06.10.2020

Feedback to the Roadmap to strengthen the automated data exchange under the Prüm framework

European Digital Rights (EDRi) is an association representing 44 human rights organisations from across Europe that defend rights and freedoms in the digital environment. We welcome this opportunity to provide feedback on the future developments of the Prüm framework. This submission has been developed with the expertise of our member IT-Pol Denmark.

I. Summary

The Inception Impact Assessment related to the existing framework of the Prüm Decisions published on 11 August 2020 shares the European Commission's plans to further expand the scope of automated exchanges of personal data between national law enforcement authorities in the EU without properly evaluating the compliance of Prüm with EU law, notably the EU Charter of Fundamental Rights. In response to the Commission's consultation call, EDRi would like to provide the following response:

- We recommend that the European Commission includes the European Parliament in the first phases of the evaluation process and takes into due account its opinion when defining the future political orientations of the Prüm framework.
- We encourage the European Commission to properly evaluate (with significant evidence) the Prüm framework against the principles of necessity and proportionality before expanding its scope.
- We strongly recommend the European Commission to conduct a thorough assessment of all Member States' transpositions of the Law Enforcement Directive (LED) in connection with the upcoming evaluation of the Prüm framework. EDRi recommends to align the Prüm framework with the current data protection rules for law enforcement.
- EDRi urges the European Commission to launch an EU-wide, truly democratic debate on facial recognition and refrain from imposing it through the Prüm framework.
- EDRi strongly opposes the extension of the Prüm framework with facial images in Member States' criminal investigation databases.
- EDRi opposes the automated disclosure of hit-follow-up data as this would be likely problematic in regards to the Law Enforcement Directive requirements. EDRi calls for a mandatory manual review by the requested Member State to ensure that all legal safeguards are guaranteed, the requested personal data is accurate and the request is proportionate and necessary. Refusal grounds should always be available to the requested Member State.
- EDRi encourages the European Commission to speed up the hit-follow-up process by improving the efficiency of the administrative process (e.g. by ensuring that Member States allocate sufficient resources for police and judicial cooperation).
- EDRi opposes the inclusion of Europol data into the Prüm exchange system.

II. Introduction

The Prüm Decisions require Member States to make their DNA, dactyloscopic (fingerprint) and vehicle registration data (VRD) databases available for automated searches on a hit/no-hit basis by law enforcement authorities in other Member States.

As any information exchange involving personal data between law enforcement authorities in the EU, the Prüm framework can lead to several violations of fundamental rights including the right to data protection, to private life and to non-discrimination.

There is very little democratic control and scrutiny over the use and development of police databases in Europe. Citizens learn every day that new technologies are being used by police forces with neither public knowledge[1] about it nor democratic debate[2] – let alone legal basis.[3] In a context where law enforcement authorities are subject to legitimate criticism and questioning for their systemic abuse of power, and notably cases of racist overpolicing and disproportionate targeting of marginalised communities, the review of the Prüm framework should assess and address the issue of structural discrimination against people whose data is held in these databases.

Beyond the review of the compliance of the Prüm automated data exchange mechanisms with fundamental rights and other legal requirements, the EU should also put into question the endless collection of people's data for law enforcement purposes that leads to a data-driven mass surveillance system.

We have the opportunity to hold this important debate this time. Originally, the Prüm instrument was an international convention between seven EU Member States, before its integration into the EU legal framework in 2008. Because the Lisbon Treaty did not enter into force before 2009, the European Parliament never had the opportunity to have a say in the decision over the Prüm rules. As a result, the initiative never benefited from genuine democratic oversight and judicial control (by the Court of Justice of the European Union) and crucially lacks in democratic legitimacy.[4] **The European Commission should ensure that the European Parliament is fully included in the first phases of the evaluation process and its opinion is taken into due account when defining the future political orientations of the framework, not left with only the technical details to debate on.**

[1] The case of Clearview AI is iconic in this regard: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[2] In the UK, a majority of the public wants restrictions on facial recognition technology: https://www.statewatch.org/news/2019/september/uk-court-rules-police-use-of-facial-recognition-is-legal-survey-finds-majority-of-public-want-restrictions-on-the-technology/

[3] Our observer La Quadrature du Net recently filed a complaint against provisions of the French code of criminal procedure which authorises the use of facial recognition to identify people registered in a criminal record police file. Learn more here: https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

[4] As pointed out by the EDPS already in 2007: https://edps.europa.eu/sites/edp/files/publication/07-04-04_crossborder_cooperation_en.pdf (p.4)

III. Main remarks

1. The Prüm framework needs to be properly evaluated against the principles of necessity and proportionality before expanding its scope

When arguing for the expansion of an instrument like Prüm, that can lead to severe fundamental rights restrictions, it is reasonable to expect more than the simple argument that police officers find Prüm "useful". Yet, what we often receive is the reporting of anecdotal evidence brought by investigators. The IIA peremptorily assures us that the Prüm framework "has helped to solve many crimes in Europe". However, there is a crucial lack of publicly available and accurate data about the impact of Prüm. In absence of such statistical analysis, it is therefore difficult to assess its contribution to our criminal justice systems in the EU.

In particular, the number of hits provided by Member States does not prove the value of the instrument. Having X number of hits does not mean having X number of crimes solved. What would be useful to know is how many of these hits led to convictions. The few studies which attempted to collect that information actually found that less than 10% of hits were used in criminal proceedings and as evidence in courts of law.[5]

In this context, it is impossible to know whether Prüm is in line with the principle of necessity and proportionality as required by the EU Charter of Fundamental Rights. It might be important to recall that Prüm implies regular exchanges of potentially sensitive and private information. **It is therefore very important that the benefits of the system to society and to the criminal justice systems are clarified as soon as possible.**

2. The implementation of the 2016/680 Directive by Member States must be thoroughly evaluated in connection with the Prüm evaluation

Most of the processing of personal data in the Prüm framework is based on Member States' national law. The automated searches in the Prüm framework are conducted in accordance with the national law of the requesting Member State, whereas the exchange of personal data in the follow-up procedure after a hit is governed solely by the national law of the requested Member State, including legal assistance rules. Even though the automated search only returns reference data in case of a hit, the search nonetheless involves processing of personal data in both the requesting and the requested Member State. The automated response could form the basis for intrusive measures taken against an individual in the requesting Member States, for example detention in case of a hit.

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

[5] Dr. Victor TOOM, "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

protection provisions in Chapter 6 of Council Decision 2008/615/JHA.

Member States' national law determine the criteria for inclusion in biometric (DNA and dactyloscopic) databases, the retention of personal data in biometrics databases (for suspects and convicted offenders, respectively), and the rules for searching biometric databases. The lack of proper EU-wide standards for data accuracy of biometric databases and searches becomes very problematic when national databases are made available for searches by other Member States. For example, the Prüm Decisions allow DNA matches based on six loci[6], which creates an unacceptable high risk of false-positive matches, especially when the search is made in a large DNA database.

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

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

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

It is of utmost importance that this assessment is made before new forms of biometrics, in particular facial recognition, are considered in the Prüm framework.

[6] The locus is a specific, fixed position on a chromosome where a particular gene or genetic marker is located. When trying to match a particular DNA trace against a DNA database, loci are compared to find the highest comparability possible. The Prüm framework defines a "hit" as matches on at least six loci, which with the current size of DNA databases creates a high risk of false-positive matches and which can lead to wrongful incrimination. According to forensics experts, the probability of a true match is only 40% with six loci, see Toom, V., Granja, R., and Ludwig, A. "The Prüm Decisions as an Aspirational regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data", Forensic Science International: Genetics, 2019 (41), 50–57 https://doi.org/10.1016/j.fsigen.2019.03.023

3. The European Commission should organise an EU-wide, truly democratic debate on facial recognition and refrain from imposing it through the Prüm framework

Facial recognition is arguably the most intrusive and privacy-invasive form of biometric identification. The technology can be used for remote identification without the knowledge of the individual. As cameras in public spaces, along with pictures posted on social media, have become ubiquitous, facial recognition creates an imminent risk of mass surveillance that seems largely impossible to control.

Besides the issue of mass surveillance, facial recognition technology in its current state has significantly higher error rates for racialised minority groups. These groups are already subject to higher scrutiny in policing and risk of discrimination to the extent of the Fundamental Rights Agency (FRA) having to produce guidelines against unlawful profiling.[7] Introducing facial recognition technology with its greater risk of false-positive identification for minority ethnic groups can only serve to exacerbate the already serious problems of discrimination affecting these communities and potential uses against activists, human rights defenders and trade unions.

In Europe and the United States, there is an ongoing substantial public discussion about the controversies of facial recognition technologies. There, we find calls for banning the technology, as some cities in the United States have done, or at least imposing a moratorium on its use. In the United States, IBM, Amazon and Microsoft have unilaterally imposed a moratorium on their sale of facial recognition technology to law enforcement. In the White Paper on Artificial Intelligence,[8] the European Commission recognised the dangers of facial recognition for fundamental rights, and emphasised the requirements of strict necessity as well as appropriate safeguards in the LED for using facial recognition. The European Commission also highlighted the importance of a broad European debate on the circumstances, if any, which might justify the use of facial recognition.

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

[7] Towards More Effective Policing, Understanding and preventing discriminatory ethnic profiling: A guide, Fundamental Rights Agency, October 2010 https://fra.europa.eu/en/publication/2010/towards-more-effective-policing-understanding-and-preventing-discriminatory-ethnic

[8] WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:65:FIN

EDRi urges the European Commission to refrain from imposing facial recognition through the Prüm framework. Introduction of facial recognition in law enforcement through EU-level initiatives requires a wider public debate for which the Prüm framework is ill-suited. EDRi is also of the opinion that this public debate about acceptable uses of facial recognition should not take place until the current problems with discrimination against ethnic minorities associated with facial recognition have been resolved at the technical level.

Although the envisaged use of facial recognition technology in the Prüm framework is admittedly less intrusive and problematic than live facial recognition in large public spaces, there are still substantial risks for fundamental rights, in particular the clear risk of illegal discrimination based on ethnicity. Facial recognition technology could also lead to a greater interest by law enforcement in using recordings from surveillance cameras in criminal investigations since video images can be analysed automatically for possible matches against police databases of facial images. If this type of investigation is done systematically, the level of intrusiveness could potentially approach that of live facial recognition.

IV. IIA Objectives and policy options

1. Speed up and streamline the hit-follow-up exchange process

Information exchange between law enforcement authorities in EU Member States without strong safeguards, redress mechanisms and transparency of the practices can have tremendously negative effects on the fundamental rights of the individuals whose personal data is transferred to authorities in other Member States.

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

The Prüm framework is primarily designed for automated checks of whether information about an individual exists in law enforcement databases of other Member States. The search in biometric databases of other Member States follows the legal rules of the requesting Member State, but any information exchange in addition to the automated hit/no-hit response ("supply of further personal data") must take place in accordance with the national law of the requested Member State.

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

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

The preferred option for EDRi is that the follow-up information exchange continues to follow the national law of the requested Member State and mutual legal assistance rules without a direct obligation to disclose specific information to other Member States (policy option 1).

In the view of EDRi, it would be highly problematic to introduce an automated procedure for exchange of additional information (policy option 3), as this processing would constitute automated decision-making within the meaning of Article 11 of the LED for the controller in the requested Member State, especially as the automated data exchange could be triggered by processing sensitive personal data (biometric data) which is prohibited by Article 11(2) unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.[9]

If a revised Prüm framework adopts minimum standards for the data provided in the follow-up procedure (policy option 2), **there must be a mandatory manual review in the requested Member States, at least in order to verify the accuracy of the personal data disclosed, and there must be grounds for refusal by the requested Member State similar to Article 11 of the European Investigation Order (EIO) Directive 2014/41/EU.**

2. *Enable automated exchange of additional data categories that are available in Member States criminal or other databases for the purpose of criminal investigations*

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

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

[9] Dr Niovi VAVOULA, "Police Information Exchange - The future developments regarding Prüm and the API Directive", LIBE Committee Study, p. 30. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658542/IPOL_STU(2020)658542_EN.pdf

safeguards for the rights and freedoms of the data subject.

EDRi recommends to follow the baseline scenario of continuing with the current data categories while aligning the Prüm framework with the modernised data protection rules for law enforcement and the legislative process of the Lisbon Treaty with democratic scrutiny by the European Parliament. Additional data categories, especially those involving biometrics such as facial recognition, should not be considered until the updated Prüm framework have been evaluated (after full implementation by all Member States). **The next evaluation of the Prüm framework should include a thorough analysis of the data protection implications**, a matter which has received very little attention in the previous evaluation by the Commission.

EDRi is strongly opposed to extending the Prüm framework with facial images in Member States' criminal investigation databases (point c of policy option 2). Although this is presented in the IIA as access to information that is already available in Member States' databases, the extension with facial images will have severe consequences. Automated searches in the Prüm framework of facial images with a hit/no-hit response can only be done with facial recognition technology, which is currently not in wide-spread use by law enforcement authorities in the EU. Adding facial images to the Prüm framework would effectively make it mandatory for all Member States to implement facial recognition technology in law enforcement in order to comply with the Prüm information exchange requirements.

Indeed, the DAPIX focus group on face recognition[10] suggested that facial images fed to the database could not only come from the national reference image databases for law enforcement but also public surveillance cameras. This is a clear example of function creep which is contrary to the purpose limitation principle. It risks encouraging the deployment of facial recognition technologies for mass surveillance in public spaces everywhere in the EU, which is likely to have a severe 'chilling effect' on people's ability to enjoy their rights and freedoms. Given the current lack of legal accountability and democratic vacuum in which biometric surveillance deployments are occurring across Europe, new obligations under the Prüm regime would contribute to growing unlawful mass surveillance and other fundamental rights abuses.

Moreover, facial recognition is a highly controversial technology which currently suffers from severe problems with accuracy and risks of discrimination against ethnic minorities, as mentioned above in our general remarks about facial recognition. The Commission's 2020 study on the feasibility of improving the information exchange under the Prüm Decisions presents certain test results for facial recognition technology with "good accuracy", even for the presumably typical case where the search in facial image databases is based on a low-quality image of a possible suspect captured by surveillance cameras.[11] However, the practical experience with facial recognition by law enforcement authorities in the United States and the

[10] https://www.statewatch.org/media/documents/news/2020/mar/eu-council-prum-facial-recognition-13356-19.pdf

[11] The study (NIST Face Recognition Prize Challenge) assumes that a single low-quality image (e.g. from surveillance cameras) is compared against a large database of high-quality images, see page 153 of "Study on the feasibility of improving information exchange under the Prüm decisions, Advanced Technical Report" https://op.europa.eu/en/publication-detail/-/publication/3236e6ae-9efb-11ea-9d2d-01aa75ed71a1 The assumption that the facial-image database only consists of high-quality images is unlikely to be representative for all Member States' databases.

United Kingdom are very different from the simulated accuracy tests presented in the Commission study.

3. Facilitate the implementation, use and maintenance of the information system

EDRi does not wish to comment on the technical architecture of the information exchange in the Prüm network. We assume that the proposed "central router" (policy option 2) instead of the current decentralised network will only serve as a pass-through server to transmit messages between Member States, and not involve the construction of new EU-level databases (apart from collection of statistical data).

4. Enable search and comparison of data received by Europol from 3rd countries

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

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

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

5. Improve automated exchange of existing data categories

Despite the existence of inclusion and matching rules as well as technical specifications, the current rules on the data quality and the minimum requirements for reporting, requesting and submitting data from/to databases are still left to Member State to determine. This has led to important divergences in the implementation of the Decisions with serious consequences on the daily use of the system and the data protection guarantees of affected individuals. As the Commission is considering the extension of the scope of the Prüm framework (Objective 5, policy option 3), **it should first look at strengthening data protection safeguards of the current automated exchanges**, for examples by revising the minimum requirements for DNA matches.

EDRi understands the motivation for replacing the current Prüm Implementing Decision 2008/616/JHA with a more flexible legal instrument, e.g. delegated acts (policy option 2). However, it is important that this option is reserved for purely technical aspects of the Prüm framework which do not in any way affect the fundamental rights and freedoms of individuals, including data protection and criminal procedure safeguards. The current definition of a hit for automated DNA searches in 2008/616/JHA does not satisfy this requirement, since matches on six loci are accepted as a hit even though it is well known that there is a very high risk of false-positive matches. Such definitions should not be left to technical standards. On the contrary, if the revised Prüm framework continues to allow automated responses that are really inconclusive (neither full hit nor no-hit, e.g. a DNA match on six loci), **there must be strict legal safeguards in EU law which prevent the requesting Member State from taking coercive measures against an individual based solely on the inconclusive automated response.**

6. Provide high level of data protection

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

The hit/no hit system on which Prüm relies is not exempt from violations of the data protection rights of suspected persons. Hits can give away a lot of personal information in an automated manner. Coercive actions (e.g. stop and search, detention) can be carried out on the sole basis of one or multiple matches.

A study on the UK's Metropolitan Police and the use of live facial recognition on the streets[12] found that there was a "presumption to intervene" when the computer detected a match. The study found that even in severe doubt over the credibility of a match and when told by control room-based intelligence teams not to intervene, police officers nevertheless investigated the match. This presumption may have grave consequences for people who experience the resultant intrusive policing. It is especially the case of marginalised communities and people of colour who are disproportionately represented in those police databases and suffering from abusive policing given the systemic racial bias of European law enforcement and criminal justice systems.[13]

Moreover, the study commissioned by the LIBE Committee and published in 2018[14] showed that because some jurisdictions request, report and/or submit personal information without proper follow-up forensic and tactical work, cases were found where citizens have been arrested or undergone police suspicion and scrutiny until proven innocent. The presumption of innocence, data protection principles and the respect for due process can therefore easily be undermined by this system. **This data protection issue does not seem to be addressed or foreseen in the upcoming evaluation.**

[12] https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

[13] See this report by ENAR: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf
See the use cases collected by EDRi here: https://edri.org/wp-content/uploads/2020/09/Case-studies-Impermissable-AI-biometrics-September-2020.pdf
See also this report on the migration and border management databases in Europe by PICUM and Statewatch: https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf

[14] Dr. Victor TOOM, 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

Since the Prüm Decisions predate the entry into force of the renewed EU data protection framework for law enforcement (LED), an assessment of **all Member States' transpositions of the LED should be carried out in conjunction with the upcoming evaluation of the Prüm framework.**