that the draft law fails to demonstrate the necessity and proportionality of its measures, in particular its vastly expanded categories of personal data. The framework and proposed expansion entail serious fundamental rights risks such as undermining the presumption of innocence, enabling mass surveillance and criminalising migration. We also question the addition of searches for missing people and unidentified remains, which do not fit the proposal's legal basis.

Given the issues described in Section 1 with the management and operation of policing databases across Europe, systemic discrimination in policing, and the EU's broader rule of law crisis, we fear that the proposed enhanced automation under Prüm II will exacerbate and further entrench these issues. Using examples, this paper will demonstrate that the proposal for Prüm II risks missing a vital opportunity to fix systemic issues in the exchange of data across borders by law enforcement agencies under the existing Prüm framework. We therefore call on the EU's co-legislators to:

1. Implement **specific rules for Member States' police databases prior to their connection** to the Prüm II system, to ensure a high level of protection of fundamental rights (Section 1);
2. Remove the sharing of **Europol-held third-country biometric data** and remove Europol's own-initiative biometric searches, which lack a legal basis (Section 1);
3. Add **additional safeguards** to the sharing of reference data, as well as more broadly throughout the Prüm system in order to **align to the LED** (Sections 1 and 3);
4. Request a thorough **necessity and proportionality assessment** of the proposal for Prüm II, including requiring evidence and statistics to clarify whether the current framework is effective. If not, the co-legislators should **delete all elements of the proposal that are not demonstrably necessary and proportionate** (Sections 2, 4 and 5);
5. **Delete** the large-scale automated exchange of **unidentified DNA data** (Section 3);
6. Ensure **all searches** can only be undertaken on the basis of **genuinely individual** cases, and only in the event of **serious crimes**, with additional safeguards (Section 3);
7. Grant member states a meaningful **right of refusal** before the exchange of personal data (Section 3);
8. Fully **reject the inclusion of facial image exchange** in Prüm II due to the serious risks of fundamental rights violations (Section 4);
9. **Limit the definition of police records** to ensure that biased assumptions, hear-say and other illegitimate records will not be shared via Prüm II (Section 4);
10. **Resist the attempt to add national driving license systems**, which would treat whole populations as if they are suspected of serious crimes (Section 4).

Background: What is Prüm II?

The '**Regulation on automated data exchange for police cooperation (Prüm II)**' (2021/0410(COD)) is a draft internal security law adopted by the European Commission on 8 December 2021. It will govern the **sharing of data** between 'authorities responsible for the prevention, detection and investigation of criminal offences', meaning police and judicial authorities. Prüm II seeks to **'modernise' the Prüm framework**, a pair of 2008 Council Decisions which facilitate the exchange of certain data between European Union (EU) member states.

The original Council Decisions (2008) codified an intergovernmental treaty (the Prüm Convention, 2005) which allowed member states to share data bilaterally across borders.[1] Entering into force before the EU's Lisbon Treaty, the original Prüm Decisions did not follow the EU process of co-decision. This means that the European Parliament's role in scrutinising the original Prüm framework was limited.

The proposal for Prüm II is part of the broader **EU 'Security Union' package**, specifically the Police Cooperation Code. Prüm II is based on the premise that whilst criminals can move freely between Schengen countries, data and information currently do not move as freely between law enforcement authorities. The implementation of bilateral connections for data exchange in the original Prüm framework has been very slow. The new proposal suggests that these issues are largely a result of problems with IT systems and a lack of technical interoperability.

According to the European Commission, **the intention of Prüm II is to remove barriers in order to streamline and accelerate the cross-border sharing of data relating to investigations of crimes such as terrorism and organised crime**. However, the proposal does not establish legal thresholds, such as the severity of the crime, to limit the sharing of data only in relation to serious crimes. Prüm II will apply to all EU Member States except Denmark; although the participation of Ireland is to be confirmed. The UK can be invited to participate in Prüm II, despite no longer being a member of the EU; it remains connected to the original Prüm network.[2]

The main novelties of Prüm II are the addition of new categories of data for exchange; and the technical developments focus on the creation of a central router by eu-LISA (the EU's Agency for Large Scale IT Systems); the creation of the European Police Records Index System (EPRIS), developed by the EU's law enforcement agency, Europol; and alignment with the EU's interoperability architecture. The new central router would remove the need for the current bilateral connections, instead centralising searches (but not centralising databases). The EPRIS system would also make police records searchable via the Prüm framework. Additionally under Prüm II, Europol will have an enhanced role, being able to search Member States' databases as well as to provide access to third-country databases.

Compared to the original framework, Prüm II seeks to:

- **Increase automation** of the sharing of data;
- **Add new categories of data** that can be shared (facial images, police records, and – in the Council of the EU's position – driving licence data);
- **Standardise the format** in which data can be shared (thus easing future integration with other systems);
- **Set new standards** on data quality, transfers, and other largely technical elements; and
- Create a legal basis for searches for **missing persons and unidentified human remains**.

1 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008D0615; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, https://eur-lex.europa.eu/eli/dec/2008/616.

2 'EU police forces authorized to transmit DNA and fingerprint data to the UK from 30 June', Statewatch, 27 June 2022; UK can join EU surveillance schemes with no parliamentary scrutiny, warns new report, Statewatch, 2- January 2022, https://www.statewatch.org/news/2022/january/uk-can-join-eu-surveillance-schemes-with-no-parliamentary-scrutiny-warns-new-report/.

Glossary

CIR: Common Identity Repository, established by the Regulations on the interoperabilty of police, judicial cooperation, migration and asylum databases
EPRIS: European Police Records Index System, established by Prüm II
eu-LISA: the European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice
Eucaris: European Vehicle and Driving Licence Information System
EUCARIS: Treaty concerning a European Vehicle and Driving Licence Information System
Requesting state: the Member State submitting a request via Prüm II
Requested state: the Member State whose database contains a potential match
SIENA: Secure Information Exchange Network Application, managed by Europol
UDF: Uniform Data Format, a technical standard for digitalising dactyloscopic data
UMF: Universal Message Format, a technical standard for the data exchanged via the central router

Summary of the data exchanged under the proposed Prüm II Regulation[3]

Type of data exchange	Mandatory elements	Searches	Access to matching data	System used	Specific requirements / safeguards	Managed by
DNA data (Arts. 5-11, 35-37)	Mandatory searchable national database(s) (5)	Individual automated searches (6); mass automated comparison of unidentified profiles (7)	Automated return of matching DNA profile + reference nr. for individual searches (6.2); manual return 'without delay' for mass comparisons (7.3) 11.2 is also relevant.	A new Central router (35) using UMF (34), with additional rules on queries, quality, logs etc for all biometric data	Confidentiality, integrity, encryption, standards via Implementing Act (IA) (10). Must meet minimum loci to be a match (11.3)	Eu-LISA (53.1)
Dactyloscopic data (fingerprints and palm prints) (Arts. 12-17, 35-37)	Mandatory searchable national database(s) (12)	Individual automated searches (13.1)	Automated return of matching dactyloscopic data + reference nr. (13)	A new Central router (35) using UMF (34)	Must follow UDF specified in an IA; be of sufficient quality, standards, confidentiality & encryption (15)	Eu-LISA (53.1)
Vehicle registration data (Arts. 18-20)	Mandatory searchable national database(18)	Individual automated searches (18)	Automated return of data relating to owners, operators and/or vehicles (18.1); codifies existing Eucaris system (bilateral)	Eucaris (pre-existing bilateral system) (Art. 19)	Must be encrypted; data elements to be specified in IA (19). Logs must be kept (20)	Currently bilateral via RDW (The Netherlands' Vehicle Authority)
Facial images (Arts. 21-24, 35-37) (new)	Mandatory searchable national database(s) (21)	Individual automated searches (22.1)	Automated return of list of facial images that are 'likely' matches (22.2, 24.2).	A new Central router (35) using UMF (34)	Must meet minimum quality standard to be specified in an IA (22.3)	Eu-LISA (53.1)

3 '(Reference) data' means both the genetic / biometric profile (e.g. DNA profile, fingerprint template) and the corresponding (non-identifiable) reference number that it has been assigned. For example, both the term 'DNA data' and 'DNA reference data' would mean the DNA profile itself, as well as the reference number.

Police records (Arts 25-28, 42-44) (new)	Not mandatory, but must contain minimum data if made available for exchange (25).	Individual automated searches (26, 43, 44)	Automated return of list of matches (26,28) but human intervention is required for the records themselves	EPRIS (42) for search, and then SIENA to send the actual police record (44.6)	Indication of quality of matches (26.2); Manual decision whether to share records (44.6); Technical procedures via IA (44.7); logs (45)	Europol (53.2)
Core data: name, DOB, nationality, birth place, gender (47 when held by MS; 50 when Europol)[4]	Mandatory exchange for DNA, dactyloscopic data and facial images matches (47)	After the initial automated search of biometric data, in the event of a match	Returned within 24 hours of a 'confirmed' match (47)	Central router (35) using UMF (34)	Prior 'confirmation' of match by requesting Member State (47)	Eu-LISA (53.1)
Interoperability (39) (new)	Not mandatory, but can be undertaken simultaneously to searches of biometric data performed via central router (39.1)	The central router shall send the query on the basis of the biometric search (39.1)	Not defined in Prüm II	Common Identity Repository (CIR) via the European Search Portal (ESP) (35.2.c, 39)	In accordance with access rights (39.2) and only if it is likely that data about the suspect, perpetrator or victim of a serious offence are in the CIR (39.4) [note that *seriousness* of offence is not a criteria elsewhere]	Eu-LISA (53.1)
Third country-sourced biometric data	Mandatory access for MS to Europol's data (49)	For purposes defined in Regulation (EU) 2016/794 (49.1)	As defined in Regulation (EU) 2016/794 (49.2)	Central router (35)	As per Regulation (EU) 2016/794 (49)	Europol (49)
Any other data	Not mandatory	n/a	n/a	SIENA	n/a	Europol
Driving licence data	*Mandatory in Council position[5]; not part of Commission proposal*	*Individual searches based on driving license number or data relating to driving license holder*	*Via Eucaris. Member States may allow access to facial images in the driving licence data, if available*	*Eucaris*	*Information exchanged must be transmitted in encrypted form*	*Currently RDW (The Netherlands' Vehicle Authority)*

A note on our choices of terminology in this paper: *whilst much literature on the topic of discrimination and law enforcement refers to "ethnic minorities", we primarily choose to use the term "racialised people". We are inspired by the Equinox Initiative for Racial Justice, who explain that racialisation is a process which focuses on 'power dynamics' that go 'beyond fixed or objective notions of race or ethnicity.' [6] We also use the term "minoritised" which refers to people who are constructed or perceived in society as being a "minority" This includes non-EU / non-Schengen nationals (although usually only if they are racialised), people on the move ("migrants"), poor people and asylum seekers. The process of minoritisation often intersects with the process of racialisation, meaning that many of the communities that are subjected to systemic discrimination and injustice have been constructed as both racialised and minoritised.*

4 In the case of a confirmed match with identified data, the Council's position would also add previously used name(s) and alias(es), date and place of biometric acquisition, the criminal offence in the framework of which the biometric acquisition was carried out, the criminal case number, the responsible authority of the criminal case; in case of a match with unidentified data (trace): date and place of biometric acquisition; the criminal offence in the framework of which the biometric acquisition was carried out; the criminal case number; and the responsible authority of the criminal case (https://data.consilium.europa.eu/doc/document/ST-9544-2022-INIT/x/pdf)

5 https://data.consilium.europa.eu/doc/document/ST-9544-2022-INIT/x/pdf.

6 https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf, page 5.

Section 1. Prüm II will exacerbate pre-existing issues with the Prüm framework, the abuse of police databases and the rule of law crisis

1.1 The EU must address existing problems with the Prüm framework

The premise underpinning the Prüm framework is that because criminals can operate freely across Schengen country borders, so too must data about them held by law enforcement authorities. But this assertion, that "law enforcement authorities in one Member State [must] have access to the same information that is available to their colleagues in another Member State" is a non-sequitur, and furthermore, is not sufficiently proven by the Prüm II proposal.[7]

This approach foregrounds the concept of convenience to the potential detriment of due process and respect of fundamental rights. Specifically, it presumes that all law enforcement and judicial agencies in the Schengen area ensure equal protections for people's personal data and due process rights, and that access to remedies, the independence of the judiciary, the effective functioning of independent oversight authorities and the protection of fundamental rights are all consistently guaranteed. The reality on the ground suggests a different picture.

> *"Without serious improvements, the proposed Prüm II Regulation will be like pouring petrol on the fire that is the state of data collection, processing and cross-border exchange by law enforcement in Europe*."
>
> - Ella Jakubowska, Policy Advisor at EDRi

Regrettably, the proposal for Prüm II does not seem to have learned from the problems with the 2008 Prüm Decisions. Criticisms have been levied by academics and civil society relating to everything from failures of implementation through to mismanagement of criminal databases.[8] EDRi has been vocal about the lack of a satisfactory assessment of the necessity and proportionality of the 2008 Decisions, and the European Parliament have also pointed to issues with the Prüm framework.[9] In his Opinion on Prüm II, the European Data Protection Supervisor (EDPS) "*notes with regret that 15 years after the first Opinion, his main concerns regarding the necessity and proportionality of the initiative are still valid and are even further exacerbated by the proposed significant extension of the scope of the automated exchange of data.*"[10]

By adding new elements without addressing the deep-rooted problems, nor taking measures to sufficiently align to the LED and the Charter, Prüm II risks exacerbating an already dangerous situation, with huge implications on people's rights and liberties.

Not only does Prüm II fail to correct such issues, it furthermore removes vital safeguards from the 2008 Prüm Decisions, such as the requirement for data protection audits and evaluation visits of member states prior to connecting their systems.[11] Given that the legal basis for Prüm II is data protection (Article 16, Treaty on the Functioning of the European Union), we argue that **strengthening data protection safeguards in the proposed law is urgently needed to ensure the legitimacy of the proposal and its aims.**

---

7 Explanatory Memorandum, https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2021/0784/COM_COM(2021)0784_EN.pdf

8 See https://www.statewatch.org/media/documents/analyses/no-197-prum-implementation.pdf; https://eurocop.org/wp-content/uploads/2020/10/IPOL_STU2020658542_EN.pdf; https://academic.oup.com/bjc/article/60/1/141/5555659?login=false

9 https://edri.org/wp-content/uploads/2021/03/EDRi_Public_Consultation_Prum_framework.pdf ; https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

10 https://edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf, p.6

11 For example: https://data.consilium.europa.eu/doc/document/ST-7523-2022-INIT/en/pdf.

1.1.1 Rules for national law enforcement databases are not harmonised

Particularly worrying in the context of Prüm II is the widely differing national rules for storing information on individuals in police databases. Whilst Member States – at least in theory – have the appropriate national frameworks to ensure that every entry in a national database has a specific legal basis, this is not consistent from one Member State to another. As the EDPS points out, thresholds vary significantly for what constitutes a serious crime, whether those convicted of minor crimes can be included included in a database, whether persons who were subsequently not convicted, or acquitted, can be included, and the inclusion of other persons (e.g. minors, non-nationals or even the whole population).[12]

This is backed up by evidence submitted by Member States to a Council working group which shows that the percentage of the population held in each national DNA database varies widely.[13] In France, for example, around 9% of the population are included in the database, and around 5% in Latvia, Lithuania and Austria. In Finland, Denmark, Czechia, the Netherlands, Cyprus and Sweden, the figures stand between 2 and 5%. This is a stark contrast to countries like Portugal and Malta, whose DNA databases contain 0.14% and 0.15% of their countries' populations respectively. Not only does this highlight that there must be vastly different national rules for inclusion, but it also calls into the question the necessity of many of the profiles included in many national databases. It is very difficult to see how almost 10% of the French population, for example, could be suspected or convicted of serious crimes.

> ***Example***:[14] *In **Sweden**, an individual's data can only be included in the national law enforcement DNA database if the person has been convicted of a crime with a sentence greater than 2 years. **Germany** has even stronger safeguards and protections. By contrast, in the **Netherlands**, a person's DNA data will be added to the national system for having committed any crime (with an exception only where the punishment is simply paying a fine). **Italy's** DNA database came under fire in 2013 for adding children. **Portugal's** government faced criticism for trying to add their country's entire population. And **Denmark** recently increased the retention period in their national DNA database for non-convicted persons from 10 to 20 years.*

This means that an individual can be included in a database in one Prüm II participating Member State when they would not be in another, creating a patchwork of rules **offering fragmented protections to individuals**. What's more, the conditions to justify a search ('query') of a biometric database also differ between Member States.

The proposal for Prüm II fails to consider these particularities, meaning that **individuals registered in a police database in a member state with lower thresholds for inclusion, weaker safeguards or less effective oversight mechanisms will be more likely to be subject to potentially unjustified police attention** than individuals who benefit from higher national standards. As a result, they will be unfairly subject to the concomitant enhanced risk of intrusions upon their rights to due process, an effective remedy, and privacy and data protection.

1.1.2 Systemic discrimination and political policing

Whilst the aim of tackling crime is a legitimate and important goal, it is intrinsic to democratic societies that this is done in a way which prevents arbitrary intrusion into people's rights,

12 https://edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf
13 https://www.statewatch.org/media/3248/eu-council-prum-statistics-2021-5436-22.pdf.
14 https://en.wikipedia.org/wiki/DNA_database; https://www.omicsonline.org/open-access/minors-inclusion-in-the-italian-forensic-dna-database-which-safeguard-between-justice-and-individual-rights-2169-0170.1000107.php?aid=20761

respects people's right to be presumed innocent, and follows due process. This does not only protect the rights of individuals; it also protects victims of crime and safeguards the general interests of justice by making sure that evidence can be admissible in court.

However, a landmark report on data-driven policing from the European Network Against Racism (ENAR) shows that many law enforcement databases across Europe, containing large amounts of biographical information as well as biometric and other sensitive personal data, suffer from dangerous inaccuracies, prejudices and examples of potentially unlawful profiling.[15] Racialised people are "systemically over-represented" in police databases across Europe, adds the Equinox Racial Justice Initiative.[16] The UK's "Gangs Matrix", for example, has come under fire for unfairly targeting young men of colour and other minoritised people;[17] and racialised people are vastly over-represented in the country's criminal justice system in general.[18] The Netherlands' 'Top400' and 'Top600' databases have received similar criticism from criminal justice watchdog *Fair Trials* for illegitimately targeting young people from poor and minoritised backgrounds, thereby automating the injustice that they face at the hands of the state.[19]

In the Netherlands, people are included in pseudo-criminal biometric databases solely for the 'crime' of being foreign, or are wrongfully included in criminal databases without a legal basis and with no course for redress or removal.[20] Politically-repressive uses can also be seen in many European countries, for example in Austria, where police added 640,000 entries to their new facial database in one year, including those of demonstrators – far from the serious criminals that the system was intended for.[21] Police in France,[22] the UK,[23] Germany[24] and no doubt other states also systematically collect substantial amounts of data on political activists.

These problems are not the result of simple errors, but in fact reveal systemic problems. In 2021, the EU's Fundamental Rights Agency (FRA) confirmed that across Europe, "Black people, Asians and Roma are still more likely to be stopped and searched by police".[25] FRA's report further explains that "ethnic minority people" are more than twice as likely to be asked for their identity papers, and are half as likely to perceive that they were treated respectfully by police during such stops. **These biases and acts of profiling are, as a result, reflected in the data that are collected and are codified in databases, and can reinforce and perpetuate discrimination.**

As argued by Dr Seda Gürses and Agathe Balayn, technical approaches to this problem are inherently limited.[26] Bias and discrimination are social and political questions, and extend not just to the fairness or quality of data put into a database, but equally to decisions about the design of a particular database, as well as the broader sociotechnical system that determines how it is used, who controls it and who is subject to it.

---

15 https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf
16 https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf, page 11
17 https://www.independent.co.uk/news/uk/home-news/met-police-gangs-matrix-database-b2004293.html
18 'Ethnicity and the criminal justice system: What does recent data say on over-representation?', House of Commons Library, 2 October 2020, https://commonslibrary.parliament.uk/ethnicity-and-the-criminal-justice-system-what-does-recent-data-say/
19 https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf
20 https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/
21 https://www.euractiv.com/section/politics/short_news/austrian-facial-recognition-database-collects-over-600000-entries-in-a-year/
22 'France: Green light for police surveillance of political opinions, trade union membership and religious beliefs', Statewatch, 13 January 2021, https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/
23 'Calls for extremism database to be abolished as ECtHR rules UK police violated peaceful pensioner's privacy rights', Statewatch, 28 January 2019, https://www.statewatch.org/news/2019/january/uk-echr-calls-for-extremism-database-to-be-abolished-as-ecthr-rules-uk-police-violated-peaceful-pensioner-s-privacy-rights/
24 'Suspicion files: German police databases on political activists'. Statewatch, 10 April 2018, https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/
25 https://fra.europa.eu/en/news/2021/police-stops-europe-everyone-has-right-equal-treatment
26 https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

1.1.3 Errors, misuse and poor quality data are common

The discriminatory over-representation of racialised people and non-EU nationals in law enforcement databases, as well as the suppression of forms of legitimate political and civil expression, is further exacerbated by the fact that generally inaccurate and poor-quality data are included at a vast scale in many European law enforcement databases.[27]

Repeated human errors, the absence of rigorous processes and safeguards, and failures to process policing data in accordance with the LED are unfortunately the reality in many European countries. For example, in Slovenia, investigations have revealed that victims and their family members have been included in criminal databases, and other examples show that non-suspects, acquitted people, victims and witnesses are routinely included in criminal databases without a legal basis.[28] Given the lack of transparency around these systems, many people are unaware that their data is being unlawfully processed, and are unable to exercise their rights to redress. Yet their inclusion in these databases can have severe repercussions on their rights and liberties.

> ***Case study**: **Switzerland** participates in the Prüm framework as part of its close cooperation with the EU. In Switzerland, 92% of criminal convictions are sentenced with summary penalty orders, of which there were 83,357 in 2020. Often without hearing the accused, a prosecutor can impose prison sentences of up to six months. If no appeal is lodged within ten days, the summary penalty order is considered a final judgment. The proportion of "fictitiously" served summary penalty orders, which the person concerned has effectively never seen, can be as high as 10% or more in certain cantons.[29]*
>
> *Sentences handed down in this summary penalty order procedure, which is problematic from the point of view of the rule of law, are entered in the Swiss criminal records database and potentially other police records / information systems. This means that these databases contain erroneous entries. For example, a conviction that was fictitiously served on a person who did not commit the offence, based solely on the fact the this person used the same alias name as the potential offender. These practices tend to disproportionately affect persons without a permanent residence in Switzerland and persons who do not understand the official language.*

There are also indications of frivolous searches under the current Prüm framework. In 2021, for example, Malta, Austria and Romania searched upwards of 99% of their national DNA profiles, raising questions about whether each of these searches could really have related to a specific, individual case and in line with due process and the rule of law.[30]

1.2 The EU rule of law crisis

These issues of the over-policing of racialised and minoritised people also exist within a broader

27 Potential sources of error for DNA evidence are discussed in Dr. Victor Toom, June 2018, 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision: LIBE Committee Study': https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf. The Danish National Police are currently reviewing thousands of criminal cases for DNA errors, Jurist, 30 June 2020, 'Denmark to review criminal cases for DNA errors': https://www.jurist.org/news/2020/06/denmark-to-review-criminal-cases-for-dna-errors/. Other examples are found in Austria (https://www.euractiv.com/section/politics/short_news/austrian-facial-recognition-database-collects-over-600000-entries-in-a-year/)

28 For example https://www.primorske.si/2012/04/18/spanski-kljuc-resitve-posilstva.

29 https://www.beobachter.ch/gesetze-recht/fiktiv-zugestellte-strafbefehle-die-grosse-macht-der-staatsanwalte

30 https://www.statewatch.org/media/3248/eu-council-prum-statistics-2021-5436-22.pdf

rule of law crisis.[31] We are witnessing the growing criminalisation of political opposition, social movements, refugees and migrants (as well as those that act in solidarity with them by providing aid and humanitarian support) and investigative journalists. *Freedom House* reports that multiple EU countries – including France, the Netherlands, Cyprus, Portugal, Poland, Lithuania and Latvia – became "less free" between 2020 and 2021, with Liberties' 2022 Rule of Law Report further highlighting how democratic standards are being eroded in several EU countries.[32] And Netzpolitik reports that Hungary, Greece and Italy have all actively criminalised the aiding of migrants.[33]

Compounding this threat, countries like Hungary and Poland have faced infringement proceedings from the European Commission in recent years for violations of the rule of law and threats to the independence of the judiciary. Systemic failings in the operation of national police databases have been documented across Europe.[34] Even the European Commission's *mechanism* for evaluating the rule of law has come under fire from the European Parliament and in independent assessments.[35] In 2022, the European Parliament even had to open an investigation into the NSO Group, whose Pegasus spyware was allegedly used for unlawful state hacking against journalists, politicians and human rights defenders, along with various other state misuses of various spyware tools.[36]

1.3 The Europol and third-country problem

The enhanced role of Europol under the Prüm II proposal is also cause for concern. In 2020, Europol was admonished by the EDPS for systematic failings which led to the Agency processing large volumes of data in a way that violated fundamental rights. Despite attempted improvements, in 2022 the EDPS once again had to intervene to order Europol to delete data that the Agency was still processing and retaining illegally.

Without serious improvements, the Prüm II Regulation is likely to facilitate these same abuses of people's most personal data. Currently, Prüm II foresees Europol becoming "the Union criminal information hub" (Recital 3), giving the agency significantly expanded powers despite its track record of abuse. Under Prüm II, European police agencies have the possibility to access data that has been exchanged with third countries by Europol (Articles 49 and 50). Similarly, Europol can search all Member States' databases with biometric data received from third countries. Information about matches could be shared with these third countries in accordance with the Europol Regulation.[37] This risks increasing political repression in third countries, while also giving European authorities the possibility to penalise dissidents or other people who are facing politically-motivated persecution from third countries, especially those residing in Europe.

We share, therefore, the European Economic and Social Committee's concern that Europol's role in Prüm II may create an "overlap with migration and asylum issues."[38] Such an issue is compounded by the fact that many Member States' criminal databases contain data of asylum seekers and migrants (see Appendix 1). Combined, these factors create a risk that Prüm II will

31 https://ec.europa.eu/info/publications/2022-rule-law-report-communication-and-country-chapters_en
32 https://freedomhouse.org/explore-the-map?type=fiw&year=2022&mapview=trend
33 https://netzpolitik.org/2022/pruem-ii-verordnung-zu-datenaustausch-eu-ausschuss-kritisiert-geplante-verpflichtung-zur-gesichtserkennung/; https://www.liberties.eu/en/get-involved/liberties-rule-of-law-report-2022/69
34 For example: https://www.enar-eu.org/data-driven-policing-the-hardwiring-of-discriminatory-policing-practices-across-europe/
35 https://www.europarl.europa.eu/news/en/press-room/20220620IPR33409/rule-of-law-in-the-eu-ways-to-better-protect-the-union-s-core-values
36 https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched
37 The amendments to the Europol Regulation, adopted in 2022, will make it easier for Europol to share personal data with third countries.
38 https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/security-union-packageschengen-package

exacerbate the criminal treatment of asylum seekers and other third country migrants, outside its purpose of tackling serious crime, and potentially in contradiction to international humanitarian obligations as part of wider trends of the criminalisation of migration.[39]

Europol's collection of biometric data is a particular source of concern. Member States should have clear rules in place regarding the collection and retention of biometric data by law enforcement authorities: for example, to prevent persons merely accused of a crime from having their biometric data retained indefinitely.[40] The EU interoperability system similarly has predictable rules for adding and removing people from biometrics databases.[41] This is not the case for Europol, which can receive biometric data from third countries under quite general conditions. Contrary to what the Prüm II proposal states in Recital 13, there is absolutely no guarantee that the biometric data concerns only convicted and suspected terrorists and other serious criminals. What's more, this assessment may be made by third countries with questionable human rights records, increasing the risk to individuals' rights.

Moreover, the 2022 amendment of the Europol Regulation has granted Europol new powers to receive and retain large data sets, whilst lowering the safeguards around transfers of personal data to and from third countries, which will only exacerbate the problems with questionable data sources. Contrary to the EDPS's important maxim: "with stronger powers should always come a stronger oversight", Europol's stronger powers have been granted in an absence of accountability.[42]

EDRi thus opposes the addition of Europol's biometric databases to the Prüm II framework and the granting to Europol of the power to search the biometric databases of Member States. We therefore recommend the deletion of Article 40 and the removal of the elements granting Europol access / power from Articles 6.1, 13.1, 22.1, 35, 36, 37, 40, 44 and 50. This is necessitated by the fact that Europol does not have executive powers, and is not supposed to initiate criminal investigations.

1.4 Protecting rights in the exchange of data under Prüm II

There is a key opportunity for Prüm II to set strong EU-wide rules and standards on the procedural elements of cross-border investigations which rely on the exchange of data within the scope of Prüm. For example, the proposal could ensure higher protections for personal data, fundamental rights and compliance with Union values by outlining specific rules which would:

- **Require all countries and agencies participating in Prüm II to pass a full, independent, ex ante data protection inspection/audit** (i.e. prior to connecting to the central router, EPRIS or Eucaris). This would verify that data in the database(s) has/have been stored in accordance with the law (in particular, requirements of 'strict necessity' and proportionality under the LED, which has come into force since the original Prüm decisions), and that officials are following the correct rules and procedures;
- **Add harmonised minimum criteria for the inclusion of persons in any criminal or judicial databases** that are connected to Prüm II. This should ensure that at a minimum, the

39 https://picum.org/wp-content/uploads/2021/10/Help-is-no-crime.pdf; https://www.coe.int/en/web/commissioner/-/pushed-beyond-the-limits-urgent-action-needed-to-stop-push-back-at-europe-s-borders

40 European Court of Human Rights, judgment in the case of S and Marper v United Kingdom, para. 125, https://hudoc.echr.coe.int/eng?i=001-90051

41 The biometric data in the Common Identity Repository is collected for border control and immigration purposes. Use of this personal data for criminal investigations means further processing for a purpose which is incompatible with the original purpose which is highly problematic. Contrary to searches of biometrics data held by Europol, which can be done solely in accordance with the national laws of Member States, the EU regulations for the interoperability framework at least have some restrictions (e.g. serious crime requirement) and safeguards, which are reflected in the Prüm II proposal (Article 39).

42 https://edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf, p.3

person meets the criteria for conviction or serious, reasoned grounds of suspicion (as per LED article 6 paragraphs b and a) and that witnesses and victims are not included;
- **Add harmonised minimum requirements for what can be considered a duly serious crime** in the scope of Prüm II and standardise terminology as recommended by the EDPS, paragraph 21 ("persons convicted of a criminal offence" instead of "criminals" etc);
- **Add harmonised minimum national requirements for the removal of persons from any criminal or judicial databases** that are connected to Prüm II, including to ensure that people who have been acquitted or not charged are removed, as well as deadlines for the removal of data following the relevant acquittal or decision not to charge;
- **Require all connecting states to have a clearly-established national definition of reasonable suspicion**, ensuring that it is publicly-accessible, clear, precise, comprehensive and non-arbitrary;
- **Require that persons are informed** about their inclusion in the databases and their rights to redress;
- **Include reporting requirements** on the number of people contained in each connected database (including by Europol), and anonymised statistics on: whether they are suspected or convicted; the types of crime which they have committed; which should be reviewed independently;
- **Request specific EDPB guidance** on how to implement rules under the LED such as on accuracy of data and other data protection rules in the context of criminal databases and cross-border exchanges of data;
- **Ensure strict necessity**: the developing case law from the European Court of Justice on the interpretation of strict necessity in Article 10 of the LED in relation to biometric databases, e.g. case C-205/21, should be taken into account and reflected in Prüm II;[43]
- **Clarify that all of these requirements are without prejudice to the LED** and other national safeguards and protections which may be higher.

Beyond creating a new chapter to achieve these aims, specific articles already in the Prüm II proposal should be improved to provide stronger data protections and safeguards:

- The proposal misses an opportunity to set requirements which would ensure that the national contact points (**Article 29**) and router users (**Article 36**) are limited to those with a strict need. It should be clarified, therefore, which authorities/roles may be authorised, and the requirements on individuals or agencies prior to their authorisation:
- The proposal stipulates that logs should be kept relating to all searches conducted via the central router (**Article 40**) and for vehicle registration data (**Article 20**) for one year. While the Council's position increases this to two years, neither would be sufficient to enable thorough audits by the EDPS, which is obliged to carry out an audit once every four years (**Article 60**). Logs in **Articles 20 and 40** should thus be kept for a minimum of four years. Logging requirements should be explicitly added for DNA and dactyloscopic data;
- **Article 33** (justification for searches) already creates a basis for certain protections. This could be expanded to include guarantees of respect for data protection, against discrimination, for access to redress, and broader fundamental rights and the rule of law;
- **Article 39.1** (CIR searches) needs to be aligned to the interoperability legislation by also requiring "reasonable grounds" of "suspicion";
- **Article 51.1** (data protection) contains a loophole in its final sentence ("Processing for other purposes…") which would allow Member States to process data via the Prüm framework but outside of Prüm's protections. This sentence must be deleted;
- **Article 51.3** (data protection) establishes that data can be processed where it is necessary for the purposes of the Regulation. As this could create ambiguity, it should be

43 As of 30 August 2022, only the Opinion of the Advocate General is available in the case C-205/21. The Advocate General proposes that Article 10 of Directive 2016/680 should be interpreted as meaning that processing of fingerprints, DNA samples and facial images is only permitted where strictly necessary for the pursuit of objectives relating to serious crime.

clarified that – in accordance with the LED – the processing must be *strictly* necessary, and the purposes should be made explicit;

- **Article 52** (Accuracy, relevance and data retention) requires that data can only be removed on the basis of a data subject's permission or alternatively a court order (52.2). It is not clear why this would not also be the case for the inclusion of a subject's data in the first place. Given that, as discussed in section 1, some Member States already require a court order to include persons in national criminal databases, such a requirement should be added here as one of the conditions for connecting a database to Prüm II;
- **Article 53** fails to specify the parts of the process in which member state authorities become data processors. This should be added into the Regulation. As the EDPS Opinion emphasises (paragraph 58), there is a need for significantly clearer data protection roles;
- **Article 58.2** (burden of proof) exempts Member States from bearing the burden of proof in the event of alleged discrimination (as established in 58.1) if the discrimination has occurred in the context of criminal procedures. As the accompanying documents to the proposal offer no explanation for this potential loophole, it should be removed;
- **Article 78** (practical handbook) requires the Commission, Europol and eu-LISA to produce "a practical handbook for the implementation and management of this Regulation." The EDPS, European Data Protection Board and EU Fundamental Rights Agency (FRA) must be involved in the drafting of that handbook, and civil society consulted;
- **Article 79.4** (monitoring and evaluation) says that "eu-LISA and Europol shall have access to the necessary information relating to the data processing operations performed in the router and EPRIS respectively" for the purposes of technical maintenance. It should be clarified that this excludes access to personal data;
- Biometric searches are referred to as de-personalised in the **Explanatory Memorandum** because individuals purportedly cannot be directly identified from the search result (hit/no hit response and reference numbers). This is misleading, as it fails to consider the fact that (sensitive) personal data are processed (about identifiable persons). 'De-personalised' should thus be deleted. On the positive note, de-personalised is an improvement over the current 2008 Council Decision where searches are referred to as 'anonymous' (which is clearly wrong).

In sum, the co-legislators should mitigate the risk that Prüm II will exacerbate the abuse of data, by strengthening the protection of fundamental rights, including through alignment to the LED and by setting rules for the databases which may be connected to Prüm. At its core, the Prüm II proposal fails to introduce any substantive provisions or safeguards which would tackle or even limit these existing problems. Nor does the proposal take any steps which would ensure that abuses, errors and discrimination are reasonably prevented as part of the proposed expansion. Giving law enforcement agencies seamless access to a much vaster array of data is thus seriously premature at best.

> "It appears to be a case of trying to get the police to run, when they currently have problems walking."
>
> - Chris Jones, Director, Statewatch

Summary of recommendations (Section 1)

1. Introduce a new chapter of the Regulation to set minimum procedural criteria for the connection of any system/database to the Prüm II central router, EPRIS or Eucaris (i.e. the Prüm framework). This includes mandating ex ante data protection audits of all connecting systems; harmonised national requirements for due seriousness of a crime to justify inclusion and for categories of persons (convicted person, suspect etc) to be included; harmonised rules for removal from a database; and national definitions of reasonable suspicion. Further details are discussed at length in chapter 1.4;
2. Strengthen the parts of the proposal where data protections are currently insufficient, particularly in Articles 20 and 40 (duration of record-keeping);
3. Clarify the parts of the proposal where data protections are ambiguous or risk conflicting with other legislation such as the LED and the Charter, in particular Article 39.1 (CIR), Articles 51.3 (necessity of processing), 53 (data processors) and 79.4 (maintenance);
4. Delete the potential loophole at the end of Article 51.1 (data protection) which could allow for exchanges of data outside of the Prüm framework; and furthermore delete Article 58.2, which would exempt police officers from discrimination claims - deletion is necessary so that individuals whose rights have been infringed can seek redress;
5. Ensure that the practical handbook accompanying Prüm II (Article 78) must have substantial input from the EDPS, the EDPB, FRA and civil society;
6. Interrogate why court orders are required to remove personal data from a database connected to Prüm II (Article 52) but not to add it, with a view to considering this as an additional safeguard for databases connected to Prüm II; and
7. At a minimum, Prüm II should require independent verification that the biometric data obtained by Europol from third countries concerns a convicted individual or a suspect in a concrete investigation concerning one of the crimes covered by Europol's mandate. However, given the documented abuses of data held by Europol, and the fact that Europol does not have a right of own-initiative investigation, as discussed in Section 1.3, we recommend that access to Europol's third-country biometric data is fully deleted (Article 40) and that Europol not be permitted to conduct searches of Member States' databases.

Section 2: Requirements when limiting fundamental rights

2.1 Fundamental rights law requirements

According to Article 52.1 of the Charter of Fundamental Rights of the European Union, any limitation to fundamental rights must respect the essence of those rights, be necessary and proportionate, and must genuinely meet the objectives that justify the infringement.[44] The burden is on the legislators to prove that this is the case. The LED further requires that limitations to people's right to personal data must be *strictly* necessary. Prüm II must therefore align to this threshold.

> "*When EU law interferes with fundamental rights, EU law must also provide appropriate safeguards*."
>
> - Jesper Lund, Chairman, IT-Political Association of Denmark

As established by the case law of the Court of Justice of the EU, when it has been demonstrated that limitations to rights are justified, any interference with fundamental rights must still be properly circumscribed and have safeguards written into EU law.

We will argue that the Prüm II proposal does not demonstrate the necessity and proportionality of the proposal, nor the strict necessity of its processing of personal data. The proposal interferes with many rights, but does not provide adequate safeguards – leaving them to national laws and discretion, which Section 1 demonstrates puts people's rights seriously at risk.

2.2 Lack of demonstration of necessity and proportionality

As we have argued, there has not been a sufficient assessment of the necessity and proportionality of the 2008 Prüm Decisions.[45] Prüm II does not resolve this concern. Data about the efficiency and effectiveness of Prüm I has never been publicly released, and the public have been asked to rely on claims from law enforcement and the European Commission regarding the supposed benefits of the system.[46] As we have pointed out previously: "The few studies which attempted to collect [relevant] information actually found that less than 10% of hits were used in criminal proceedings and as evidence in courts of law."[47]

> ***Example:*** *A 2018 study for the European Parliament's Civil Liberties (LIBE) Committee found that whilst law enforcement often claim that the cross-border exchange of DNA thanks to Prüm is useful and effective, available figures show that there is actually a "low utility" of the system to get information after a confirmed 'hit'. The study further explains that several innocent persons have been falsely arrested as a result of the poor-quality DNA matches via the Prüm framework, combined with systematic failures to conduct supporting investigatory work and 'disregard for due process'.*[48]

44 "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others," Charter of Fundamental Rights of the European Union, Article 52.1.
45 https://edri.org/our-work/edri-challenges-expansion-of-police-surveillance-via-prum/
46 https://edri.org/wp-content/uploads/2021/03/EDRi_Public_Consultation_Prüm_framework.pdf
47 Ibid, pp.7-8.
48 https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf, pp.8-9 and pp.18-19.

This inability to demonstrate that it can achieve its central objective poses a serious question about whether the Prüm framwork is – in legal terms – necessary. The lack of necessity and proportionality of the expanded categories of data are also major problems that will be explored further in Section 4.

This problem is exacerbated by the fact that the small amount of data that civil society have been able to analyse does not demonstrate any statistically-significant correlation between the number of DNA searches undertaken via the Prüm framework by Member States in 2021, compared to the number of matches that these searches led to.[49] In particular, Austria and Germany's vast number of searches did not lead to a statistically significant increase in matches. This casts doubt on the fundamental premise of Prüm II, namely that the search for criminals requires more searches via Prüm.

It is likewise concerning – given that the objective necessity and proportionality of the Prüm II proposal have not been justified, and that there are open questions about the efficacy and necessity of the centralised system – that the proposed Regulation requires a significant investment. This has been estimated at an additional central cost of 23 million euros, which does not include the 15 new staff members that would also need to be recruited to implement it.[50]

2.3 Legal basis

One of the legal bases of Prüm II is Article 16(2) of the Treaty on the Functioning of the European Union, concerning the protection of personal data. As Prüm II not only fails to better protect but actually weakens protections of personal data, this must be corrected if the proposal is to be legitimate.

The other legal bases of Prüm II are police cooperation (Article 87(2)(a)) and the prevention, detection or prosecution of criminal offences (Article 88(2)), which the proposal limits to the context of serious cross-border crimes. We have concerns, therefore, about the inclusion of identifying missing persons or identifying unknown remains. Whilst missing persons and unknown remains may have links to serious cross-border crimes, there are also many circumstances where they will not. The indiscriminate inclusion of 'missing persons and unidentified human remains' (Article 2) in Prüm II thus lacks a specific legal basis. Its broad scope and lack of specificity also creates serious risks of over-use and abuse.

Such an objective does not seem to be legally necessary, as the EU's SIS II system already permits alerts for missing persons on the basis of fingerprints and even DNA, when fingerprints are not available. As such, the inclusion of missing persons and unknown remains in the Prüm II framework has not been proven to be lawful nor necessary and we recommend that it be removed from the scope of the proposal.

Summary of recommendations (Section 2)

1. Request further analysis from the European Commission of the necessity and proportionality of the Prüm II proposal, including statistics about the effectiveness

49 Analysis based on https://www.statewatch.org/media/3248/eu-council-prum-statistics-2021-5436-22.pdf and available on request.

50 https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1685618&t=e&l=en.

of Prüm I which would support this, to determine the legality of the Prüm framework as well as the novelties introduced in Prüm II;
2. Where elements of the proposal cannot be demonstrated to be necessary and proportionate, they should be deleted from Prüm II. If compliance cannot be demonstrated for critical elements (such as the central router), the proposal should be suspended until proof is provided;
3. Provide safeguards for each justifiable limitation of fundamental rights (particularly rights to data processing as posed by the central model) by implementing data protection safeguards and protections as per the recommendations in Sections 1 and 3;
4. Remove missing persons and unknown remains from the scope of Prüm II (Article 2), which lacks a legal basis and unnecessarily duplicates SIS II.

Section 3: The scale of the problem when you automate and centralise

3.1 Intrinsic limitations of a central model

One of the main goals of Prüm II is to replace current bilateral connections between national databases with two centralised exchanges (the Prüm II central router and the European Police Records Index System, EPRIS) which would connect all relevant national databases. A third type of connection would give Member States automated access to third-country data held by Europol, and Europol automated access to their databases for the purpose of checking third-country data. In the event of a potential match, there will be the fully-automated release of the biometric profile, vehicle data or 'pseudonymised' police record data, followed by the subsequent compulsory release of the core data (name and other biographical information about the person whose profile has matched) or full police record. This is a complicated architecture which is unlikely to be the silver bullet that the Commission seems to expect.

For each category of data exchanged via the central router, EPRIS, or Eucaris, Prüm II requires that the search must be "in compliance with the national law of the requesting member state".[51] This is an intrinsic feature of the centralised model. Of course, the requesting Member State cannot know until after they have conducted their search (i.e. *ex post*) in which country's database the information may be held (if at all). Logically speaking, this seems reasonable.

However, as a result, the centralised model of Prüm II will eliminate the option to introduce safeguards based on the laws of the requested Member State, which is a problem given the tapestry of national protections discussed in Section 1.

> *A **German** citizen, for example, could have data about them treated in a way that does not comply with **German** law, because the search has come from another member state with fewer national data protection safeguards and potentially arbitrary or unfair criteria for conducting searches (which section 1.1 has explored extensively).*

Furthermore, Article 39 allows for simultaneous searches of national databases, Europol data and the Common Identity Repository "in cases where it is likely that data on a suspect, perpetrator or victim of a terrorist offence or other serious criminal offences [...] are stored in the Common Identity Repository", further increasing the scale of these risks. Although we do not explore them in the scope of this paper, we note that the central router could create further issues due the complexity of its architecture, including (non-)transparency of procurement processes, the potential role of commercial entities, and the relevance of the bloc's future rules on artificial intelligence to the router technology.

3.2 The automated exchange of sensitive personal data

Prüm II's ideology of seamless data sharing and 'efficiency' through increased automation poses an existential challenge to some of the tenets of fundamental rights to privacy and data protection. Prüm II enables law enforcement agencies to access people's most sensitive data without putting in place adequate safeguards to ensure that this cannot be done spuriously, arbitrarily or for politically-motivated reasons. It does not put in place sufficient checks for accuracy, to prevent errors, and to ensure other data protection standards are met.

51 DNA data under Art. 6.1; dactyloscopic data under Art. 13.1; vehicle registration data under Art. 18.1; facial images under Art. 22.1; and police records under Art. 26.1.

3.2.1 Biometric searches

In particular (and similarly to the Prüm rules currently in force), Articles 6 and 11 (DNA), 13, 15 and 17 (dacytloscopic data) and 21, 22 and 24 (facial images) allow the automated release (hit/no hit) of the biometric profile (for example fingerprint, DNA profile or facial image), as well as a corresponding reference number. This is done without review – even from the country in which the data are held. The requested Member State thus has no opportunity to assess the necessity or proportionality of a search, nor the accuracy of the held data, before the release of the biometric profile. By definition, personal data will be transferred across borders *before* the confirmation that it matches the search profile is undertaken, which raises concerns about how the proposal complies (or not) with the LED. The same process of *ex post*-only review also applies to vehicle registration data (Article 18).

This is particularly concerning for DNA, dactyloscopic data and facial images, as the profiles that will be returned are not guaranteed to be a match (as biometric matches only meet a certain threshold of statistical likelihood, not absolute certainty). Furthermore, the profiles that are returned are always returned in the form of a 'list' of potential matches (1st most likely match, 2nd most likely match, etc) (Article 37.5). An intrinsic feature of Prüm's hit/no hit exchange is that the sensitive biometric profiles of non-matching persons (i.e. everyone on the list that did not turn out to be the match) will *always* be automatically shared for the purpose of performing a comparison.

Given the issues discussed at length in Section 1, the risks of errors – and therefore illegitimate and potentially unlawfully sharing the data of 'candidates' (Article 13) – is high. The risks to the concerned individual(s) can be severe – for example, detention by police – especially given the previously-discussed procedural issues that have led to false arrests and detention. In the context of the mismanagement of data, the systemic inclusion of non-suspects/non-perpetrators in criminal databases, and concerns about data accuracy (which are especially prevalent in the case of facial images, as we will explore in Section 4), Prüm II could therefore facilitate the illegal automated exchange of sensitive data.

The fact that the proposal requires that reference data "shall not contain any data from which an individual can be directly identified" (Articles 5.2, 12.2, 21.1) does not mitigate this issue, as sensitive personal data is still being automatically processed. In addition, the concept of 'directly identifiable' here is very much misleading; biometric data are, according to the LED, identifiable even without being stored alongside biographical information. In the case of facial images (21.1) the proposal's claim is even more misleading: facial images can be identified by the naked eye in ways that DNA and dactyloscopic data cannot.

3.2.2 Biometric and vehicle registration queries

The procedure for 'Queries' (Article 37) describes the automated release of personal data, along with a complex technical architecture to 'rank' the results from different Member States on the basis of how likely they are to match (37.4). This is a complicated process with risks of bias and opacity (sometimes known as the black-box problem of algorithmic systems), yet the proposal for Prüm II simply states that this will be resolved in an implementing act (37.6). It is overly-optimistic and even potentially dangerous to leave such a complex process fully outside of the legislative process, given the significant risk that the ranking process will pose to fundamental rights. Similar concerns arise for how the central router will interface with Eucaris for searching vehicle records (19.3), although such an interface is presumably less complex.

As the EDPS points out, it is concerning that there is no specific legal basis for the automated exchange of vehicle registration / driving license data in the proposal (Article 19), but rather an

intergovernmental treaty (paragraph 59, EDPS Opinion on Prüm II). We support the recommendations by the EDPS that responsibility for the driving license data processed via Eucaris should be explicitly defined in the proposal, and that the legal basis for this exchange be clarified.

The broad scope of the data that can be exchanged relating to vehicle registration is also concerning, for example: 'data relating to owners or operators' (Article 18.1.a). Article 19.3 states that this will be defined further in an implementing act. This is not sufficient: Prüm II must specify the exact data that can be considered strictly necessary and proportionate for the purpose of investigating serious crimes to ensure that vehicle registration data are not misused to gather disproportionately large volumes of data about individuals.

3.2.2 Police record searches

An equivalent problem to the 'directly-identifiable' issue of biometric profiles also appears in the automated release of indexed information about police records (the equivalent of 'reference data' for police records). The Prüm II proposal calls these data (name, alias, date of birth, nationality/ies, birth location and gender) 'pseudonymised' (Article 25).

However, pseudonymisation does not stop these data from being personal data. Moreover, given that a particular person is being sought, we find it very problematic that the proposal considers the data to be pseudonymised. Pseudonymisation is a process which entails that the data in question are unidentifiable. To the contrary, in the context of Prüm II, these indexed data would be directly identifiable in the event of a 'hit' because they would return data based on the identifiable biographic data submitted in the search. As such, the proposal should clarify that full pseudonymisation is not possible, and that these data remain personal data and should therefore not be exchanged in a fully automated manner.

3.3 Core data, police records and the need for a right of refusal

Under the current Prüm framework, the follow-up exchange of biographical data about the purportedly matching profile after the requesting Member State confirms a 'hit' is undertaken according to mutual legal assistance rules. This means that the requested Member State can apply its national law and refuse certain requests, for example those that would prejudice a national investigation, those where there are concerns about the necessity or proportionality of the search, or where there are concerns that the rights of the individual concerned might be violated.

But under Prüm II, the release of core data after a 'hit' will become mandatory (Article 47) within 24 hours: first and family name, date of birth, nationality/ies, birth location and gender. These data are, of course, personal data. This step will eliminate the very important right of refusal that currently exists for the disclosure of biometric and vehicle registration data.

Article 44.5 and 44.6 '[EPRIS] Queries' (for police records) are more positive from a fundamental rights perspective, requiring a 'reasoned follow-up request' and introducing safeguards which give the requested authority review and discretion over whether to share police records. Article 44.4 further implies that there may be a check on the veracity of a match ('shall indicate the quality of the match'). **Such provisions are important, and we recommend that the ability for Member States to review data prior to exchange should be standard across all data categories, not just police records, and at all stages of the process (including the initial automated search).**

That being said, such checks are not infallible; as the 2018 LIBE study confirmed, some Member

States have previously performed vastly insufficient checks, leading to false arrests of innocent persons. Recital 17 of the proposal also refers to this manual check as "a certain degree of human intervention"; a weak phrasing, which does not give confidence in the level of procedural safeguards to prevent misidentification. This already potentially insufficient protection does not appear in the Articles of the proposal itself. The 24-hour period for review is not only very short, but provides no formal opportunity to object. This is unlikely to meet the requirements under the LED for a 'human in the loop' to prevent fully-automated processing. In the current wording, the human review is meaningless window-dressing and the processing of data functions as if it were fully-automated. **It is vital that Prüm II includes additional provisions to ensure *meaningful* human review when exchanging core data.**

Also problematically, the requesting Member State has a vested interest in finding a match, which can be problematic. In response to these challenges, there should, therefore, be a requirement for a level of robustness of these checks. This could include minimum standards on the number and type/qualifications of persons that must independently review the match, as well as rules on the supporting evidence/investigative actions which must be taken before a match could be considered sufficiently confirmed.

Having rules, restrictions and checks on the sharing of people's most sensitive data must be done according to a very high standard of accuracy as well as due process. These steps might be seen be some as a 'burden' which should be eased. But when people's liberty is at stake, it is essential that shortcuts and technosolutionism are not allowed to prevail over fundamental rights. This protects not only the individuals concerned and the rule of law more broadly, but also the law enforcement or judicial authorities in the event of alleged wrongdoing.

3.3 Individual and mass searches

3.3.1 'Individual' automated searches and the need for due seriousness

Automated searches of data can be undertaken on the basis of 'individual cases' (for DNA data under Art. 6.1; dactyloscopic data under Art. 13.1; vehicle registration data under Art. 18.1; facial images under Art. 22.1; police records under Art. 26.1). This is presented as a safeguard to keep the searches in line with due process and rule of law requirements such as individual suspicion.

However, it is notable that under Art. 4.9, an 'individual case' is defined as "a single investigation file". This suggests that whilst the search will be on the basis of a particular investigation, if the national law of the requesting Member State allows it, there will be nothing preventing the search from including any person with a link to that file. That could include, for example, persons against whom there is *not* reasonable suspicion of, nor a conviction for, having committed a serious crime. As discussed in Section 1, there is evidence of witnesses as well as relatives and partners of victims, who themselves are not linked to the crime, being included in national criminal files and databases. It is essential, therefore, that Article 4.9 (Definition of 'individual case') is amended so that it expressly applies only to individual persons, and not to an entire investigative file, which may also include people who are not suspected or convicted. This means that the automated searches on the basis of 'individual cases' would genuinely apply only to the suspect/ convicted person, and not to other people associated to the case.

It is vital that each search ('query') permitted under Prüm II meets thresholds for due seriousness, which the EDPS notes need to be higher than in the proposal, given the scale of the infringement on individuals' right to data protection. Currently, Articles 6(1) and 26(1) allow the comparison of DNA profiles and police records "for the investigation of criminal offences". Articles 13(1) and 18(1) allow searches of dactyloscopic and vehicle registration "For the prevention, detection and investigation of criminal offences". It should be noted that whilst

Article 22(1) contains equivalent wording in regard to facial images, this is a type of search which we argue must be entirely deleted from Prüm II, as even a "serious crime" threshold would not provide sufficient justification. .

All of these criteria are exceptionally broad, and contradict Prüm II's mandate for tackling *serious* cross-border crime. It is vital, therefore, that Prüm II is amended to explicitly allow searches only in the cases of "serious crime(s)" with evidence of a cross-border nature. As the EDPS reinforces in his Opinion on Prüm II, the processing of biometric data constitutes a serious infringement on the right to data protection and thus needs to be suitably justified. As emerging case law from the CJEU further confirms, only the pursuit of specific objectives relating to *serious* crime can justify an interference with the protection of biometric data.[52]

3.3.2 The risks of mass automated searches

Beyond individual automated searches based on specific investigations, Prüm II (Article 7) allows for the perpetual automated searches of *all* unidentified DNA profiles against all other DNA profiles in the framework. Although Article 5 says that these data cannot be directly identifiable (a term which has little meaning in the context of biometric profiles), this does not stop what in effect constitutes the constant searching of and comparison between sensitive, personally-identifiable genetic (or biometric, according to Prüm II) data on a massive scale.

This mass automated search also flips the principle of individualised, warranted suspicion and targeted investigations on its head, and instead treats every person whose unidentified DNA is in the system as a suspect (which is highly likely to include people without a sufficient basis, as explored extensively in Section 1). This is manifestly disproportionate, violating the essence of the right to the presumption of innocence, and is also unnecessary. It poses a serious risk to rights to privacy, data protection and good administration. As limitations which infringe on the essence of a right are not permissible under the Charter, it is important for the protection of the rights and liberties of the entire EU population (who, given the broadness of Member States' DNA databases, could find themselves unfairly included in such a database),– along with nationals of third countries whose data may be accessible through the Prüm framework, that Article 7 is deleted.

Whilst the proposal reserves mass automated searches to DNA, it is also foreseeable that the Prüm II architecture will establish the technical capability for other categories of data to be searched in an equivalent (i.e. mass, automated) way. This poses a very high risk of enabling forms of biometric mass surveillance.[53] This further emphasises the need to remove this inherently risky form of mass processing, instead explicitly restricting Prüm II to genuinely individual searches. In sum, Article 7 will enable the large-scale automated processing of biometric data in a way that cannot be mitigated with safeguards because it precludes individualised searches. As the processing of unidentified profiles is possible under Article 6, Article 7 is manifestly unnecessary and thus should be deleted.

3.3 Automation safeguards

The automated searching of certain data does not necessitate that the release of profiles needs to be fully automated. In fact, one way in which the safeguards of Prüm II could be improved would be to require the relevant authority in the requested Member State to check and authorise each profile before it is released to the requesting Member State for additional verification for consistency with the LED, meaning that no personal data, not even apparently 'de-personalised' or 'pseudonymised' data (both terms which we contest) can be exchanged in a fully-automated

52 See footnote 37 on CJEU case C-205/21.
53 See, for example, https://edri.org/our-work/blog-ban-biometric-mass-surveillance/.

manner.

In an attempt to introduce safeguards, Prüm II states that exchanges must be done in accordance with "the procedure referred to in **Article 76(2)" (comitology requirements)**, meaning that technical standards will be further developed. These rules, however, can and should only help to set the technical elements of exchange. It is vital that any political and fundamental rights-based requirements are established in Prüm II directly, as part of democratic scrutiny of the proposal, so that the implementing act(s) can further specify only those elements that are genuinely technical.

To address the risks raised by the automated access to reference data and to set conditions for the implementing acts, we therefore recommend that:

- **Types of crime:** Prüm II should expressly restrict all searches (Articles 6(1), 13(1), 18(1) and 26(1)) to "the investigation of **serious criminal offences**" in line with Prüm II's purpose; 22(1) (facial images) should be deleted entirely (as the next chapter will discuss). Article 2 should clarify that the purpose is "the exchange of information between authorities responsible for the prevention, detection of criminal offences **for the purpose of the prevention or detection of serious crimes**." Anywhere else in the proposal which discusses the crimes for which a search can be undertaken or a database connected should also be limited to "serious" criminal offences;
- **Genuinely individual searches**: mass searches should be deleted, and searches should be ring-fenced to ensure that they are genuinely individual;
- **Human discretion and right of refusal to share data**: It is important to recognise that automated biometric, vehicle registration and police records searches would entail the near-instant transfer of personal data across borders, and therefore that extra safeguards are needed. We suggest potential measures which could mitigate this, including:
    - Deleting the automated release of biometric reference data in Articles 6 and 11 (DNA), 13, 15 and 17 (dacytloscopic data) and 18 (vehicle registration), and replacing it with an automated notification to the requested Member State that data they hold have been matched in a search. This would then trigger a *mandatory* human review of the accuracy and veracity of the profile, as well as the legitimacy of the request by the requested Member State, prior to confirming the hit/no-hit (by releasing reference data). This would complement (not replace) the subsequent confirmation of a match by the requesting Member State ahead of the exchange of core data;
        - Note that we do not include recommendations for removing the automated release of facial images because we believe that facial images must be entirely removed from the scope of Prüm II as they pose such a severe risk that it cannot be mitigated sufficiently through safeguards (see next section);
    - Introduce a right for the requested Member State to refuse to return biometric reference or vehicle registration data following the initial purported match;
    - Require a formal reasoned follow up request to be submitted to the requested Member State by the requesting Member State before any core data are shared;
    - Introduce a right for the requested Member State to refuse to return any core data, as well as police records, as per current mutual legal assistance rules to ensure meaningful human intervention (essentially making the release of core data and police records non-mandatory);
- **DNA**: Article 11(3) requires that automated comparisons of DNA data must meet a minimum number of loci. However, current Prüm rules allow a very low threshold for this (6-7 loci), generating a high risk of false-positive matches, especially given the size of the databases being searched, which will only increase as the architecture is centralised.[54] Articles 11(3) and 76(2) should therefore specify that the number of loci must be

54 https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

independently verified to ensure the threshold is sufficiently high to ensure accuracy and reasonably minimise the risk of misidentification;

- **Procedural and technical**: the proposal should set criteria for the Implementing Acts to elaborate on, for example:
  - Place requirements on the requesting Member State to ensure that they have corroborating evidence before arresting or detaining an individual, meaning that such actions cannot be pursued solely on the basis of a purported match via Prüm;
  - Consider restricting the number of potential matches ('candidates') that can be returned on the basis of a biometric searches;
  - Establish standards for the number of persons who should check a decision before it is confirmed, as well as any requirements for independent verification and/or review;
- **Vehicle registration data**: conditions for searching Eucaris for driving license / vehicle registration data must be sufficiently defined and safeguarded, as they are currently not specified in the proposal;
- **Transparency**: to ensure transparency, we recommend additional provisions in Prüm II to require the public disclosure of which national and Europol databases are connected to the framework, and any relevant controllers and processors.

Summary of recommendations (Section 3)

1. Expressly restrict all searches (Articles 6(1), 13(1), 18(1) and 26(1)) to "the investigation of **serious** criminal offences" where the offence has a specific cross-border nature, in line with Prüm II's purpose. Article 2 should confirm that the purpose of the Regulation is "the exchange of information between authorities responsible for the prevention, detection of criminal offences **for the purpose of the prevention or detection of serious cross-border crimes**."
2. Require checks of accuracy and veracity of biometric profiles prior to their release by the requested Member State, in addition to the requirement for confirmation of the match by the requesting Member State;
3. Introduce a right of refusal so that the requested Member State has the possibility to decline a request to share core data or police records, and only allow these data to be released following a specific, reasoned follow-up request;
4. Request an impact assessment to demonstrate the necessity and proportionality of the central router, especially given the additional costs compared to the currently-functioning bilateral system;
5. Improve the wording of Articles that could create ambiguity leading to a lowering of protection, in particular Article 4(9) (clarifying what constitutes an individual case);
6. Require human checks prior to the sharing of reference biometric data (Articles 11, DNA and 13, dactyloscopic data, respectively);
7. Delete Article 7 (mass automated searches) as well as deleting Europol's access in Articles 6.1 (automated access to DNA databases) and 13.1 (automated access to dactyloscopic databases), both of which fail to meet the legal test of necessity;
8. Set clear requirements which can then be standardised via Implementing Acts, including on the number and loci of searches, on the ranking process of the central router (Article 37)
9. Introduce procedural measures to ensure that matches cannot be used as the sole basis for arresting or detaining persons;
10. Better define requirements for vehicle registration data, including limiting which data may be shared (Article 18); and
11. Require easily-accessible public disclosure of all databases, and the relevant controllers and processors, that are connected to the Prüm framework.

Section 4. Serious risks created by new data categories

4.1 Facial images

The Prüm II proposal seeks to add facial images to the Prüm framework without considering the specific fundamental rights risks of the processing of facial images, nor considering the severe risk of enabling and even incentivising mass surveillance by facial recognition. The current inconsistencies in the rules and operation of national facial image databases across Europe illustrates the risk (discussed at length in Section 2) of people in different countries enjoying different levels of rights protections due to a lack of harmonised procedures.

> A *freedom of information access* (FOIA) request made in 2021 by Chloé Berthélémy, Policy Advisor at EDRi, shows that of the 11 Member States who operated facial images databases for law enforcement at that time, not one had the same criteria for inclusion as any of the others. Some of the most concerning categories of included persons include any civil document applicant (Hungary) and asylum seekers (Finland, Germany, Italy and the Netherlands).[55] It is also clear that in at least some countries, persons are included in those databases despite not fitting any of the official categories. In Slovenia, for example, facial images have been scraped from the web and added to the database.[56]

Whilst Prüm II considers facial images to be biometric data, under national rules according to the LED, facial images only become biometric data when they undergo specific technical processing (usually interpreted as meaning the creation of biometric templates). This means that national facial image databases may not offer the protections that they would if they were processing biometric templates. However, the intention of Prüm II is to use the facial images to perform facial recognition, meaning that in effect, Prüm II might allow law enforcement agencies to derive biometric templates from information that has been collected without the protections required for biometric data. This further demonstrates the fundamentally unsuitable nature of facial images within the Prüm framework.

As discussed in Section 2, the European Commission, as the institution proposing Prüm II, must bear the burden of demonstrating its necessity and proportionality. We do not believe that the necessity of the expansion to facial images has been justified especially given the wide range of data already available under Prüm II.

On the question of proportionality, we have even greater concerns. The processing of facial images poses an especially pronounced risk to a wide range of fundamental rights, including potentially the essence of several rights (dignity, non-discrimination, privacy). The potential for generalised surveillance is severe, and the risk of misuse high. As the European Economic and Social Committee notes "with great anxiety" in its Opinion on Prüm II, the proposed expansion of facial recognition in the context is even more alarming given the Russian invasion of Ukraine, leading the EESC to also question the necessity and proportionality of adding facial images.[57] In the context of artificial intelligence, the European Parliament has already warned about the risks arising from law enforcement uses of facial recognition, calling to prohibit uses which would constitute biometric mass surveillance.[58]

55 The details about and results of the FOIA are available at https://www.asktheeu.org/en/request/commission_technical_workshops_o. See Appendix 1.
56 https://www.primorske.si/2012/04/18/spanski-kljuc-resitve-posilstva.
57 https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/security-union-packageschengen-package, in particular paragraphs 3.2.2 and 3.2.5.
58 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

Facial recognition is notoriously error-prone and unreliable, exacerbates discrimination, has led to several high-profile false arrests, and – as a statistical prediction – will never provide a conclusive match. Therefore, beyond the pronounced fundamental rights risks, it seems unlikely that the expansion to facial images can be successful in achieving the objectives of fighting cross-border crime or identifying missing persons or unidentified remains, further undermining the necessity of this expansion.

4.1.1 Incentivising the creation of at least 9 new national facial image databases

According to the Explanatory Memorandum of the proposal, "The automated exchange of additional data categories, such as **facial images** and police records, is crucial for effective criminal investigations and for identifying criminals. **The introduction of these additional data categories would not lead to storing new categories of data** as Member States already collect them under national law and store them in national databases" [our emphasis in bold].

The financial assessment which accompanies the proposal reveals that the reality is, in fact, the opposite of what is stated in the Explanatory Memorandum. 13 EU Member States do not currently have national facial image databases. As of 2020, 9 of these had no own-initiative plans to do so.[59] Prüm II will put force such plans on them: firstly, the proposal makes the connection of facial image databases mandatory for participation in Prüm II (Article 21.1) and supports this financially from the EU's general budget (Article 72). Secondly, Prüm II will mean that these national databases must be searchable by the central router, entailing that facial recognition software must be in use for all these national databases, even in cases where it is not currently.

Building on the issues of increased automation as discussed extensively in Section 3 (automation), there are particular issues raised in the context of the accuracy of facial recognition which further challenge the legitimacy of this category of data. Under the automatic search of facial images in Articles 22.2 and 24, the requesting member state automatically receives a list of "matches concerning likely candidates". By definition, this means processing and sharing the sensitive personal data of several persons that are not the suspect.

We know that facial recognition systems are notoriously poor at recognising racialised people, women, and people with certain disabilities.[60] Such individuals are therefore at a disproportionately increased risk of misidentification, and therefore false accusation. As Article 37.5 establishes that searches for *all* biometric data would return "a list" and "scores" of potential matches, this risk can also apply in the case of DNA and dactyloscopic data (which also suffer from issues of biased misidentification, including on the basis of skin colour or limb difference).

The example of 'Mr H' in Lyon, France in 2019 showed that a racialised man was convicted of theft solely on the basis of a facial recognition match, selected from a list of 200 potential 'candidate' matches. The potential for inaccuracy and false convictions is thus enormous, and the scale of the processing of sensitive data of persons that are not the suspect enormous. Mr H is now appealing his conviction and his lawyer has raised serious accusations of due process and fundamental rights violations.[61]

Prüm II tries to safeguard against the risk of biased misidentification by requiring matches to be confirmed by the requesting Member State (Article 22.2). It is a fallacy that human review can mitigate against such biases in the case of facial recognition. In a well-known case in the US,

59 https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf, p.10.
60 https://edri.org/our-work/blog-ban-biometric-mass-surveillance/
61 https://korii.slate.fr/et-caetera/justice-lyon-banbanaste-reconnaissance-faciale-proces-photo-algorithme-preuve

police officers searching for a suspect that they thought looked a bit like actor Woody Harrelson ran an image of Woody Harrelson through their facial recognition system, found a match, and arrested that person based only on their resemblance to the actor.[62]

The socio-technical phenomenon of automation bias makes it more likely that law enforcement agents will defer to machine decisions, finding it psychologically hard to justify overriding what a facial recognition system has 'said'.[63] It is important, therefore, to problematise the idea of a 'confirmed match' (Article 22.2), given that 'confirmed match' in the context of Prüm II does not mean that the suspect or convicted person has been conclusively identified.

Another phenomenon, this time mathematical, is also important here. The so-called 'base rate fallacy' is a statistical analysis which demonstrates that even a close to 100% accurate facial recognition system will always suffer from not just false positives (people who are incorrectly identified as being the wanted person) but also false negatives (people who the system thinks are not wanted, despite them actually being the relevant suspected or convicted person).[64] While false positives can lead to discrimination, arbitrary detention and other risks to civil liberties, false negatives can pose a risk to security and justice. This is because if facial recognition systems are relied on too heavily, the existence of false negatives means that those persons will be falsely discounted because the system fails to make the correct match.

Moreover, a 2020 study funded by the European Commission shows that just one member state – Latvia - has specific protections for the use of facial images in criminal proceedings.[65] "It appears," the report says, "that other EU Member States have different approaches towards law-making [regarding facial images] [...] Special law only on facial images collection, use or processing as per se for the purpose of law enforcement does not exist" (p.8). The idea that Prüm II would facilitate the exchange of facial images in the almost total absence of national protections for the use of facial images in criminal proceedings means that cross-border exchange of these data will happen with no control over which images will be entered into the databases. The report continues with the chilling warning that:

> "In most cases, Member States' laws allow use of personal data, including facial images, that has been collected for other (civil) purposes in offence proceedings. [...] The topic has been left in the hands of Member States and their national courts until it gets challenged before the CJEU."[66]

This would constitute a de-facto get-out-free from rules such as the Law Enforcement Directive which are designed to provide appropriate data protections in the context of law enforcement. Facial images collected for civil purposes will end up as part of the Prüm system, the concomitant serious risk of harm even further compounded by issues of inaccuracy, poor quality data, discriminatory and political policing, and so forth.

As such, we do not see any safeguards that can mitigate the severe risks posed by an expansion of the Prüm framework to include facial images. Articles 22-24, and any subsequent references to facial images, must be entirely deleted.

62 https://www.flawedfacedata.com/

63 For example, a report on the use of automated facial recognition technology by the UK's Metropolitan Police found that there was a "presumption to intervene" when the system in use detected a match between an image on a police list and an individual in the street. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

64 https://edri.org/our-work/why-eu-passenger-surveillance-fails-its-purpose/

65 https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf

66 https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf, page 18.

4.2 Police records

Prüm II defines police records (Article 4.16) as "any information available in the national register or registers recording data of competent authorities, for the prevention, detection and investigation of criminal offences". Notwithstanding the limitations imposed by Article 25.1 (in which the proposal refers to "suspects and criminals"), the extremely broad scope of this provision ("any information available") indicates that information that is inaccurate or unverified may be made available for cross-border searches and exchange. Given the aforementioned issues of data quality as well as discrimination, such a wide scope poses a serious risk to fundamental rights.

Under Prüm II, the exchange of police records will be voluntary. However, to be able to search police records held in another country, a participating country must allow their police records to be searchable (principle of reciprocity, Recital 12). In this way, the exchange of police records may not be considered genuinely voluntary, but rather heavily incentivised.

As with other parts of the proposal, the necessity and proportionality of the inclusion of police records in Prüm II has not been demonstrated. As the EDPS points out, as criminal records can already be shared via the European Criminal Records Information System (ECRIS), it is difficult to see how it could be considered necessary to also share police records, especially given the discretion and ambiguity that are an intrinsic part of police records, as well as the fact that – unlike criminal records – there is no judicial oversight of police records (EDPS, para 42).[67]

The idea of exchanging police investigative files among European authorities is not new. It has been repeatedly brought back on the security agenda of the EU, especially in the aftermath of mass protests in the context of international summits like the G8 in Heiligendamm in 2007 and the G20 in Hamburg in 2017. In 2007, the German government tested the waters for such exchange system during a Police Chiefs meeting at the Council of the EU, following the protests. The origin of the introduction of police records within the scope of Prüm II can be traced back to the pilot project called "Automation of Data Exchange Processes (ADEP)/European Police Records Index System (EPRIS)" launched in 2017 by France, Germany, Finland, Spain, and Ireland with the participation of Europol and supported by the European Commission. This long-standing desire on the part of police forces and interior ministries, however, does not make the proposal necessary or proportionate.

Police records should only remain in the scope of Prüm II if they are proven to be strictly necessary in addition to ECRIS, about which we are sceptical. If they remain in scope, we recommend, at a minimum, an explicit, narrow definition of "police record" to ensure that biased information does not prejudice the presumption of innocence of suspects. In particular, this should mean only information that has been officially recorded (e.g. via a court or independent administrative authority) can be shared.

4.3 National driving license databases

The Council's position would mandate the connection of **data about all driving licence holders** – both biographical data and facial images. This raises equally profound necessity, proportionality and mass surveillance concerns as the connection of national facial image databases, and also introduces a backdoor by which the sharing of not just the facial images of convicted persons – but rather of the entire driving population – would be included.

67 The Commission's own study of ECRIS in 2012 concluded that this functionality was already sufficiently covered in other systems, further demonstrating the lack of necessity of the expansion of Prüm to include police records: https://digit.site36.net/2020/12/18/query-on-suspicion-german-eu-council-presidency-wants-criminal-records-index/

Member states pushed hard for the Commission to include driving licence data as part of its proposal for Prüm II, but their efforts were rebuffed. The Commission concluded that doing so would respect the principle of necessity, but not that of proportionality, recognising that "the measure concerns the processing of data of a large share of the population."[68]

Nevertheless, the member states, inserted new provisions on the exchange of driving licence data into the Council's general approach (Article 20a):[69]

> *1. For the prevention, detection and investigation of criminal offences, Member States shall allow national contact points of other Member States and Europol access to driving licence data to conduct automated searches in individual cases. Member States may allow access to facial images as part of driving licence data, if available.*
>
> *2. Searches may be conducted only with the driving licence number or, if authorised by the national law of the requested Member State, with data relating to the driving licence holder (first name(s), family name(s), place and date of birth).*
>
> *3. Searches may be conducted only in compliance with the national law of the requesting Member State.*

A previous version of the text circulated in the Council by the Presidency replaced the third paragraph with the following, but this was not maintained:

> *"Searches may be conducted only in respect of the same guarantees and safeguards that are required for similar searches at national level, and after a prior search has been conducted in the national driving licence database."*[70]

While driving licence data will certainly be more accurate than that gathered from CCTV footage or through other means by the police, making it generally available for policing purposes raises a more profound problem: it transforms data collected for civil, administrative purposes into a policing tool, and effectively places all driving licence holders into a "perpetual line-up".[71] As Carole McCartney, a law professor at Northumbria University, told *Politico Europe*:

> "*What you're saying is, for me to own a car and to drive, I have to submit that my photo and information is going to be used for policing purposes across the entire EU... Are we all walking around as citizens? Or are we all walking around as suspects?"*[72]

Given that the purpose of Prüm II is to tackle serious crime, it is clear that the mere fact of holding a driving license would not reach the necessarythreshold for having one's data accessible via the system. **As such, it is essential for the protection of the rights and freedoms of a very high number of people that any attempts to add driving license databases to Prüm II is firmly rejected.**

Expanding the Prüm framework to include facial images, the data of all driving license holders, or police records (in the current overly-broad formulation) will fundamentally violate the

68 'Policy option 2.3: introducing the exchange of driving licence data in the Prüm framework' in European Commission, 'Impact assessment', SWD(2021) 378 final, 8 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0378

69 https://data.consilium.europa.eu/doc/document/ST-9544-2022-INIT/x/pdf

70 Council doc. 8020/22, available here: 'EU: Policing: France proposes massive EU-wide DNA sweep, automated exchange of facial images', Statewatch, 13 April 2022, https://www.statewatch.org/news/2022/april/eu-policing-france-proposes-massive-eu-wide-dna-sweep-automated-exchange-of-facial-images/

71 https://www.perpetuallineup.org/

72 https://www.politico.eu/article/eu-police-facial-recognition-surveillance-report/

commitment in Recital 6 of the proposal that: "The processing of personal data and the exchange of personal data for the purposes of this Regulation should not result in discrimination against persons on any grounds. It should fully respect human dignity and integrity and other fundamental rights, including the right to respect for one's private life and to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union."

Summary of recommendations (Section 4)

1. Delete facial images entirely from the scope of Prüm II, as such an expansion is unnecessary, disproportionate and has poses severe fundamental rights risks;
2. Assess the necessity of the exchange of police records given the current functioning of ECRIS. If it is proven that including police records within Prum II is justified, then the proposal should limit the forms of police records that may be shared under Prüm II to only information that has been officially recorded by a judicial or administrative authority;
3. Reject any proposal to add driving license databases to the scope of Prüm II, which would place vast numbers of citizens and residents in a perpetual criminal line-up and treating them as guilty until proven innocent.

Section 5. Other issues

5.1 Procedural deficits

The original Prüm decisions (2008) were passed into EU legislation on the basis of a 2005 intergovernmental treaty, in a dangerous democratic deficit. Rather than following the ordinary legislative procedure or another method of co-decision, the Prüm decisions were a pair of decisions issued by the Council of the EU, which were fast-tracked into EU law with minimal opportunities for scrutiny by the European Parliament.

Rather than addressing or fixing this lack of legitimacy, the proposal for Prüm II further entrenches the dominance of the Council in setting the agenda. A **2021 access to documents request submitted by EDRi shows that the proposal was driven by Member States' desires for an expanded data-sharing regime, rather than on evidence or assessment of deficits of the current regime or the necessity of a new regime**.[73] The Commission did not follow its own principles for better regulation, and instead allowed the Council to set the agenda, whilst – as the access to documents request shows - scrabbling for evidence that could support what had already been decided by the Council.

5.2 Interoperability issues

As discussed at various points throughout this paper, the many risks raised are frequently compounded by the fact that searches can be made of different systems simultaneously. In particular, this proposed simultaneous connection to the Common Identity Repository (CIR) (Article 39) will have a disproportionate impact on foreign nationals. Almost all foreign nationals who are or have been present in the EU will have their data held in the CIR, which will be connected to the central router and searched any time an official with access rights to the CIR makes a search in Prüm. Furthermore, the ongoing expansion of centralised EU migration databases means that data on some EU citizens will also be held in CIR, thus potentially exposing them to a disproportionate level of surveillance.[74]

This provision appears to lower the threshold for searches included in the interoperability legislation, which requires "reasonable grounds" and "suspicion" rather than simply an idea that it is "likely" that relevant data is held in the CIR.[75] The wording should, at the very least, match that in the interoperability rules, or the Prüm II proposal risks creating a loophole around whether or not the "relevant conditions" under Union law (Article 39.1) have been fulfilled for such searches to take place. It may also be remarked that the introduction of simultaneous searches of Prüm and the CIR will further fuel the over-representation of foreign nationals in law enforcement investigations, given that the CIR will only hold data on foreign nationals.

73 https://www.asktheeu.org/en/request/commission_technical_workshops_o

74 According to Prof. Niovi Vavoula '[under the Interoperability Regulations] personal data [of EU citizens] will also be processed in an incremental manner, for example, by the law enforcement branch of the SIS II; by the VIS, as regards sponsors or family members of visa applicants'. In https://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/. As explained further in the following report by Statewatch, data on EU and third-country dual nationals stored in the ECRIS-TCN will be held in the CIR: https://www.statewatch.org/news/2019/january/eu-inclusion-of-dual-nationals-in-new-criminal-records-database-incompatible-with-the-right-to-non-discrimination/.

75 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

Summary of recommendations (Section 5)

1. Ensure that the European Parliament is enabled to exercise its role of democratic scrutiny according to the Ordinary Legislative Procedure set in Article 289 TFEU;
2. Ensure that CIR searches require "reasonable grounds" of "suspicion" in line with interoperability rules.

Appendix 1

Excerpt from EDRi's freedom of information access request (2021) (https://www.asktheeu.org/en/request/commission_technical_workshops_o):

EU Member State	Year of impl.	Database	No. of images	No. of persons	Person categories
Austria	2020	EDE - Criminal identification database	1.25 M	620 000	criminals
Finland	2020	RETU - registered persons identifying features database and Aliens database			suspects, asylum seekers and aliens
France	2013	TAJ - criminal case history database	6 M	21 M	suspects and victims (i.e. unknown dead bodies, seriously injured and missing persons)
Germany	2008	INPOL - criminal case management system	5.5 M	6.2 M	suspects, convicts, arrestees, missing persons, wanted persons and asylum seekers
Greece	2019	mugshot database	Not specified	377 000	suspects who have been arrested and convicts who have been sentenced to imprisonment
Hungary	2016	Facial Image Registry	30 M	Not specified	civil document applicants
Italy	2017	AFIS	17 M	9 M	convicts, arrested suspects, unidentified persons, immigrants and asylum seekers
Lithuania	2019	HDR - Habitoscopic Data Register	400 000	185 000	suspects, convicts, arrested persons, wanted persons, unidentified dead bodies and unidentified helpless persons
Latvia	2012	BDAS - Biometric Data Processing System (criminal data array)	Not specified	Not specified	detained, suspected, accused and convicted individuals, and unidentified dead bodies
Netherlands	2016	CATCH criminal and CATCH alien	Not specified	8.3 M	suspects, convicts, visa and asylum applicants
Slovenia	2015	the record of photographed persons	Not specified	110 000	suspects, missing persons and unidentified dead bodies

Operational