STUDY

Requested by the LIBE committee

European Parliament

Police Information Exchange

The future developments regarding Prüm and the API Directive

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 658.542 - September 2020

EN

Police Information Exchange

The future developments regarding Prüm and the API Directive

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to provide background information and policy recommendations concerning police information exchange and in particular the future developments regarding Prüm and the API Directive (Directive 2004/82/EC).

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHOR
Dr Niovi VAVOULA, Queen Mary University of London
The study has been reviewed by Professor Valsamis MITSILEGAS, Queen Mary University of London.

ADMINISTRATOR RESPONSIBLE
Alessandro DAVOLI

EDITORIAL ASSISTANT
Ginka TSONEVA

LINGUISTIC VERSION
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in September 2020

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
AFSJ	Area of Freedom, Security and Justice
API	Advance Passenger Information
ADEP-EPRIS	Automation of Data Exchange Processes – European Police Records Information System
BMS	Biometric Matching Service
CJEU	Court of Justice of the European Union
CLOUD	Clarifying Lawful Overseas Use of Data Act
CODIS	Combined DNA Index System
ECRIS	European Criminal Record Information System
ECHR	European Convention on Human Rights
ECRIS-TCN	European Criminal Record Information System for Third-Country Nationals
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EPRIS	European Police Records Information System
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EUCARIS	European Car and Driving License Information System
FR	Facial Recognition
GDPR	General Data Protection Regulation
HLEG	High-level Expert Group on information systems and interoperability

iAPI	Interactive Advance Passenger Information
ISS	Internal Security Strategy
JHA	Justice and Home Affairs
MLA	Mutual Legal Assistance
NDNAD	National DNA Database
NIST	National Institute for Standards and Technology
NPC	National Contact Point
PIES	Prüm Implementation, Evaluation and Strengthening (Research Programme)
PIU	Passenger Information Unit
PNR	Passenger Name Record
SCC	Standard Contractual Clauses
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents (Database)
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
US	United States
VRD	Vehicle Registration Data

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Addressing security challenges related to terrorism, organised crime and cybersecurity has led to increased efforts to enhance police cooperation amongst national law enforcement authorities. A central pillar of EU action in that context relates to the facilitation of information exchange, particularly by eliminating obstacles to the exchange of personal data between national authorities. Thus, a wide range of EU legal instruments in the field of police cooperation has been adopted in accordance with elaborate agenda-setting by the EU institutions. For example, the report by the Special Committee on Terrorism by the Parliament published in November 2018 has called for enhanced cooperation and information exchange within and among Member States. The latest document in this regard is the Communication on the EU Security Union Strategy published by the Commission on 24 July 2020, calling *inter alia* for a modernisation of the Prüm Decisions (Decision 2008/615/JHA and Decision 2008/616/JHA) and the API Directive (Directive 2004/82/EC).

Aim

This study aims to provide background information and policy recommendations on the future developments regarding Prüm and the API Directive. In relation to the former, emphasis is placed on the implementation of the Prüm Decisions at the national level, the possible ways forward with a view to establishing the next generation Prüm, as well as the potential for opening up the Prüm framework to the United Kingdom (UK) and third countries, particularly the Western Balkans. As for the latter, the analysis is focused on the implementation of the API Directive, particularly in relation to the use of API data for law enforcement purposes and the possibility of embedding interoperability components in the API system.

Key findings: Prüm

Member States must ensure the availability of DNA, fingerprint (constituting special categories of personal data) and vehicle registration data from their national databases and allow automated searches through designated national contact points (NPC) who may compare these categories of data in individual cases and in compliance with the requesting Member State's national law. Prüm operates on a hit/no hit basis. In case of a hit, traditional channels of mutual legal assistance are activated, but these are not technically part of the Prüm regime and exchanges of further available personal data are governed by the national law of the requested Member State. The implementation of the Prüm Decisions necessitated the establishment of national databases, including enacting national legislation in that respect

State of implementation: Overall, according to the latest information on the state of play of implementation of Prüm, a large majority of Member States are operational and enable automated searches of DNA analysis files, fingerprints and vehicle registration data (VRD). However, a few Member States have not yet been operational, whereas amongst the operational ones the degree of connectivity with other Member States' databases varies considerably.

a) DNA analysis files: Greece and Italy are still not operational, although the relevant software has been installed. Furthermore, amongst the 25 operational states, the degree of connectivity considerably varies. The different types of national DNA analysis files (convicted persons, suspects, crime stains, victims, unidentified persons, unidentified human remains, missing persons, relatives of missing persons) to which Member States give each other access for the investigation of criminal offences also vary; all participating States allow searches of any crime stains stored in their national database, whereas in relation to convicted criminals and suspects few exceptions are noticed; 18 out

of 29 participating countries allow access to DNA files concerning unidentified human remains. Search of their national DNA analysis files of unidentified persons and missing persons is less widespread and discrepancies are observed, as around half the participating countries (14 out of 29) allow access to such files.

b) Fingerprint data: Greece, Italy, Croatia and the UK do not allow or launch fingerprint data exchanges. Greece and Croatia are in the testing phase. Amongst operational countries, connectivity discrepancies similar to those observed in relation to DNA analysis files are noted here as well. Searches to national Automated Fingerprint Identification Systems (AFIS) containing fingerprint data of criminals, suspects and those found in a crime scene are widely allowed with few exceptions, however around half of countries give each other access to their national AFIS databases containing fingerprints of unidentified human remains, but automated searches to missing persons' fingerprints is currently enabled in seven countries only.

c) VRD: Greece, Italy and the UK are not operational.

Next generation Prüm: With the implementation of Prüm coming to an end, the aspiration for a next generation Prüm with a view to broadening its scope and, to that end, updating the necessary technical and legal requirements has come to the forefront. A revision of the Prüm framework will enable the incorporation of modernised data protection safeguards in line with the current EU legal framework on data protection law, particularly Directive 2016/680. Furthermore, in the post-Lisbon Treaty era a revised Prüm will be scrutinised by the Parliament during the legislative process. Four focus groups – DNA, fingerprints, VRD and facial images - were established with the task of setting out how to further develop the current information exchange mechanisms and to support the Commission's feasibility study on improving information exchange under the Prüm Decisions.

A feasibility study on improving information exchange under the Prüm Decisions was published in May 2020,[1] proposing a wide array of possible amendments in five areas as below. The options were designed to remedy certain shortcomings identified by the study and to include new solutions resulting from changes in the technological landscape and maximise the performance of the Prüm network.

1. Improving the automated data exchange: This includes the expansion of the Prüm by allowing searching for missing persons and identifying deceased persons. This option presents certain challenges; exchanges will be enabled in respect of persons who do not have a criminal activity or are suspected of such activity and may include vulnerable groups of individuals. Additional safeguards are required in relation to the retention of such data and the authorities' rights to launch searches. A way forward could be to distinguish data exchanges concerning missing and deceased persons from those related to criminals. As for deceased persons, the level of personal data protection is subject to national law and is considered uneven among Member States.

Furthermore, improvements on the types of data exchanged are proposed, such as implementing standards on the quality of fingerprints and improvements of statistical data on usage (but accuracy statistics are discarded as an option).

2. Improving the follow-up procedure (Step 2), whereby a limited core data set is provided by default in cases of 'high-accuracy searches' of fingerprint data only. This development that introduces automaticity in data exchanges should be reserved for cases where the possibility of false matches is very low.

[1] Commission, 'Study on the feasibility of improving information exchange under the Prüm Decisions (May 2020).

3. Introducing new data categories, namely facial images, driving licenses and biographic data. The inclusion of facial images will enable law enforcement authorities to employ facial recognition technology with the aim of identifying unknown perpetrators of criminal offences. Challenges to the protection of the rights to private life and protection of personal data, as well as non-discrimination are raised stemming from the risks of false matches which may be due to various factors; the possibility of comparing low quality images will affect the searches increasing the potential of false positive matches; the size of the national databases, the age of facial images and the number of results displayed for all requests. Furthermore, research demonstrates that in comparing facial images, the underlying Facial Recognition technology is inaccurate particularly for people of colour and individuals may be wrongly bothered by the police due to algorithm bias. The creation of index databases containing an extract of police records with pseudo-anonymised data is also foreseen, but the fundamental rights implications and safeguards such as on the purposes, retention period and data contained in national indexes must be carefully determined.

4. Introducing a new IT architecture, by implementing a central router, which will receive and send Prüm requests between Member States, instead of requiring bilateral arrangements and connections. This solution is preferred in comparison to a centralised information system, which has been rejected due to legal constraints on storing such data outside the national territory, for various reasons; processing personal data at EU level will be avoided; accurate statistical data at central level will be produced and technical difficulties posed by bilateral connections will be eliminated.

5. Exploring the possibility of linking Prüm to other information systems and embedding interoperability solutions. This might involve the possibility of connecting the Prüm databases to the European Search Portal (ESP) and providing access to Prüm data to Europol, Interpol and certain third countries. These solutions must be assessed in light of the principles of necessity and proportionality.

The participation of the UK in Prüm: The UK is operational with regard to DNA analysis files. As for fingerprint data exchanges, notwithstanding the UK's departure from the EU and the Parliament's opposition, a Council Implementing Decision was recently (in August 2020) adopted. A new partnership agreement is currently negotiated featuring *inter alia* Prüm-like provisions. At the same time, the UK seeks a Commission adequacy decision; at the time of writing, it is uncertain as to whether these efforts will be fruitful. If not, other options are the adoption of a partial adequacy decision or access via Interpol.

Western Balkans: The Police Cooperation Convention for Southeast Europe (PCC SEE) signed a 'Prüm Agreement for South-East Europe' mirroring the Prüm rules. Though the third countries involved in this agreement are in an accession trajectory, concerns are raised as to whether such cooperation may indeed take place without the EU involvement. In October 2019, the Commission decided to launch infringement procedures by sending letters of formal notice to Austria, Bulgaria, Hungary and Romania for signing the agreement in breach of the EU's exclusive competence under Article 3(2) TFEU.

Key findings: API Directive

In February 2020, an evaluation report on the implementation of the API Directive was released. It found a series of implementation issues, particularly in relation to the data processing rules (Article 6). This assessment includes Article 6(1) last subparagraph that foresees the use of API data for law enforcement purposes, when the use of such data is authorised by national law, but implementation of this option has left at Member States' discretion the possibility of using API data for law enforcement purposes; all but two Member States have made use of this discretion. At the same time, the PNR Directive has established the obligation for air carriers to transmit API data, as well as flight reservation data, where API data are collected in the normal course of their business. As a result, the processing of

API data at EU level is governed by two separate instruments, which are strongly linked. However, there are discrepancies between the two instruments, as the API Directive lacks a definition of what 'law enforcement' purposes may encompass, the API data elements do not entirely match in both Directives, the two instruments do not apply to the same type of flights and no requirements on the data retention period are foreseen for the use of API data for law enforcement purposes. Overall, though more clarity and coherence is needed, it must be emphasised that the PNR framework is currently under scrutiny by the CJEU. Finally, it has been pointed out that the forthcoming introduction of the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) will require an interactive API (iAPI), so that API data will be sent once through a single point (the carrier gateway) to different destinations: both centralised systems and national systems. This solution presents a number of expected implementing challenges, such as the lack of financial resources and insufficient analytical and processing capacity. iAPI is currently at a very early stage in the EU. Currently, only one Member State has implemented an interactive API system and three Member States have partially integrated their API systems with their electronic systems for travel authorisation and visa verification.

1. POLICE COOPERATION IN THE EU: A SKETCH

1.1. The current legal framework

In an EU Area of Freedom, Security and Justice (AFSJ) underpinned by the free movement of persons without internal border controls, the aim of ensuring a high level of security for EU citizens scores high in the agenda. A series of important challenges have been identified in that regard, highlighting the need for action at EU level. Terrorism, including radicalisation to terrorism and recruitment, terrorism financing and the growing phenomenon of foreign terrorist fighters, remains a top priority. Furthermore, organised crime has been considered a major threat since the 90s, due to its continuously changing nature in terms of organisation, targets, *modi operandi* and perpetrators.[2] More recently, the evolution of digital technologies has brought to the forefront challenges in relation to cybercrime and cybersecurity.[3]

Addressing these perceived threats has led to increased efforts to enhance collaboration and foster mutual trust amongst national law enforcement authorities. In that respect, rules on police cooperation in criminal matters may be adopted in accordance with Articles 87-89 of the Treaty on the Functioning of the European Union (TFEU). In the post-Lisbon Treaty era, with the abolition of the pillar structure, the institutional framework has been simplified to a considerable extent, with most police cooperation measures now adopted under the ordinary legislative procedure and subject to judicial review by the Court of Justice of the European Union (CJEU).[4]

A 'central pillar' of EU action in that context relates to the facilitation of information exchange across national law enforcement authorities.[5] The possibilities offered by modern technologies for law enforcement authorities to collect, combine and exchange data seamlessly and in a timely manner have resulted in the emergence of an elaborate legal framework on the processing of personal data, particularly with a view to combating terrorism and other serious crimes. Initiatives have been twofold: on the one hand, the establishment of EU-wide centralised information systems; and on the other hand, the elimination of obstacles to the exchange of personal data between national authorities.[6] The competence to embark on these measures relies upon Article 87(2)(a) TFEU, providing for the setting up of information exchange mechanisms, which enable the collection, storage, further processing, analysis and exchange of relevant information. Legislative action has also been influenced by the Roadmap to enhance information exchange and information management.[7] In addition, the report by the Special Committee on Terrorism by the Parliament published in November 2018 has called for enhanced cooperation and information exchange within and among Member States.[8] Overall, under the principle of availability as the guiding concept for law enforcement information exchange, as proclaimed in the Hague Programme,[9] a wide range of EU legal instruments in the field of police cooperation have been adopted, including: the establishment of a Schengen-wide centralised

[2] See Valsamis Mitsilegas, *EU Criminal Law* (Hart 2009) ch 2.

[3] For example see the Conclusions of the Council of 14-15 June 2015 on the Renewed European Union Internal Security Strategy 2015-2020 in Document 9798/15 (15 June 2015).

[4] There are still certain original features retained: in particular, see Articles 76, 89 and 87(3) TFEU. Also see, Valsamis Mitsilegas, *EU Criminal Law after Lisbon* (Hart 2016) ch 2.

[5] Commission, 'The European Agenda on Security' (Communication) COM(2015) 185 final.

[6] For an analysis see Mitsilegas, *EU Criminal Law* (n 2) ch 5.

[7] Council, Document 9368/1/16 REV 1 (6 June 2016).

[8] Parliament, Special Committee on Terrorism, 'Report on Findings and Recommendations of the Special Committee on Terrorism' (P8_TA(2018)0512, 21 November 2018).

[9] European Council, The Hague Programme: strengthening freedom, security and justice in the European Union [2005] OJ C53/1.

information system, the Schengen Information System (SIS);[10] the setting up of avenues for exchange of information on criminal records through the European Criminal Record Information System (ECRIS)[11] and ECRIS-TCN (for third-country nationals),[12] as well as DNA profiles, fingerprints and vehicle registration data (VRD) via the Prüm framework.[13] Furthermore, expedited exchanges of existing information and intelligence are regulated by the so-called Swedish initiative.[14] The private sector has also been co-opted in these efforts though obligations to transfer passenger name record (PNR) data[15] and financial information.[16] In addition, automaticity in information exchange and aggregation of data from different sources will be achieved through the introduction of interoperability amongst the EU centralised information systems.[17] Importantly, according to Article 88 TFEU, police cooperation is promoted through Europol that supports cooperation among domestic law enforcement authorities through the collection, storage, further processing, analysis, and exchange of personal data, whether provided by Member States or produced by the agency itself.[18]

1.2. Agenda setting

These developments must be viewed in the broader context of agenda-setting in the sphere of EU criminal law, at the epicenter of which is the elaboration of an Internal Security Strategy (ISS). The latter is a cross-cutting task concerning wider areas within the overall field of EU criminal law, whereby the common threats and challenges in the EU, the internal security policy and the principles underpinning

[10] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56.

[11] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States [2009] OJ L93/23.

[12] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135/1.

[13] 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 [2008] OJ L210/1; 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 [2008] OJ L210/12 (collectively Prüm Decisions).

[14] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L386/89 (Swedish Initiative).

[15] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132 (PNR Directive).

[16] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA [2019] OJ L186/112.

[17] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L 135/85. For border controls and asylum see Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L135/27 (Interoperability Regulations).

[18] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53.

it are set out.[19] Following the Internal Security Strategy (2010-2014),[20] the Council adopted its Renewed Internal Security Strategy (2015-2020), defined in Council Conclusions of 16 June 2015,[21] which *inter alia*, set out as a priority the improvement of information exchange and operational cooperation so as to address the security threats posed by terrorism and serious and organised crime. The Strategy was informed by the European Agenda on Security, issued by the Commission, which has acquired a key role in the development of this field.[22] Emphasis on security is also exemplified by the emergence of creating an 'effective and genuine Security Union' as the driving force for legislative action.[23]

The latest instalment in this regard is the Commission Communication on the EU Security Union Strategy, adopted on 24 July 2020.[24] The Communication is influenced by the current COVID-19 pandemic and the newly emerged safety and security threats to the EU and lays out four strategic priorities for action at EU level for the period 2020-2025. One of the four main building blocks of the new strategy is the protection and resilience of independent critical infrastructure, physical and digital.[25] Tackling cybercrime and identity theft through modern law enforcement tools, including artificial intelligence, are also foreseen.[26] Furthermore, terrorism and organised crime remain at the top of the EU agenda, with efforts concentrating on anti-radicalisation, trafficking in human beings, smuggling, drug and illegal firearm trafficking.[27] The final component of the strategy involves the establishment of a 'strong security ecosystem', whereby cooperation and information sharing are promoted.[28] Central in this respect are the role of EU and international agencies, particularly Europol, Eurojust and Interpol. The revision of certain existing legal instruments is also in the pipeline.[29] In relation to police information exchange in particular, the Security Union Strategy identifies two main legislative priorities, which are relevant for the present analysis: on the one hand, the modernisation of the Prüm framework 'to enable the automated exchange of additional data categories that are already available in Member States' criminal or other databases for the purpose of criminal investigations', as well as the exchange of police records;[30] on the other hand, the revision of Directive 2004/82/EC on the use of Advanced Passenger Information (API) data for the purposes of improving border control and reducing irregular migration,[31] which 'could allow for more effective use of the information, while ensuring compliance with data protection legislation and facilitating the flow of passengers'.[32]

Against this backdrop, this study aims to provide background information and policy recommendations on the future developments regarding Prüm and the API Directive, so as to inform

[19] 'A European Security Strategy: A Secure Europe in a Better World' was adopted in 2003 and reviewed in 2008. Then, an Internal Security Strategy was approved by the Council. See Council, Document 5842/2/10 (23 February 2010).

[20] See n 3.

[21] Commission, 'The European Agenda on Security' (n 5).

[22] For an analysis on agenda setting in EU criminal law see Valsamis Mitsilegas and Niovi Vavoula, 'European Union Criminal Law' in Herwig Hofmann et al. (eds), *Specialized Administrative Law of the European Union - A Sectoral Treatment* (Oxford University Press 2018) 179-181.

[23] Commission, 'Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union' (Communication) COM(2016) 230 final.

[24] Commission, 'The EU Security Union Strategy' (Communication) COM(2020) 605 final.

[25] Ibid, 6-7.

[26] Ibid, 10-13.

[27] Ibid, 15-20.

[28] Ibid, 20-23.

[29] Ibid, 21-22.

[30] Ibid, 22.

[31] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data [2004] OJ L261/24.

[32] Commission, 'EU Security Union Strategy' (n 24) 22.

the forthcoming Security Dialogue with the European Commission. Through desk research of EU documentation (legislation, evaluation reports, feasibility studies, Council documents, Commission Communications etc.) and relevant secondary literature, the study focuses on the implementation of the Prüm Decisions and the API Directive at the national level, as well as the possibility of expanding the interoperability components to incorporate these legal instruments. Furthermore, the possible ways forward of the next generation Prüm and the potential for opening up the Prüm framework to the United Kingdom (UK) and third countries, particularly the Western Balkans, are analysed.

2. THE PRÜM FRAMEWORK

2.1. From the Prüm Convention to the Prüm Decisions

On 27 May 2005, seven EU Member States (Belgium, Germany, Spain, France, the Netherlands, Luxemburg and Austria) signed the Prüm Convention on the 'stepping up of cross-border co-operation, particularly in combating terrorism, cross-border crime and illegal immigration'.[33] It is considered to have been an initiative driven by the view that the abolition of internal border controls and free movement of persons implied that irregular migrants and criminals would also move freely, thus increased cross-border cooperation between national law enforcement authorities of the Member States was necessary. Through the Prüm Convention participating States decided to push ahead on an intergovernmental basis and forge closer cooperation in home affairs matters,[34] and agreed to commence the exchange of information relating to DNA, fingerprints and vehicle registration data.[35]

From the outset, it was stated that participation in their group was open to all EU Member States and that a proposal would be tabled in three years from the entry into force of the Convention, leading to its incorporation into the legal framework of the EU.[36] Such initiative happened much earlier, when in February 2007, the Justice and Home Affairs (JHA) Council agreed to integrate into the EU legal framework the majority of the parts of the Prüm Treaty relating to police and judicial co-operation in criminal matters.[37] In August 2008, Council Decision 2008/615/JHA was finally published,[38] along with an accompanying Decision (2008/616/JHA) on Prüm implementing measures (together referred to as Prüm Decisions).[39] In the meantime, between 2007 and 2008, Bulgaria, Portugal, Sweden, Greece, Finland, Hungary, Italy, Romania, Slovakia and Slovenia ratified or acceded to the Convention.

2.2. The Prüm Decisions in a nutshell

Law enforcement agencies have always sought each other's assistance in tracking down a suspect or determining whether crime scenes in different countries could be related through matching fingerprints or DNA profiles. However, what the Prüm Decisions achieved was the removal of barriers for the circulation of specific categories of information.[40] Indeed, the Preamble of Decision 2008/615/JHA refers to the need to introduce procedures for promoting fast, efficient and inexpensive means of personal data exchange for the investigation of criminal offences, particularly terrorism and cross-border crime,[41] 'whereby Member States grant one another access rights to their automated DNA

[33] Council, Document 10900/05 (7 July 2005).

[34] Thierry Balzacq and Amelia Hadfield, 'Differentiation and Trust: Prum and the Institutional Design of EU Internal Security' (2012) 47(4) *Cooperation and Conflict* 539.

[35] For an early analysis see Thierry Balzacq et al., 'Security and the Two-Level Game: The Treaty of Prum, the EU and the Management of Threats' (CEPS Working Document no 234, 2006); Thierry Balzacq et al., 'The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security' in Thierry Balzacq and Sergio Carrera (eds), *Security versus Freedom? A Challenge for Europe's Future* (Ashgate 2006). Also see Valsamis Mitsilegas, 'What Are the Main Obstacles to Police Co-Operation in the EU?' (Briefing Paper for European Parliament LIBE Committee, IP/C/LIBE/FWC/2005-24, 2006). reproduced in Didier Bigo and Anastassia Tsoukala (eds), *Controlling Security* (Centre d'études sur les conflits/l'Harmattan 2008).

[36] Victor Toom, 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision' (Study for the LIBE Committee, PE 604.971, 2018) 10. Barbara Prainsack and Victor Toom, 'The Prüm Regime: Situated Dis/empowerment in Transnational DNA Profile Exchange' (2010) 50(6) *British Journal of Criminology* 1117; Barbara Prainsack and Victor Toom, 'Performing the Union: The Prüm Decision and the European Dream' (2013) 44(1) *Studies in History and Philosophy of Biological and Biomedical Sciences* 71.

[37] Council, Document 5922/07 (15 February 2007) 7.

[38] See n 13.

[39] Ibid.

[40] Prainsack and Toom, 'Performing the Union' (n 36) 73.

[41] Decision 2008/615/JHA, recitals 4 and 8 respectively.

analysis files, automated dactyloscopic identification systems and vehicle registration data'.[42] The text effectively mirrors the provisions of the Prüm Treaty.[43] Member States must ensure the availability of DNA,[44] fingerprint[45] (constituting special categories of personal data)[46] and vehicle registration data[47] from their national databases[48] and allow automated searches through designated national contact points (NPC) who may compare these categories of data in individual cases and in compliance with the requesting Member State's national law.[49] In effect, Decision 2008/615/JHA obliges Member States to establish national databases containing these types of information,[50] with the processing of personal data being subject to the national law applicable to the processing.[51] Hence, Prüm constitutes a decentralised network for information exchange, composed of national databases connected to each other.

In practice, police cooperation is divided into two steps, whereby as a first step information relating to DNA, fingerprints and VRD may be automatically exchanged pursuant to the Prüm rules. Therefore, the automated exchange covers the search and comparison of data, the notification of a hit/no hit and the supply of reference data only, so as to minimise the exchanged data. In case of a match (hit), traditional channels of mutual legal assistance, including the prescriptions of Framework Decision 2006/690/JHA (Swedish Initiative),[52] are activated, but these are not technically part of the Prüm regime.[53] Thus, Member States may exchange further available personal data and other information, which is governed by the national law of the requested Member State.[54]

Furthermore, Decision 2008/615/JHA prescribes rules on the supply of personal and non-personal data in case of major events with a cross-border dimension (Chapter 3) and for the prevention of terrorism offences (Chapter 4).[55] Rules on other forms of cooperation, such as joint operations[56] or assistance in cases of mass gatherings, disasters and serious accidents[57] are also foreseen (Chapter 5). Finally, a series of data protection rules are laid down (Chapter 6); that the processing of personal data by the receiving Member State shall be permitted solely for the purposes for which the data have been supplied and

[42] Ibid, recital 10.

[43] For an overview see House of Lords European Union Committee, 'Prüm: An Effective Weapon Against Terrorism and Crime?' (18th Report, session 2006-07, HL Paper 90).

[44] Decision 2008/615/JHA, art 2(2). By mutual consent, unidentified DNA profiles may also be compared with all DNA profiles from other national DNA databases (art 4) In ongoing investigations and where there is no DNA profile available for a particular individual present in the requested Member State, it is also possible that cellular material is collected and become available (art 7).

[45] Decision 2008/615/JHA, art 8. Interestingly, automated searching may take place in connection to both the prevention and investigation of criminal offences, whereas in the case of DNA data such search is prescribed for the investigation of criminal offences only. Compare arts 2 and 8.

[46] In line with Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Law Enforcement Directive), art 10. For the protection of special categories of personal see *S and Marper v UK* (2009) 48 EHRR 50.

[47] Decision 2008/615/JHA, art 12. Such searches may involve data relating to owners or operators and to vehicles.

[48] In specific the reference data, which are DNA profiles established from the non-coding part of DNA and a reference number.

[49] Decision 2008/615/JHA, art 3(1). On national contact points see arts 6, 11 and 15.

[50] Mitsilegas, *EU Criminal Law* (n 2) 260; Toom (n 36) 11.

[51] Decision 2008/615/JHA, art 2(1).

[52] See n 14.

[53] Toom (n 36) 11.

[54] Decision 2008/615/JHA, art 5.

[55] Ibid, arts 13-15.

[56] Ibid, art 17.

[57] Ibid, art 18.

any processing for other purposes must be subject to prior authorisation of the Member State administering the file, and subject only to the national law of the receiving Member State;[58] rules concerning the accuracy, relevance and storage period of the data are also included, including the possibilities to correct or delete that data;[59] and individual rights are prescribed.[60] However, at the time of its adoption, the legal framework on data processing for law enforcement purposes was missing, as Framework Decision 2008/977/JHA had not yet been adopted,[61] let alone its successor: Directive 2016/680/EU (Law Enforcement Directive).[62]

As for participation, Prüm applies to the 27 EU Member States, the UK and the Schengen Associated States (Iceland, Norway, Switzerland and Liechtenstein), the national databases of which are interconnected bilaterally.

2.3. The rocky implementation of the Prüm Decisions

2.3.1. An overview

All Member States were expected to have implemented the Prüm Decisions in two phases: the deadline for transposition of the rules on the supply of information relating to major events and the prevention of terrorist offences and data protection was 26 August 2009, whereas in relation to provisions on the automated searching of DNA profiles, dactyloscopic data and vehicle registration data (VRD) the deadline was set for 26 August 2011.[63] However, the practical implementation has been fraught with technical complications.

As mentioned above, with the Prüm Decisions becoming part of the EU *acquis*, it became mandatory for Member States to make data stored in national databases available to other Member States on a hit/no hit basis. This presupposed the existence of such databases at the national level, which was not always the case. As a result, the implementation of the Prüm Decisions necessitated the establishment of national databases, including enacting national legislation in that respect. As these databases are subject to national law, their underlying governing rules may differ significantly.

In addition to technical implementation, Member States have to fulfil numerous formal requirements.[64] The supply of personal data for a specific Member State needs prior evaluation, which requires a series of steps to be undertaken: firstly, Article 25(2) of Decision 2008/615/JHA foresees that the data protection provisions (Chapter 6) are implemented in national law prior to the supply of personal data, and Member States must reply to the relevant data protection questionnaire; and secondly, according to Article 20 of Decision 2008/616/JHA, before a Member State can start the operational automated searching of any of the categories, it should pass an evaluation procedure. The procedure consists of a questionnaire, which the Member State must fill in connection with the data category (DNA analysis files, fingerprints, VRD) that it wishes to start the implementation, a pilot run and an

[58] Ibid, art 26(1).

[59] Ibid, art 28.

[60] Ibid, art 31.

[61] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60.

[62] See n 46. Decision 2998/615/JHA refers to the Council of Europe Convention for the Protection of Individuals with regards to Automated Processing of Personal Data of 28 January 1981, and its Additional Protocol of 8 November 2001.

[63] Decision 2008/615/JHA, art 36(1).

[64] In particular, Member States must provide a series of declarations and notifications in relation to national contact points (NCPs) in accordance with arts 6(1), 11(1), 12(2), 15 and 16(3) of Decision 2008/615/JHA, as well as notification of the national data protection authorities in accordance with art 19 of Decision 2008/616/JHA.

evaluation visit. On the basis of these, an evaluation report is submitted to the Council, which must unanimously decide whether the conditions have been met after consultation of the Parliament.[65] Afterwards, the Council can adopt the Implementing Decision that the Member State concerned can start the operational data exchange.

In analysing the current state of play this section is based on Council document 5197/1/20 REV 1, dated 25 June 2020.[66] For the sake of a holistic approach, this section is accompanied by a Table indicating the relevant legal instruments pursuant to which Member States operate Prüm information exchanges. Overall, the implementation process has been rather slow[67] and these delays may be attributed to various factors, primarily linked to financial and technical difficulties. For example, Greece, Italy and Ireland did not have DNA databases or dedicated legislation when the Prüm Decisions were adopted. Besides, these countries were severely hit by financial crises.[68] As for the UK, it was part of Prüm when the Decisions were adopted, but then it withdrew in December 2014, subject to its opt-out privileges and then re-joined (see Section 2.5.1). Such implementation issues had even led the Commission to send formal notices against several Member States (Croatia, Ireland and Italy, as well as Greece and Portugal) for failing to comply with the Prüm Decisions.[69] The infringement proceedings remain open in respect of Italy and Greece.

At the time of writing, **the large majority of Member States are operational and enable automated searches of DNA analysis files, fingerprint and vehicle registration data. However, as shown below, few Member States have not yet been operational, whereas amongst the operational ones, the degree of connectivity with other Member States' databases varies considerably.**

2.3.2. DNA data

When the deadline for implementation of the Prüm Decisions expired in August 2011, apart from the ten Member States already operational, no more than two additional Member States had complied with the legal and technical provisions for DNA data exchange.[70] In October 2012, the Commission published its implementation report stating that 18 Member States had implemented the Prüm Decisions in relation to DNA data, whereas another five had considerably advanced in the required steps for the automated exchange of DNA data and were likely to become operational in early 2013.[71] Greece, Ireland, Italy and the UK, however, were still lagging behind in implementation.

The latest information on the state of play of implementation of Prüm indicates that **Greece and Italy (and Norway) are still not operational, although the relevant software has been installed**.[72] Furthermore, amongst the 25 operational states, **the degree of connectivity considerably varies**; the Netherlands exchanges DNA data with 24 countries, whereas Denmark exchanges with seven

[65] This provision does not apply to those Member States where the supply of personal data as provided for in the Decision has already started pursuant to the Prüm Treaty.

[66] Council, Document 5197/1/20 REV 1 (25 June 2020). The state of play does not provide information about Schengen Associated States. Limited information is provided on Norway, which is not operational yet.

[67] Council, Document 17761/11 (5 December 2011) For an appraisal see Chris Jones, '"Complex, Technologically Fraught and Expensive" - The Problematic Implementation of the Prüm Decision' (Statewatch, 2012).

[68] Council, Document 5197/1/20 REV 1 (n 66) 5.

[69] The latest information is found in Commission, 'Ninth progress report towards an effective and genuine Security Union' COM(2017) 407 final.

[70] Council, Document 17761/2011 (n 67).

[71] Commission, 'The implementation of 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 (the "Prüm Decision")' (Report) COM(2012) 732 final, 3.

[72] Council, Document 5197/1/20 REV 1 (n 66) 16 and 20.

countries, Bulgaria with 12 countries, the UK with nine countries and Ireland with two countries only. Annex I demonstrates that nine years after the deadline indicated in Decision 2008/615/JHA, the implementation is still not fully complete and participating countries must continue broadening operational connectivity among themselves.[73]

Another issue that merits further exploration involves the different types of national DNA analysis files to which Member States give each other access for the investigation of criminal offences.[74] The different categories of files may concern convicted persons, suspects, crime stains, victims, unidentified persons, unidentified human remains, missing persons, relatives of missing persons and other categories.[75] Annex II provides a comparative overview of these categories, on the basis of which the following remarks must be made. From the outset, it is recalled that the Prüm Decisions have been adopted to assist in the investigation of criminal offences, but participating states apply this scope in relation to national legislation. Therefore, states are bound as to which categories to allow other countries to launch queries and what restrictions are imposed on their own law enforcement bodies by their national legislation. **The most widespread categories are crime stains, convicted criminals and suspected criminals;** all participating States allow searches of any crime stains stored in their national database, whereas in relation to convicted criminals and suspects few exceptions are noticed (with regard to convicted criminals, exceptions are Greece, Poland and Slovenia, and as for suspects exceptions are Cyprus and Portugal). **The majority of participating countries (18 out of 29) allow access to DNA files concerning unidentified human remains**.[76] Search of their national DNA analysis files of **unidentified persons and missing persons is less widespread and discrepancies are observed, as around half participating countries (14 out of 29) allow access to their DNA analysis files**.[77] In the remaining categories, automated searches are the exception; only Hungary and Slovakia allow automated searches to DNA files related to crime victims, and Malta enables searches to DNA of relatives of missing persons. Overall, the countries with the most permissive legal frameworks are Malta, Slovakia and the Czech Republic, whilst in Germany, Ireland, Greece, Luxembourg, Portugal, Finland and Sweden law enforcement officers are entitled to use Prüm on fewer occasions. As it will be shown below, when analysing the proposed reforms to the Prüm framework, these discrepancies do not allow reciprocity in launching automated searches.

2.3.3. Fingerprint data

The implementation of the rules on automated searches of fingerprint data was initially the thorniest one, with the Commission reporting in October 2012 the highest number of Member States seriously lagging behind in transposing the respective rules; only 14 Member States were ready for searches in their automated fingerprint identification systems (AFIS) by other Member States. Another seven were expected to complete their technical implementation in early 2013. However, in relation to six Member

[73] Ibid, 20.

[74] Ibid, 21 .

[75] This is a particularly ambiguous category. For example, in the Czech Republic that category encompass 'any situation not covered by the above'. See Council, Document 13903/11 (8 September 2011) 2.

[76] These are: Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Spain, France, Italy, Cyprus, Hungary, Malta, the Netherlands, Austria, Poland, Romania, Slovenia, Slovakia, and the UK. See Council, Document 5197/1/20 REV 1 (n 66) 21.

[77] Ibid. In relation to unidentified persons the participating countries that allow search are: Czech Republic, Estonia, Spain, France, Hungary, Cyprus, Latvia, Lithuania, Malta, Netherlands, Austria, Poland, Romania and Slovakia. In relation to missing persons the participating countries that allow search are: Belgium, Czech Republic, Denmark, Estonia, Hungary, Italy, Latvia, Malta, Netherlands, Austria, Poland, Romania, Slovenia and Slovakia.

States (Greece, Ireland, Italy, Poland, Portugal and the UK), the timeframe for implementation was unclear.[78]

The current state of play confirms that the implementation is in its final stages, but remains incomplete.[79] Annex III demonstrates that considerable discrepancies are still evident. Firstly, **Greece, Italy and Croatia (as well as Norway) do not allow or launch fingerprint data exchanges; Greece and Croatia are operational, but they are in the testing phase.** The UK case is analysed in detail in Section 2.5, therefore, it suffices here to mention that despite its departure from the EU, a Council Implementing Decision was adopted allowing automated searches on fingerprint data.[80] Amongst operational countries, discrepancies similar to those observed in relation to DNA analysis files are noted here as well. On the one hand, whereas the majority of countries are connected to around 20 other partners, Latvia is operational with nine countries, Sweden with five countries and Ireland with two countries only.[81] On the other hand, Belgium is operational with nine countries for both incoming and outgoing requests, but also allows incoming launches for an additional 12 countries.[82] Finally, it is to be mentioned that every participating state has indicated the maximum search capacities per day for dactyloscopic data of identified and unidentified persons, which is mutually agreed with each country.[83]

As with DNA analysis files, it is worth noting the differences found in connection to the national AFIS repositories to which Member States allow each other access for automated searching of fingerprint data, which are due to divergent national legal frameworks.[84] From the outset, it is stated that there is no information provided by Greece, Italy and Norway. In relation to the remaining participating countries, **searches to national AFIS containing fingerprint data of criminals are widely accepted**, with two exceptions: Poland and Slovenia.[85] Furthermore, **search launches of fingerprints of suspects are also widespread** and the sole exceptions are Finland and Romania. However, Portuguese law enables such searches only when the suspect is accused of a criminal offence.[86] Moreover, **except for the UK, fingerprints found in a crime scene may be automatically compared with those in national AFIS of other countries**. Notably, in Austria and Portugal, such searches must relate to open cases. In addition, **around half of countries give each other access to their national AFIS databases containing fingerprints of unidentified human remains,[87] but automated searches to missing persons' fingerprints is currently enabled in seven countries only**,[88] with France adding this

[78] Commission, 'The implementation of Council Decision 2008/615/JHA' (n 71) 4.

[79] Council, Document 5197/1/20 REV 1 (n 66) 22-27.

[80] Council Implementing Decision (EU) 2020/1188 of 6 August 2020 on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom [2020] OJ L265/1.

[81] Council, Document 5197/1/20 REV 1 (n 66) 23-24 and 26.

[82] Ibid, 22.

[83] For the latest list, see Council, Document 10119/20 (14 August 2020). Three types are foreseen; tenprints against tenprints, latent against tenprint/palmprint and searches against unsolved fingerprint latent (UL) and unsolved palmprint latent (ULP) databases.

[84] Council, Document 5197/1/20 REV 1 (n 66) 28.

[85] Ibid.

[86] Ibid.

[87] Ibid. These are: Czech Republic, Denmark, Germany, France, Croatia, Cyprus, Latvia, Lithuania, Luxembourg, Netherlands, Austria, Portugal, Romania and Norway. In the Netherlands, the unidentified human remains must be crime related.

[88] Ibid. These are: Czech Republic, Cyprus, Luxembourg, Austria, Portugal, Romania and Norway. In Austria and Portugal, such searches must be crime related.

capability by the end of 2020. Searches of victims' fingerprints or relatives of missing persons are exceptional.[89]

2.3.4. Vehicle registration data

As for vehicle registration data, in October 2012 only 13 Member States were operational; however, another four had passed or were ready for Council evaluation and for seven serious efforts were observed.[90] At the time of writing, only three Member States (Greece, Italy, UK) are not operational, as well as Norway. Annex IV provides a comparative outline of where VRD exchange is operational. In the case of Italy, EUCARIS (European Car and Driving License Information System), which is an information exchange system that provides an infrastructure and software to countries to share VRD, is installed and testing has successfully concluded and internal procedures are set up.[91] In relation to the UK, an inbound capability to process incoming requests from Member States has been developed and the feasibility of short-term and long-term outbound capabilities is under consideration.[92] As for Norway, EUCARIS is in production/testing at the road authorities, but there is no client integration in the police yet.[93] There is a wide variety of license plates/vehicles for which a Member State may make VRD available: regular (such as cars, motorcycles, microcars and mopeds, trucks), special (for instance, agricultural and forestry, vehicles with personalised license plates, military, diplomatic, vehicles with international and EU number plates, foreign owners, police, taxi, etc) and temporary (transit/transfer, export/import, etc). Overall, registration data concerning regular vehicles is generally accessible by the law enforcement authorities in other countries.[94] However, automated searches in respect of special vehicles are highly divergent due to the wide range of vehicles and their different treatment at the national level, thus creating a convoluted landscape.[95]

Table 1: Council Implementing Decisions per country and per category of data

	DNA analysis files	Fingerprint data	Vehicle Registration Data
Belgium	Council Decision 2014/410/EU (OJ L 190/80); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision (EU) 2015/2050 (OJ L 300/17)	Prüm Treaty
Bulgaria	-	Council Decision 2010/758/EU (OJ L 322/43); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2013/230/EU (OJ L 138/12); Council Decision (EU) 2017/947 (OJ L 142/ 97)

[89] Ibid. Searches on victims' fingerprints are allowed in the Netherlands (if crime related) and Norway. Searches on fingerprints collected from relatives of missing persons are allowed in the Czech Republic and Norway.

[90] Commission, 'The implementation of Council Decision 2008/615/JHA' (n 71) 4.

[91] Council, Document 5197/1/20 REV 1 (n 66) 33.

[92] Ibid, 35.

[93] Ibid.

[94] There are few exceptions though: for instance, in Belgium there are exceptions for some protected plates, in Ireland there is no access to trailers' data, in Malta not on microcars and mopeds or trailers, in Austria not of trucks and buses, in Romania microcars and mopeds are not registered.

[95] For example, in Bulgaria and Ireland a series of special vehicles are treated as regular ones, thus providing access to their data to other countries. In the Czech Republic information on diplomatic vehicles is kept separately, administered by the Ministry of Transport and may be available after discussion with the Ministry of Foreign Affairs. In Estonia, information on diplomatic vehicles only is accessible. Finland enables access to information on diplomatic vehicles only.

Czech Republic	Council Decision 2012/58/EU (OJ L 30/12); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2011/434/EU (OJ L 190/72); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision (EU) 2017/1866 (OJ L 266/6)
Denmark	Council Decision (EU) 2016/2047 (OJ L 318/8)	Council Decision (EU) 2016/2048 (OJ L 318/10)	Council Decision (EU) 2017/618 (OJ L 89/6)
Germany	Prüm Treaty	Prüm Treaty	Prüm Treaty
Estonia	Council Decision 2012/299/EU (OJ L 151/13); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2012/710/EU (OJ L 321/61); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2014/744/EU (OJ L 308/102); Council Decision (EU)2017/943 (OJ L 142/84)
Greece	Not operational Councl Decision (EU) 2017/617 (OJ L 89/4)	Not operational Council Decision (EU) 2017/1868 (OJ L 266/10)	Not operational
Spain	Prüm Treaty	Prüm Treaty	Prüm Treaty
France	Prüm Treaty	Council Decision 2011/355/EU (OJ L 161/23); Council Decision (EU) 2017/946 (OJ L 142/93)	Prüm Treaty
Croatia	Council Decision (EU) 2018/1035 (OJ L 185/27)	Council Decision (EU) 2018/1802 (OJ L 296/33)	Council Decision (EU) 2017/1020 (OJ L 155/21)
Ireland	Council Decision (EU) 2018/1801 (OJ L 296/31)	Council Decision (EU) 2018/1839 (OJ L 298/15)	Council Decision (EU) 2019/1697 (OJ L 259/63)
Italy	Not operational	Not operational	Not operational
Cyprus	Council Decision 2012/673/EU (OJ L 302/12); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2012/672/EU (OJ L 302/11); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2014/743/EU (OJ L 308/100); Council Decision (EU)2017/943 (OJ L 142/84)
Latvia	Council Decision 2011/715/EU (OJ L 285/24); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2014/911/EU (OJ L 360/28); Council Decision (EU) 2017/944 (OJ L 142/87)	Council Decision (EU) 2016/254 (OJ L 47/8)

Lithuania	Council Decision 2011/887/EU (OJ L 344/36); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2011/888/EU (OJ L 344/38); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2012/713/EU (OJ L 323/17). Council Decision (EU) 2017/947 (OJ L 142/ 97)
Luxembourg	Prüm Treaty	Prüm Treaty	Prüm Treaty
Hungary	Council Decision 2012/445/EU (OJ L 202/22); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2012/446/EU (OJ L 202/23); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2014/264/EU (OJ L 137/7). Council Decision (EU) 2017/947 (OJ L 142/ 97)
Malta	Council Decision 2013/152/EU (OJ L 86/20); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision 2013/153/EU (OJ L 86/21); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2014/731/EU (OJ L 302/56); Council Decision (EU)2017/943 (OJ L 142/84)
Netherlands	Prüm Treaty	Council Decision 2012/46/EU (OJ L 26/32); Council Decision (EU) 2017/946 (OJ L 142/93)	Prüm Treaty
Austria	Prüm Treaty	Prüm Treaty	Prüm Treaty
Poland	Council Decision 2013/3/EU (OJ L 3/5); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision (EU) 2015/2009 (OJ L 294/70)	Council Decision 2012/236/EU (OJ L 118/8); Council Decision (EU) 2017/947 (OJ L 142/ 97)
Portugal	Council Decision 2011/472/EU (OJ L 195/71); Council Decision (EU) 2017/945 (OJ L 142/89)	Council Decision (EU) 2017/1867 (OJ L 266/8)	Council Decision (EU) 2018/397 (OJ L 71/38)
Romania	Prüm Treaty	Council Decision 2013/229/EU (OJ L 138/11); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2011/547/EU (OJ L 242/8); Council Decision (EU) 2017/947 (OJ L 142/ 97)
Slovenia	Prüm Treaty	Prüm Treaty	Council Decision 2011/387/EU (OJ L 173/9); Council Decision (EU) 2017/947 (OJ L 142/ 97)
Slovakia	Council Decision 2010/689/EU (OJ L294/14); Council Decision (EU) 2017/945 (OJ L142/89)	Council Decision 2010/682/EU (OJ L 293/58); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2013/692/EU (OJ L 319/7); Council Decision (EU) 2017/947 (OJ L 142/ 97)

Finland	Prüm Treaty	Council Decision 2013/792/EU (OJ L 349/103); Council Decision (EU) 2017/946 (OJ L 142/93)	Council Decision 2010/559/EU (OJ L 245/34); Council Decision (EU) 2017/947 (OJ L 142/ 97)
Sweden	Council Decision 2013/148/EU (OJ L84/26); Council Decision (EU) 2017/945 (OJ L142/89)	Council Decision EU 2015/2049 (OJ L 300/15)	Council Decision 2012/664/EU (OJ L 299/44); Council Decision (EU) 2017/947 (OJ L 142/ 97)
UK	Council Decision (EU) 2019/968 (OJ L156/8)	Not operational	Not operational
Norway	Not operational	Not operational	Not operational

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) (The compilation of this information has been carried out by the author)

2.4. The next generation Prüm

Article 36(4) of Decision 2008/615/JHA foresees that following the implementation of Prüm at the national level, the Commission is to provide recommendations for further development of the instrument. However, with implementation lagging behind considerably, aspirations to improve information exchange under the Prüm Decisions remained on hold. With the implementation of the Decisions coming to an end, the desire to improve the functionalities of this tool has now come to the forefront, as mentioned above. The initiative to reflect on the development of a next generation Prüm (Prüm.ng) was launched in the Council Conclusions on the implementation of the Prüm Decisions ten years after their adoption.[96] There, the Council invited the Commission to consider revising the Prüm Decisions with a view to broadening their scope and, to that end, to updating the necessary technical and legal requirements.[97] Four focus groups were established with the task of setting out how to further develop the current information exchange mechanisms and to support the Commission's feasibility study on improving information exchange under the Prüm Decisions. The three groups focused on the existing data types (DNA, fingerprints and VRD) already exchanged, whereas facial recognition was the subject of a fourth group.[98]

The revision of the Prüm framework will enable the incorporation of updated data protection rules, in line with the current EU legal framework on personal data protection, particularly Directive 2016/680. Furthermore, a key shortcoming of the Prüm framework was its incorporation into the EU *acquis* with 'no democratic control by the European Parliament and no judicial control by the Court of Justice',[99] thus lacking legitimacy and guarantees that all the public interests were equally balanced. [100] In light of the above and following the entry into force of the Lisbon Treaty that abolished the pillar structure, a

[96] Council, Document 11227/18 (17 July 2018).

[97] Ibid. 5.

[98] Council, Document 13356/19 (30 October 2019, not publicly available).

[99] European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM)2005) 490 final)' (2006) 13.

[100] See among others House of Lords (n 43); Rocco Bellanova, 'The "Prüm" Process: The Way Forward for EU Police Cooperation and Data Exchange' in Elspeth Guild and Florian Geyer (eds), *Security Versus Justice? Police and Judicial Cooperation in the European Union* (Ashgate 2008).

new generation Prüm will be negotiated pursuant to the ordinary legislative procedure and the legislative proposal will be scrutinised by the Parliament on an equal footing as the Council.

Deloitte conducted a feasibility study on improving information exchange under the Prüm Decisions that was published in May 2020,[101] proposing a wide array of possible amendments in five areas as follows:

1. Improving the automated data exchange;
2. Improving the follow-up procedure (Step 2);
3. Introducing new data categories, with emphasis on adding facial images;
4. Introducing a new IT architecture; and
5. Adding interoperability solutions.

This section will summarise the findings of the study, by emphasising on those reforms that are beyond mere technical adjustments and will provide an initial appraisal of the possibilities and risks that such enhancements may pose to the protection of fundamental rights, particularly the rights to respect for private life and protection of personal data, as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights respectively. However, from the outset it is stressed that the feasibility study is essentially a technical report, where the impact of possible reforms to the Prüm framework is only discussed to a very limited extent. As a result, **it is essential that before the proposal of any legislation an Impact Assessment be conducted** to consider the fundamental rights issues raised by the forthcoming next generation Prüm. The feasibility study cannot replace that exercise.

2.4.1. Improving automated data exchange

a. Expanding the Prüm scope

As illustrated in Section 2.3, there are significant discrepancies in the scope of the Prüm framework, as in certain Member States law enforcement authorities may launch DNA or fingerprint queries via Prüm to search for missing persons and for identifying deceased persons, if those are considered part of a criminal investigation under national legislation, whereas in others this is not possible. In order to eliminate such discrepancies in national legislations, rectify the fragmentary legal landscape at national level and enhance reciprocity in searches, the feasibility study explores the possibility of the expansion of the material and personal scope of the Prüm Decisions by allowing searching for missing persons and identifying deceased persons so as to create a level playing field across Member States.[102] The 'identification of deceased persons' encompasses two categories referred to in the previous section, namely information on unidentified persons and on unidentified human remains, which, as shown earlier, are not treated in the same manner at the national level. As a result, such reform would benefit around half the Member States which cannot use Prüm for these purposes due to restrictions in their national legal frameworks.[103]

[101] Commission, 'Study on the feasibility of improving information exchange under the Prüm Decisions (May 2020).

[102] Ibid, 21-24.

[103] The feasibility study refers to a 'limited number'. Ibid, 23. This amendment could be considered as Member States aiming at circumventing their restrictions imposed by national law, by exporting their national limitations to the EU level. On what has been termed as 'politics of scale' see Paul De Hert, 'Division of Competences between National and European Levels with Regard to Justice and Home Affairs' in Malcom Anderson and Joanna Apap (eds), *Police and Justice Cooperation in the new European Borders* (Kluwer Law International 2002) 70; also see Irene Wieczorek, *The Legitimacy of EU Criminal Law* (Hart 2020) 169-172.

However, it is recalled that automated data exchanges are allowed for the prevention and investigation of criminal offences, with emphasis on combating terrorism and cross-border crime. Whereas searches on missing persons and unidentified human bodies/remains through DNA or dactyloscopic data (or in the future, facial recognition as well) may be linked to the investigation of criminal offences and thus be covered by the current Prüm scope, this is not always the case and such searches may not be inherently linked with criminal law purposes. As a result, new purposes will have to be added to the revised Prüm legal framework, so that searches with the aim of locating missing persons and identifying human bodies/remains could take place, even if no direct link to a criminal investigation exists. Consequently, Certain Member States will be required to amend their national legislations so that the required data is first collected and stored at the national level and then automatically searched by the law enforcement authorities of other countries.

Furthermore, by including missing persons, the personal scope of Prüm will expand and that category will be added next to persons who have a criminal history or record, suspects of criminal activity and persons subject to investigation or prosecution.[104] The fact that missing persons may include vulnerable groups of individuals, such as elderly persons, persons with mental health issues or children, should be taken into account.[105] As a result, concerns are raised about the handling of data concerning missing persons in the same systems that process information on convicted criminals. Therefore, a**dditional safeguards are required in relation to the retention of such data on missing persons and the authorities granted rights to launch searches, considering that different bodies may handle those cases in comparison to open criminal investigations. Furthermore, given that the new purposes are not always linked to law enforcement different data protection safeguards depending on which category of individuals a search concerns will have to be applicable.** A way forward in that respect could be **to distinguish data exchanges concerning missing and deceased persons from those related to criminals**.[106]

As for unidentified human bodies or remains, it is noted that the scope of the EU data protection regime does not apply to deceased persons, but States enjoy the discretion to provide for rules regarding the processing of personal data of deceased persons.[107] This is currently not the case in the majority of Member States.[108] Furthermore, other rights may also come into play, such as the right to dignity, the scope of which may also vary at the national level. If the scope of Prüm is expanded to incorporate data flows related to unidentified humans, **it is worth considering how these rights will be safeguarded**.[109] Besides, as Decision 2008/315/JHA already lays down specific data protection safeguards (*lex specialis*), it is possible to provide for certain safeguards.

b. Improvements on the types of data exchanged

Improving automated data exchange further requires a series of technical reforms, such as the adoption of technical standards for exchanging biometric data,[110] as well as adjustments in all three types of data exchanged. In particular, the feasibility study discusses changes to enhance **fingerprint**

[104] Commission, 'Study on the feasibility' (n 101) 22.

[105] Ibid.

[106] Ibid.

[107] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) [2016] OJ L 119/1, recital 27.

[108] Commission, 'Study on the feasibility' (n 101) 23.

[109] Ibid.

[110] Ibid, 25-33.

efficiency through standardising the quality of fingerprint images. Indeed, the Prüm Decisions are currently vague on the quality requirements of fingerprint images, merely requiring them to be suitable for automatic matching with a national AFIS, and the Member States' quality control mechanisms vary significantly.[111] **Implementing standards on the quality of fingerprint images will enhance data quality**, which is a key principle of EU data protection law, enshrined in Article 4(1)(d) of the Law Enforcement Directive and foreseen in Article 28(2) of Decision 2008/615/JHA.

In relation to **DNA matching**, it must be noted that a hit may be reported based on six and seven matching loci to be utilised. When millions of DNA profiles may be compared, hits based on six and seven loci raise the number of false positive matches[112] 'to an unmanageable level' and therefore the minimum threshold for matching should be increased.[113] Sometimes a false-positive match can be recognised immediately, but in most cases additional DNA testing is necessary to verify or disprove a false-positive match.[114] In 2011, Van der Beek, Kloosterman and Sjerps calculated the expected number of matches for a comparison of 20,000 Dutch 7-loci and 5,000 Dutch 6-loci DNA profiles with a database of 600,000 German reference profiles, which was compared with the actual number of matches that resulted. On this basis, they concluded that 6-loci matches have a probability of 41% and 7-loci matches of 8.5% of being false positive.[115] Additional research by Van der Beek showed that the percentages of false positive matches in the Netherlands since Prüm became operational in 2008 was 67% for 6-loci matches and 5% for 7-locie matches.[116]

Whereas some experts have called for increasing the matching standards, some Prüm Member States have opposed such changes, because that could potentially lead to missing many matches. Furthermore, it is important that hits are followed-up in order to ensure that these are weeded out rigorously and avoid wrongful incrimination.[117] With such large volumes of data, six and seven loci become problematic. It is true that every reported hit must be validated and assessed for evidential value; however, Toom has reported that not every country conducts the required follow-up research, resulting, in certain cases, in the arrest of individuals in violation of due process.[118] This has led to increased calls for additional legal safeguards.[119] The feasibility study notes that 'most Member States wish to increase the number of loci used in determining matches,' and proposes a flexible approach, whereby Member States may define an alternative threshold level to be used by establishing different matching requirements as part of bilateral agreements with other Member States.[120] The flexibility in its implementation based on Member States' discretion may result in the reform becoming of no practical effectiveness.

---

[111] Ibid, 35.

[112] Toom (n 36) 18, 44.

[113] Commission, 'Study on the feasibility' (n 101) 141.

[114] Kees Van der Beek, 'Forensic DNA Profiles Crossing Borders in Europe (Implementation of the Treaty of Prüm)' (2011) https://worldwide.promega.com/resources/profiles-in-dna/2011/forensic-dna-profiles-crossing-borders-in-europe/.

[115] Michele Taverne and Tom Broeders, *The Light's at the End of the Funnel! Evaluating the Effectiveness of the Transanational Exchange of DNA Profiles Between the Netherlands and Other Prüm Countries* (Paris Legal Publishers 2015).23; Kees van der Beek, Ate Kloosterman, and Marjan Sjerps, 'De Detectie van Vals Positieve en de Preventie van Vals Negatieve Matches bij Grootschalige DNA-Databankvergelijkingen' (2011) 6 *Expertise en Recht*, 219.

[116] Van der Beek (n 114).

[117] Toom (n 36) 15,

[118] Ibid, 19. Also see Helena Machado and Rafaela Granja, 'Ethics in Transnational Forensic DNA Data Exchange in the EU: Constructing Boundaries and Managing Controversies' (2018) 27(2) *Science as Culture* 242, 252.

[119] Genewatch, 'Parliamentary vote on the Prüm Decisions: Sharing DNA profiles and fingerprints across the EU requires further safeguards' (2015).

[120] Commission, 'Study on the feasibility' (n 101) 36-37, 50.

Furthermore, the study addresses the issue of **statistical data** to allow measuring or reporting of use and accuracy. The feasibility study recommends that Prüm is updated to implement reporting requirements by laying down a minimum set of usage statistics that should be stored for all requests and responses received.[121] That way Member States and the Commission will understand and report statistics on their search usage, requests received, errors or downtime and DNA matching. As long as the statistical data do not involve personal identifiable information, the production of accurate statistics has been long awaited.[122] Reporting on the accuracy of a hit by the requesting Member State to the requested one, once it has been manually verified, is also considered as an option, so the Member States are enabled to receive and store hits for their own AFIS. Regrettably, this option is discarded due to its complexity.[123] However, from an operational perspective, such data is highly useful so as to measure the effectiveness of Prüm.

As for **vehicle data**, the feasibility study proposes a series of changes to improve process efficiency. In particular, currently when officers search for VDR, they have to mandatorily specify the license plate's country of origin. It is suggested making this field optional, so that Member States can look for matches in all national databases.[124] It must be stated that vehicle data constitute personal data to the extent that they lead to the identification of a natural person.[125] Such reform would entail the increase of data processing activities, as the automated search will take place against the data present in all Member States. As a result, the number of hits may increase. The feasibility study notes that in order to comply with the principle of data minimisation, only a core set of data (license plate, origin, brand, model and colour of the vehicle) will be provided so that the appropriate vehicle is identified.

Another important suggestion concerns the **development of an index** containing all searches per vehicle, which will become accessible to Member States,[126] which will transform Prüm for an information exchange instrument to a more proactive investigation tool. In setting up such an index, a series of considerations must be taken into account, *inter alia*, the necessity of its establishment, the elements that should be included to identify a very limited number of vehicles, the retention period, the conditions for access by requesting officers to the index, the keeping of logs of using the index and the content to which access is provided.

Moreover, the study considers the possibility of searching all vehicles registered under a single person or entity; the owner's name will only be used as a second step in the search when the input received after the first request includes the owner's name, which is not in the mandatory list of data categories that the requested Member State should report.[127] Whereas the search as a second step is welcomed, ex-post supervision by national data protection authorities should be foreseen on the basis of logs of these activities. Finally, it is proposed that vehicle colour and mileage could also be added as new categories of data; this will require Member States to collect and store such data.[128] The principles of

[121] Ibid, 36 and 47.

[122] Toom (n 36) 16-17, 42-44; Victor Toom, Rafaela Granja and Anika Ludwig, 'The Prüm Decisions as an Aspirational regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data' (2019) 41 *Forensic Science International: Genetics* 50. It is noteworthy that though Chapter 4 of Decision 2008/616/JHA foresees the production of statistical data, that data is not publicly available.

[123] Commission, 'Study on the feasibility' (n 101) 37.

[124] Ibid, 52.

[125] Law enforcement Directive, art 3(1).

[126] Commission, 'Study on the feasibility' (n 101) 55-57.

[127] Ibid, 55-58.

[128] Ibid, 58-59.

necessity, proportionality and data minimisation should be taken into account when considering this option and whether it is possible and useful to collect mileage data.[129]

2.4.2. Amending the follow-up procedure

As mentioned above, the Prüm regime foresees a two-step approach, whereby a match between data sets (hit) on the basis of automated searches is followed by mutual assistance procedures or Mutual Legal Assistance (MLA) requests. Such requests are not part of the Prüm Decision and they are governed in accordance with national laws.

The differences in national legislations and processes have led to operational inefficiencies; reported issues include lengthy follow-up procedures, using different channels of communication and without harmonisation of which data sets are to be supplied.[130] Tensions may arise in cases when a Member State issues an MLA request, but officers of different backgrounds and competencies are involved or different authorities may have custody of specific databases.[131] The final report of a research programme on the Prüm Implementation, Evaluation and Strengthening (PIES) noted in that respect that:

> '[I]n Requested Country, DNA-based information might be judicial evidence and must achieve higher standard of validity (hence the stricter reporting rule), whereas in Requesting Country, DNA-based information might be law-enforcement investigative evidence and is exploited differently than in Requested Country'.[132]

In that respect, ideas to streamline the follow-up procedure have been central in designing the next generation Prüm. In line with the focus groups, the feasibility study suggests a limited core data set is provided by default in cases of 'high-accuracy searches' of fingerprint data only.[133] That could be the case when a full set of fingerprints is checked against another full set, where the level of accuracy is generally high enough to validate a correct hit by default. For such searches, a limited set of data (name, gender, data of birth, nationality, crimes, contact details of the law enforcement authority responsible for the case) could be returned by default without human intervention. After the minimum set is received, and only where needed, Member States could request additional information on the suspect as Step 3, which will follow traditional information exchange avenues. **This intermediate step will thus introduce automaticity in follow-up requests and retrievals of the minimum data set, so that the NCP will merely validate the data and authorise their transmission.** This option entails an important advantage in that it will facilitate the MLA procedures and will enable faster access to relevant data, thus overcoming lengthy follow-up procedures and to a large extent is the true embodiment of the principle of availability.

Article 11(2) of the Law Enforcement Directive prescribes that exchange of information shall not be based solely on automated processing, including profiling, with respect to special categories of personal data, such as those envisaged in the Prüm Decisions, without safeguarding the data subject's rights and freedoms and legitimate interests being in place. Furthermore, in Opinion 1/15, the CJEU stressed that automated processing must be based on reliable, updated and relevant data and that any individual measures that may have an adverse impact should not be based solely on automated

[129] Ibid.

[130] Commission, 'Study on the feasibility' (n 101) 61.

[131] Toom (n 36) 33.

[132] PIES, 'PIES Project – 4000002150 – Final implementation report' (2016) 28.

[133] Commission, 'Study on the feasibility' (n 101) 61-64.

processing.[134] Such automaticity presupposes a high level of trust among national law enforcement authorities. It is welcome that human intervention is retained in all other searches (latent fingerprints, facial images and DNA searches). Future legislation should clarify that **any automation should be reserved only in cases where the possibility of error remains very low and adequate and efficient safeguards are established. Even in those cases, it may be useful to allow discretion for Member States to maintain manual authorisation, perhaps with a specific limited timeframe, in cases of concerns that the personal data in another Member State's fingerprint database may not be trustworthy. Furthermore, it will be useful in a forthcoming impact assessment to have information as to how often such searches take place, in order to determine in approximately how many cases time will be saved through the proposed new step**.

In that respect, it is noteworthy that the proposed reforms do not address a central concern on Prüm regarding its practical effectiveness. While many hits may be generated during Step 1, these are subject to selection, evaluation and prioritisation, resulting in drop-out of reported hits. Matches reported to investigative authorities are also subject to further selection, evaluation and prioritisation, resulting in further drop-out. As a result, many of the initially reported matches are not followed-up in Step 2 and therefore only a small percentage of the hits generated under Step 1 are used as evidence. Research on the Dutch use of the Prüm shows that although data indicated that (between 2008 to 2016) 3,876 DNA profiles were matched with data held in foreign databases, only 6% of these matches made it to court and that only 2% of the total number of matches identified were actually used in court.[135] Thus, if the 6% remained stable, approximately 230 suspects were prosecuted between 2008 and 2016; that number definitely sends a different message. In addition, there has been limited research on how many of these hits have led to convictions.[136] Overall, the available information on the effectiveness of the Prüm regime is not objective or reliable enough to evaluate its effectiveness and, consequently, its proportionality, also in view of the significant resources that the operationalisation of Prüm has required.

2.4.3. Introducing new data categories

The emergence of new technologies and investigation tools has resulted in calls to introduce new data categories in Prüm, particularly facial images, driving licenses and biographic data. The feasibility study also explores the possibility of exchanging ballistic and firearms data, but does not yet recommend an automated exchange system.[137]

a. Facial images

Facial images have increasingly become an additional biometric tool in forensics, which may be of added value in a criminal investigation for the identification of unknown perpetrators. By including facial images into Prüm, law enforcement authorities shall be able to check images (for example, taken by surveillance cameras near crime scenes) of unknown perpetrators of criminal offences against the national reference image databases, as provided for and governed by national legislation.

As with the DNA analysis files and fingerprint data, not all Member States currently hold a national central electronic image database with reference images or national Facial Recognition (FR) software, but a number of Member States are currently in the process of implementing such databases and FR.[138]

[134] Opinion 1/15, ECLI:EU:C:2017:592, paras 172-174.

[135] Toom (n 36) 17.

[136] Taverne and Broeders (n 115).

[137] Commission, 'Study on the feasibility' (n 101) 91-92.

[138] Council, Document 13356/19 (n 98) 5.

This study could not find information on how many Member States currently operate image databases. That said, the focus group on facial recognition notes that 'not a single Member State has already set up its own trace image databases with images of unknown perpetrators, which could be used regularly as a search data pool in addition to a reference picture data pool', but some Member States plan on setting up such gallery of unidentified offenders.[139] If the legal framework on the next generation Prüm is adopted prior to all Member States implementing a central electronic image database and FR software at the national level, then the setting up of databases containing facial images will become mandatory, as was the case with DNA and fingerprint databases.

The exchange of data will follow the existing rules for other types of data exchanged under Prüm, subject to specific provisions on facial images. Importantly, the forensic and technical framework and preconditions of latent fingerprints are very similar to the search technology of FR and therefore the planned processes could be intertwined.[140]

It must be emphasised that facial images constitute biometric data, thus a special category of personal data under Article 10 of the Law Enforcement Directive. Furthermore, facial images fall within the remit of Article 8 of the European Convention of Human Rights (ECHR).[141] The degree of accuracy in facial recognition technology is vital, so as to minimise the risk of **false positive matches, namely results that may be unrelated to the investigation, or false negative results, when the FR algorithm fails to identify correct matches.** This is crucial since facial recognition technology will be used in the course of criminal investigations with the aim of identifying unknown perpetrators, therefore national authorities will perform 1:N searches, which are searches on the basis of a facial image (a 'mug shot' or a probe retrieved from a camera) against the full content of other national databases[142] and the top results will be ranked. **False positive matches in particular may have important consequences for individuals, who may be** bothered by the police because of incorrect matching, be subject to criminal investigation and even be **subject to discriminatory practices** by national authorities.

Data quality is a key issue and ensuring high quality of facial images will be in line with the Prüm framework (Article 28) and Article 4(1)(d) of the Law Enforcement Directive. The feasibility study stresses that in order to ensure a minimum level of accuracy across Member States, facial images must be of 'as high-quality as possible'.[143] A 'mug shot' style image for example, which is subject to certain quality standards, will ensure high confidence matching, however probe images (latent, wild or trace images of unidentified persons) will inherently be of lower quality. Overall, having bad image data in the national gallery will affect all requests, whereas a probe image of lower quality will impact that specific request only.[144] In turn, if a high-quality database is operated, then the expected results can be more reliable.[145] In addition, Member States may already collect facial images, the quality of which may also be lower. For example, the National Institute for Standards and Technology (NIST) has found that the risk of false negative matches when using databases storing up to 1.6 million 'mug shots' and ranking the top 20 results is very low (0.15%).[146] However, testing concerned images that follow specific technical standards, hence of higher quality. Indeed, wild data sourced from various and contained in

[139] Ibid, 14.
[140] Ibid, 15.
[141] For example *Peck v UK* (2003) 36 EHRR 41; *Gaughran v UK* (Appl. No. 45245/15).
[142] That is not the same process as the verification (1:1 search).
[143] Commission, 'Study on the feasibility' (n 101) 79.
[144] Ibid, 79.
[145] Ibid, 80.
[146] Ibid, 149.

a database of 1.1 million datasets produce around 4% of false negative matches.[147] In order to mitigate this challenge, the feasibility study rightly suggests that pre-existing images in existing image galleries, as well as images from surveillance cameras, are separated from the 'primary' mug shot-quality database.[148] However, the focus group on facial recognition has opined that '(s)plitting the database in different qualities would require disproportionate technical effort and has no apparent added value'.[149] Since Member States have not already set up their own trace image galleries and in view of the risk of false positive matches, this idea should be further explored.

Furthermore, the **size of national databases** may also impact accurate identification; the higher the number of data which may be of insufficient quality, the higher the possibility of false matches. In the present case, the possibility may increase considering that the feasibility study acknowledges that 'the stock of images (image galleries), being available within the national law enforcement authorities is larger than the ones for the fingerprints and DNA'.[150] The feasibility study notes that in cases of databases storing up to 12 million 'mug shots', current technology shows resilience,[151] but as mentioned, the next generation Prüm will also allow searches of facial images that will not align to specific technical standards. Another factor that may impact the accuracy of the results is the **age of the facial image** and there is gradual increase in the possibility of a false match as the years since the capture of a facial image pass by.[152] The feasibility study suggests a series of safeguards to minimise the risk of false matches as well: laying down a maximum limit of 50 results for all requests,[153] dictating non-matched data to be deleted within a limited timeframe and allowing Member States to lower the number of candidate matches at their request.[154] The focus group has nevertheless pointed out that the number of needed candidates depends on the quality of the images and that in cases of terrorism or other serious crimes more results may have to be displayed, namely up to 100 results.[155] Finally, the inherent limitation of FR should also be underlined; though Prüm will not be used in surveillance activities by law enforcement authorities, the algorithms embedded in FR produce higher false positive matches in cases of black people, particularly of black women.[156] Therefore, as **research by the NIST demonstrates** it may be the case that in investigations people of colour may find themselves wrongly bothered by the police authorities in more cases than white people, due to algorithm bias. Therefore, **human intervention in establishing a hit must be ensured at all times.**

As for the follow-up procedure, the focus group has identified three different cooperation levels, following different response timelines; the 'classical' follow-up procedure via the existing channels and timeframes; the 'faster' supply of 'core data', whereby pre-defined certain important data will be provided following a forensic confirmation by a national expert, who confirms a possible 'match' as a real 'hit'. Replying to such a follow up request may be subject to a supplementary authorisation in the

[147] Ibid, 153.

[148] Ibid, 80-81.

[149] Council, Document 13356/19 (n 98) 16.

[150] Commission, 'Study on the feasibility' (n 101) 85.

[151] Ibid, 150.

[152] Ibid, 151.

[153] Notably some Member States want 100. Ibid, 81.

[154] Ibid.

[155] Council, Document 13356/19 (n 98) 12.

[156] Patrick Grother, Mei Ngan and Kayee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (National Institute of Standards and Technology, 2019) 63. Also see Zach Campbell and Chris Jones, 'Leaked Reports Show EU Police Are Planning a Pan-European Network of Facial Recognition Databases' (*The Intercept*, 21 February 2020) https://theintercept.com/2020/02/21/eu-facial-recognition-database/.

requested Member State on the basis of national legislation or organisational concepts.[157] The third option involves an 'automated follow-up' in cases of confirmed hits, whereby the supply of data by the requested state will no longer be dependent on an additional decision of an officer, if the requested data comply with the specified minimum data quality. As mentioned above in relation fingerprint data, such automation in data exchanges should be reserved only to cases where the possibility of false match is very low.

b. Driving licenses

Member States already exchange data on driving licenses through the RESPER application; however, this is not for the investigation of criminal offences. Furthermore, in the majority of Member States, law enforcement authorities have access to national driving license databases. Similar to the previous section, further information is needed on how many Member States allow such searches, for which offences and at which stage (prevention, investigation, or both).

c. Biographic data

Another potential development involves the possibility of including automated searches to biographic data so as to facilitate searches for personal information recorded at national level. This idea has stemmed from a pilot project named Automation of Data Exchange Processes – European Police Records Information System (ADEP-EPRIS) conducted among five Member States[158] in 2017. The scope of the project concerns the current manual process of identifying whether certain law enforcement data is available in the police records databases of a Member State. The project required the **creation of index databases containing an extract of police records with pseudo-anonymised data and launches of searches to that index are on a hit/no hit basis**. As a result, it constitutes a tool to automate the process of pinpointing the Member State where relevant police records could be present. This idea echoes previous efforts to set up a European Police Records Index System (EPRIS), which has been on the EU agenda for years, as evidenced by a study conducted in 2012.[159] The feasibility study does not touch upon privacy and data protection concerns, noting that these should be the subject of a dedicated Impact Assessment. For the purposes of this analysis, it suffices to mention that issues that will have to be discussed include: **a definition of what constitutes a police record; the necessity of setting up such national indexes and its added value, particularly in view of the work of Europol and possibilities offered by the Swedish Initiative; the amount of information included in the index; the retention period of a police record; the purposes for which it may be used**.[160]

---

[157] Council, Document 13356/19 (n 98) 6-8.

[158] These are: France, Germany, Finland, Ireland and Spain.

[159] Commission, 'Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European police records index system' (October 2012).

[160] In that respect, reference is made to Council, Document 11434/19 (6 September 2019) 7 which reads: 'While the results of the pilot so far show that the project is most likely technically feasible at EU level, some Member States voiced concerns about the performance of the project and the added value to existing systems like the Europol Information System or have indicated that granting a cross-border automated hit-no-hit access to a pseudonymised index of national law enforcement databases is not currently legally possible for them. Also, these Member States consider that the Swedish Initiative Framework Decision**1**, where the principle of availability is established, does not provide sufficient legal grounds to establish indexes and grant access to other Member States' indexes. Resolving legal issues, for example by defining a legal framework for EPRIS-ADEP type of exchanges and minimum standards for the content of data to be indexed, should be considered a priority.' The document is not publicly available but may be found here https://www.statewatch.org/media/documents/news/2019/sep/eu-council-automation-data-exchange-national-11434-19.pdf.

2.4.4. A new IT architecture?

As mentioned earlier, Prüm organises a network of information exchange on a decentralised basis. The IT architecture does not entail any central technology available at EU level to process Prüm requests and Member States must provide access to national databases. Though several Member States find the current IT architecture appropriate, limitations exist in the coverage of biometric data exchange;[161] as stressed in the Section 2.3 bilateral connection are not yet established between several countries.

Plans for a new IT architecture, for example within the 'Biometric Matching Service' (BMS), which will be established in the framework of interoperability of EU centralised information systems, have been

> 'unanimously and strictly rejected by all experts due to legal constraints on storing such data outside the national territory, as well as of forensic and organisational reasons related to work processes and quality requirements of international criminal police cooperation and crime scene stain processing'.[162]

One recommendation is to implement **a central router (hub-and-spoke solution),** which will essentially receive and send Prüm requests between Member States, instead of requiring bilateral arrangements and connections. This solution was also proposed by the High-Level Expert Group on information systems and interoperability (HLEG).[163] The central router will allow Member States to connect to and route messages to the respective matching engines of every Member State through one connection. It will thus act as a brokering service that will receive and send Prüm requests among Member States. The topology will switch from a mesh to a star architecture and the number of connections established and maintained will be significantly reduced. Another advantage will be the possibility of more easily integrating the information systems of other countries if it is so decided.[164]

Furthermore, the revised architecture will also enable the compilation of more accurate statistical data, as sometimes the number of outgoing requests by a Member State does not correspond to the number of incoming requests.[165] This is because when the router will receive the incoming request, it shall be able to extract originator and destination routing information, through which it will count the number of requests sent, received and errors, as well as timing of transactions. Similarly, when the router will forward the response by the requested Member State statistical usage information will be recorded.[166] However, such option will not enable the gathering of information on the follow-up MLA procedures and the use of Prüm hits in court proceedings as evidence.

Whereas Member States will remain in charge of the data processing operations involved (as data controllers), it must be clarified which agency (eu-LISA or even Europol) will receive the legal mandate for providing the central router and which data processing activities will fall under its mandate.[167] The distinction between a joint data controller (that determines the purposes and means of processing) and a data processor (that processes the personal data on behalf of the data controller) is crucial in that respect;[168] the revised IT architecture should not provide an EU agency access to the personal data exchanged between Member States, which is sensitive criminal investigation content. Consequently, the decryption of data should not be possible and clean data should be decrypted exclusively at the

[161] Commission, 'Study on the feasibility' (n 101) 96.
[162] Council, Document 13356/19 (n 98) 9.
[163] High-level expert group on information systems and interoperability (HLEG), 'Final report' (May 2017) 19.
[164] Commission, 'Study on the feasibility' (n 101) 102.
[165] Ibid.
[166] Ibid, 101.
[167] Ibid, 106. No private company should be involved. See Council, Document 13356/19 (n 98) 11.
[168] See Articles 21 and 22 of Directive 2016/680 (n 46).

national level. The use of data should not be allowed for other purposes than technical and statistical support of Member States.[169] Data security rules are also necessary and the EDPS should get supervision tasks.

2.4.5. Interoperability solutions

a. Implementation of interoperability

Immediately after the adoption of the interoperability legal framework,[170] discussions about whether or not it is possible to combine certain Prüm queries to the queries that will be made through the European Search Portal (ESP) under interoperability to the centralised EU information systems have been made.[171] Such addition (potentially of the fingerprint databases) to assist in police identification under Article 20 of Regulation 2019/818/EU cannot be justified, as **its purpose is the identification of a third-country national and not the prevention or investigation of offences**. Besides, **the potential for discrimination and profiling against certain groups of people could be accentuated**, particularly if facial recognition is also implemented in the future.[172] The fundamental rights implications should be analysed carefully.

b. Access to Prüm by Europol, Interpol and third countries

The final recommendations involve the possibility of opening up Prüm to new actors, such as Europol or Interpol.[173] Participation by third countries, such as acceding countries, candidate countries and potential candidates is also a possible way forward and this aspect is further analysed under Section 2.6.

In particular, Europol receives data from third countries, including biometrics, on suspected terrorists or internationally active criminals that could be compared with national reference data under Prüm rules. The possibility of giving the agency a role in the Prüm system raises a series of issues that merit further exploration. Firstly, the requirement that Europol treat those special categories of personal data as such, a safeguard which is currently missing from the Europol Regulation, must be discussed. Secondly, the relationship of Europol with third countries either by entering data received by third countries,[174] or by transferring data retrieved from participating countries to third countries requires attention. It would have to be ensured that follow-up data will not be sent from Europol to third countries without the prior information and consent of the Member State(s) concerned.[175] Overall, the issue of whether third states ensure a high level of fundamental rights protection, particularly in relation to the rights of private life and protection of personal data is central.

In relation to Interpol, concerns may be raised particularly in view of the fact the organisation is not bound by EU data protection law, which provides for high standards of protection of individuals, and Interpol partners include countries outside the EU which also safeguard personal data through their own legislations. Therefore, the inclusion of Interpol as a Prüm actor must ensure that no transfer of personal data to third countries takes place unless the Commission has adopted an adequacy decision

[169] Council, Document 11356/19 (n 98) 11.

[170] See n 17.

[171] Council, Document 10581/19 (27 June 2019); Commission, 'Study on the feasibility' (n 101) 121-126.

[172] See Niovi Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?' (2020) 26(1) *European Public Law* 131.

[173] Commission, 'Study on the feasibility' (n 101) 129-132.

[174] 'Europol: plans afoot to legalise unlawful acts' (*Statewatch*, 6 July 2020) https://www.statewatch.org/news/2020/july/europol-plans-afoot-to-legalise-unlawful-acts/.

[175] Commission, 'Study on the feasibility' (n 101) 131; Council, Document 13356/19 (n 98) 17.

ensuring the adequate level of personal data protection in that country.[176] This is particularly relevant in the case of the UK, which is examined below. That is because if Interpol is connected to Prüm, it may provide a gateway for the UK to access EU data, if the UK does not secure an adequacy decision.

2.5. The participation of the UK in the Prüm framework: Past, present and future

The UK's participation in the EU *acquis* in general and the AFSJ in particular has always been underpinned by constitutional complexity, exemplified by the existence of extensive opt-outs in the field of EU migration and criminal law.[177] With the departure of the UK from the EU, the reconfiguration of the EU-UK relationship creates additional complications. This section aims at shedding light into the current participation of the UK in the Prüm Decisions and the prospects for such participation after the end of the transitional period that ends on 31 December 2020.

2.5.1. Pre-Brexit

With the adoption of the Lisbon Treaty, the UK negotiated extended 'opt-outs' in the AFSJ, according to which the UK had the right not the participate in the whole Title V TFEU, including criminal law matters. The right to not participate also extended to legislation amending existing legal instruments which were binding upon the UK. UK concerns about the impact of the Lisbon Treaty to national sovereignty in the field of criminal justice have led to a further political compromise, which involved measures adopted before its entry into force. In particular, Protocol No. 36 on Transitional Provisions retained the pre-Lisbon limited powers of EU institutions with regard to (former) third pillar law for a transitional period of five years after the entry into force of the Lisbon Treaty. At least six months before the end of that period the UK could notify to the Council its non-acceptance of the full powers of the EU institutions in third pillar law.[178] In case of a decision not to accept these powers, third pillar law would cease to apply to the UK, but the later could notify subsequently its wish to participate in such legislation.[179] When the transitional period came to an end on 1 December 2014, the UK notified the EU Presidency that it did not accept the powers of the EU institutions, thus third pillar law would cease to apply in the UK.[180] However, the UK eventually stated that it would seek to opt back into 35 third pillar measures, including the Prüm Decisions.[181]

These extended opt-outs of the UK to criminal justice cooperation have caused significant delays in the implementation of the Prüm Decisions into the UK legal order.

In particular, in relation to **DNA analysis files**, in June 2019[182] the Council adopted Implementing Decision 2019/968 giving the green light to the UK to receive and supply DNA data in accordance with the Prüm rules.[183] This was despite the fact that the UK did not have the intention to make available dactyloscopic data of suspects, contrary to the Council expectations and contrary to similar decisions adopted by other Member States. In fact, the Commission had provided a negative opinion due to the

[176] Commission, 'Study on the feasibility' (n 101) 131.

[177] For an overview see Valsamis Mitsilegas, 'European Criminal Law after Brexit' (2017) 28 *Criminal Law Forum* 219.

[178] Protocol (No 36) on transitional provisions, art 10(4).

[179] Ibid, art 10(5).

[180] Council, Document 12750/13 (26 July 2013).

[181] For the positive view of Prüm by the House of Lords see (n 43).

[182] Following the filling of a questionnaire on data protection and on automated DNA data exchange, a pilot run, an evaluation visit and a report

[183] Council Implementing Decision (EU) 2019/968 of 6 June 2019 on the launch of automated data exchange with regard to DNA data in the United Kingdom [2019] OJ L156/8.

breach of the principle of full reciprocity. Therefore, the Council inserted a 'review clause' requiring the UK to 'review its policy on the exchange of suspects' profiles'[184] and set 15 June 2020 as the deadline to notify the Council of that outcome. The Implementing Decision makes clear the Council should 're-evaluate the situation with a view to the continuation or termination of DNA Prüm automated exchange'[185] should the notification not be made.

On 15 June 2020 the UK Government dropped its opposition to sharing criminal suspects' DNA data with EU law enforcement bodies.[186] Furthermore, by letter of 19 June 2020 the UK informed that its Government had decided to include suspects' data in its automated biometric (DNA and, as appropriate, fingerprints) data exchanges within the shareable Prüm dataset for all of the UK'.[187] This move has been eloquently referred to as the UK offering an olive branch[188] to the EU in light of the negotiations for the future relationship between the EU and the UK on security aspects, including information exchange.

In parallel to these developments, on 2 December 2019 the JHA Council formally approved the UK's participation in the Prüm system in connection to **fingerprint data**, concluding that the UK is, in principle, ready to exchange fingerprint data with the other EU Member States that are part of the Prüm network.[189] In its conclusions, the JHA Council reiterated, however, the deadline set for the UK to review its policy of excluding suspects' dactyloscopic files.[190] It is noteworthy that on 11 May 2020, the Parliament Rapporteur proposed the rejection of the draft decision on Prüm fingerprint data exchange with the UK for a series of reasons: a) the (at that time) pending issue of excluding data from suspects from data exchanges; b) it makes no sense due to the forthcoming end of the transition period on 31 December 2020, as long as no new legal framework for the new partnership cooperation with the UK has been concluded (see below); and c) the Parliament did not receive the evaluation report summarising the results of the questionnaire, the evaluation visit and the pilot run concerning dactyloscopic data exchange that were presented to the Council;[191] a Resolution was adopted in that respect on 13 May 2020.[192] In the end, a Council Implementing Decision was formally adopted on 6 August 2020.[193]

As for **vehicle registration data**, as mentioned earlier, at the time of writing the UK is not yet operational.

2.5.2. From 1 January 2021 onwards

On 31 January 2020, the UK left the EU and the Withdrawal Agreement concluded with the EU entered into force. On 31 December 2020, the transitional period will terminate, after which EU law will cease to apply and the UK will become a third country. Although the future relationship between the UK and

[184] Ibid, recital 9.

[185] Ibid, art 2.

[186] See Council, Document 8879/20 (19 June 2020).

[187] Ibid.

[188] Jennifer Rankin, 'UK Agrees to Share Suspects' DNA with EU Crime-Fighting System' (*The Guardian*, 15 June 2020) https://www.theguardian.com/politics/2020/jun/15/britain-agrees-share-suspects-dna-eu-crime-fighting-system.

[189] Council, Document 14755/19 (2-3 December 2019).

[190] Council, Document 14744/19 (2 December 2019).

[191] Parliament, 'Report on the draft Council implementing decision on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom (14247/2019 – C9-0198/2019 – 2019/0819(CNS)) (8 May 2020)'.

[192] Parliament, 'European Parliament legislative resolution of 13 May 2020 on the draft Council implementing decision on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom (14247/2019 – C9-0198/2019 – 2019/0819(CNS)).

[193] See n 80.

the EU was not discussed in the Council conclusions of December 2019, which gave the green light to the UK's participation in the Prüm system in relation to dactyloscopic data, or in other EU documents,[194] negotiations for a **new partnership agreement** are underway since March 2020.[195] It is clear that maintaining police and judicial cooperation is a priority for both the EU and UK and the continued efforts of the UK to implement the Prüm Decisions even after it had decided to leave the EU indicate the UK interest in maintaining access.

In its policy paper on the **UK's approach** to the future EU-UK relationship, the UK expressed its interest to conclude an agreement on law enforcement and judicial cooperation in criminal matters, including arrangements that support data exchange for law enforcement purposes.[196] The UK position maintains that any agreement on law enforcement cooperation 'should not provide any role for the Court of Justice of the EU in resolving UK-EU disputes,' which is consistent with the EU's approach to cooperation with third countries on law enforcement and judicial cooperation in criminal matters, including between the EU and neighbouring non-EU countries on tools such as the Schengen Information System (SIS) and Prüm.[197] Furthermore, the agreement should not specify how the UK or the EU Member States should protect and enforce human rights and the rule of law within their own autonomous legal systems. In connection to the Prüm decisions, the UK posits that the agreement should provide for the fast and effective exchange of national DNA, fingerprint and vehicle registration data between the UK and individual EU Member States under similar capabilities to those currently delivered through the Prüm system, drawing on the precedent for such cooperation between the EU and the Schengen Associated States. These precedents include a political dispute resolution mechanism with no jurisdiction in those third countries for the CJEU.

The extent to which Prüm-like cooperation is of mutual added value is illustrated by the following: the UK national DNA database (NDNAD) is the oldest national forensic database worldwide, established in 1995,[198] and currently holds profiles of more than 5 million people and 500,000 samples from crime scenes,[199] which makes it the largest measured by the proportion of citizens on the database (over 8.2%)[200] The report on the state of play of the Prüm framework from February 2020 indicates that the UK has been operational in connection to DNA analysis files since July 2019 with Austria, Germany, Spain, France, the Netherlands and Poland.[201] By June 2020, the UK was connected to nine countries.[202] In this short period of time it has been reported that around 12,000 initial hits have been identified relating to UK investigations, whereas EU Member States have received approximately 41,000 initial hits from matching their data with that held by the UK. These exchanges have already been fruitful in

---

[194] Council, Document 12511/19 (8 October 2019) not publicly available but retrieved in https://www.statewatch.org/media/documents/news/2019/nov/eu-council-uk-prum-fingerprints-report-12511-19.pdf.

[195] This is indeed the most desirable scenario in comparison to alternative arrangements, such as bilateral agreements between the UK and individual Member States or falling back to existing Council of Europe mechanisms of co-operation. See Mitsilegas, 'European Criminal Law after Brexit' (n 178) 241-246.

[196] UK Government, 'The Future Relationship with the EU – The UK's Approach to Negotiations' (February 2020) 24-25.

[197] Ibid, 25.

[198] Toom (n 36) 22. For an analysis see Carole McCartney, 'Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach' (2004) 12 *Critical Criminology* 157; Robin Williams and Paul Johnson, *Genetic Policing: The Use of DNA in Criminal Investigations* (Willan Publishing 2008).

[199] 'UK and EU Law Enforcement Boost Co-Operation on DNA Databases' (*UK Government*, 13 June 2019) https://www.gov.uk/government/news/uk-and-eu-law-enforcement-boost-co-operation-on-dna-databases.

[200] Aaron Opoku Amankwaa and Carole McCartney, 'The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012' (2018) 284 *Forensic Science International* 117. By way of reference, the Dutch and Portuguese databases hold approximately 1.6% and 0.02% of the population. See Filipe Santos, Helena Machado and Susana Silva, 'Forensic DNA Databases in European Countries: Is Size Linked to Performance?' (2013) 9(1) *Life Science, Society and Policy* 12.

[201] Council, Document 5197/20 (21 February 2020) 20.

[202] Council, Document 5197/1/20 REV 1 (n 66) 19.

the UK, as an unidentified crime stain from a sexual assault in Glasgow in 2012 was identified as a subject convicted for theft offences in Austria.[203] In light of the above, it will be of added value to enable national law enforcement authorities to automatically search the NDNAD.

Consequently, unsurprisingly, the new partnership agreement, the latest publicly available draft of which is from 14 August 2020, features provisions on the exchange of DNA, dactyloscopic and vehicle registration data under rules that largely replicate those in Decision 2008/615/JHA.[204]

In order for the UK to maintain such relationship in police and judicial cooperation, any transfer of personal data to the UK may take place where the Commission has decided in accordance with Article 36 of the Law Enforcement Directive that the UK (or one or more relevant specified sectors within the UK) ensures an adequate level of protection. That term has been clarified by the CJEU in the case of *Schrems* as meaning that the level of data protection should be 'essentially equivalent' to that offered by the EU.[205] As a result, in order for the Commission to declare the adequacy of the UK data protection framework, it must demonstrate that the UK provides a level of protection 'essentially equivalent' to that offered by EU legal framework, including on onward transfers to third countries.[206] Although *Schrems* involved the transfer of personal outside the scope of law enforcement, the interpretation of the term 'adequate' level of personal data protection ought to be the same across the field of EU data protection law. In its assessment of whether to grant the UK an 'adequacy decision', the Commission will have to take into account an array of requirements and concerns regarding the UK legal framework on the protection of fundamental rights, including (but not limited to) the rights to private life and protection of personal data. Without pre-empting the outcome of the negotiations, an anthology of such issues is concisely provided below:

a. Data protection standards

Whereas the UK's status as a former EU Member State signifies that it already applies the GDPR and the Law Enforcement Directive,[207] any substantial deviation from the EU data protection rules could amount to an obstacle to a finding of adequacy, provided that such deviation lowers the level of protection of personal data afforded in the UK.[208]

---

[203] UK Parliament, 'Prüm – Data Sharing Update: Written statement - HCWS290' (15 June 2020).

[204] 'Amended draft text of Title I Part III of the Agreement on the New Partnership with the United Kingdom and its Annexes LAW-1 to LAW.7' (14 August 2020) https://ec.europa.eu/info/sites/info/files/additional_draft_text_of_the_agreement_on_the_new_partnership_with_the_united_kingdom_14_august_2020_law_enforcement_and_judicial_cooperation.pdf. The draft agreement does not foresee exchanges in cases of major events or terrorist events or joint operations.

[205] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

[206] See also Parliament, 'European Parliament recommendation of 18 June 2020 on the negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland (2020/2023(INI))' (18 June 2020).

[207] Data Protection Act 2018.

[208] In that respect see EDPS, 'Opinion 02/2020 – EDPS Opinion on the opening of negotiation for a new partnership with the UK' (February 2020). On the UK views see UK Parliament, 'UK / EU relations: Written statement - HCWS86' (3 February 2020) where the UK Prime Minister notes that the UK will develop separate and independent policies in the field of personal data protection. Also see UK Government, Department for Digital, Culture, Media and Sport, 'Explanatory framework for adequacy discussions' (13 March 2020) https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions; UK Government, Department for Digital, Culture, Media and Sport and The Rt Hon Oliver Dowden CBE MP, 'Digital Secretary's closing speech to the UK Tech Cluster Group' (23 June 2020) https://www.gov.uk/government/speeches/digital-secretarys-closing-speech-to-the-uk-tech-cluster-group.

b. ECHR

Furthermore, in the first round of negotiations, the UK had informed that with regard to police and judicial cooperation, it will not commit to enforce the ECHR.[209] Be that as it may, it should be noted that the latest draft of the EU-UK partnership agreement contains Article 3, which explicitly refers to the obligation to respect fundamental rights and fundamental legal principles, as enshrined in the ECHR.[210]

c. Use of SIS

Another issue relates to the identified serious deficiencies in relation to its use of SIS, with the Parliament considering that the modalities of the future cooperation between the EU and the UK in the area of law enforcement may only be discussed once the deficiencies are remedied.[211] Thus, one might argue that the degree of trust to the UK has already been somewhat damaged.

d. Cooperation with the US

The UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, signed on 3 October 2019, is also a central matter of concern, particularly with regard to the requirement to ensure continuity of protection in case of 'onward transfers' from the UK to another third country'.[212]

e. Surveillance practices

Finally, the UK approach to accessing personal data for reasons of national security is also important.[213] Central in that context is the width of the Investigatory Powers Act 2016, which has already been the subject of European litigation in *Tele2 and Watson* on the retention of telecommunication data by the CJEU[214] and *Big Brother Watch* by the European Court of Human Rights (ECtHR).[215] Furthermore, on 15 January 2020, in his Opinion in the case of *Privacy International*, currently pending before the CJEU, Advocate General Campos Sánchez-Bordona found that the bulk data collection allowed by the Act is unlawful.[216] Furthermore, the judgment of 17 July 2020 in *Schrems II* [217] is relevant here. The CJEU has clarified that in assessing whether a third country offers an 'adequate' level of personal data protection the intrusiveness of the surveillance programmes undertaken by its law enforcement, including intelligence services, are central. As it has been rightly pointed out, the judgment serves as 'a warning

[209] Parliament, 'Report' (n 192) 8.

[210] See 'Amended draft text' (n 205) art 3.

[211] Nikolaj Nielsen, 'UK Unlawfully Copying Data from EU Police System' (*EUobserver*, 28 May 2018) https://euobserver.com/justice/141919; 'UK Taking 'Steps' after Illegal Copying of EU Schengen Data' (*EUobserver*, 25 July 2019) https://euobserver.com/justice/145530; 'MEPs Slam UK for Violating EU Police Database' (*EUobserver*, 10 January 2020) https://euobserver.com/justice/147084.

[212] European Data Protection Board (EDPB), 'EDPB response to MEPs Sophie in't Veld and Moritz Körner n the US-UK agreement under the US Cloud Act' (15 June 2020). The Chair of the European Data Protection Board (EDPB) has noted that in the event of a conflict between the agreement and the CLOUD Act (particularly its Section 3), which implements the agreement in the US, it is unclear as to whether the safeguards enshrined in the UK-US Agreement will prevail

[213] 'EDPB Casts Doubt over GDPR Adequacy Decision for the UK' (*Finextra*, 17 June 2020) https://www.finextra.com/newsarticle/36043/edpb-casts-doubt-over-gdpr-adequacy-decision-for-the-uk.

[214] Joined Cases C- 203/15 and C- 698/15 *Tele2 Sverige AB v Post-och telestyrelsen* (C- 203/15) and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* (C- 698/15) ECLI:EU:C:2016:970.

[215] *Big Brother Watch v UK* (Appl. Nos 58170/13, 62322/14 and 24960/15).

[216] Case C-623/17 *Privacy International* (pending).

[217] Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559.

shot' for the UK,[218] the domestic surveillance programmes of which may be deemed to be intrusive from an EU data protection law standpoint.

If the UK is not granted an adequacy decision, a partial adequacy decision concerning specific information exchange instruments, such as Prüm, is possible. However, the UK practices on facial recognition may play a role in determining the level of personal data protection offered in the UK.[219] In addition, Article 37 of the Law Enforcement Directive foresees transfers of personal data subject to appropriate safeguards in a legally binding document, or where the data controller has assessed all the circumstances surrounding the transfer of personal data and concluded that appropriate safeguards exist with regard to the protection of personal data. With such clear duties, it may be difficult for transfers of Prüm data to the UK unless appropriate safeguards are embedded in the Partnership Agreement or outstanding concerns are resolved. **Finally, another option for the UK is to seek access through Interpol, as mentioned above.**

2.6. Cooperation with the Western Balkans

Centralised and decentralised channels of information exchange are traditionally reserved to EU Member States and, therefore, third countries outside the EU cannot have direct access to the data stored. Schengen Associated States constitute an exception to that rule, but since the Prüm system is not part of the Schengen *acquis*, those countries can only join on the basis of separate agreements with the EU.

On top of challenges regarding the UK participation to the Prüm Decisions, another outstanding issue concerns the possible cooperation with the Western Balkans. Western Balkans are comprised of: Albania, Northern Macedonia, Serbia and Montenegro, which are EU accession candidates, whereas Bosnia and Herzegovina and Kosovo are considered potential candidate countries. All governments therefore receive so-called Pre-accession Assistance for the development of police and border police capabilities. Such assistance is based on a Stabilisation and Association Agreement that the countries have concluded with the EU. For example, in EU's efforts to deepen and expand cooperation with the Western Balkans in police investigations, a Joint Action Plan on counter terrorism for the Western Balkans has been drawn, defining five priority areas, including 'countering violent extremism and 'exchange of information and cooperation'.[220] This Action Plan is in line with the Commission vision for enhanced strategic and operational cooperation, whereby '[l]aw enforcement cooperation and information sharing at national and at regional level among Western Balkan partners should […] be enhanced'.[221]

Strengthening cooperation with the Western Balkans was one of the main priorities of the then Austrian Presidency in 2018. These efforts culminated in the Police Cooperation Convention for Southeast Europe (PCC SEE) signing on 13 September 2018 of a 'Prüm Agreement for South-East Europe' on the automated exchange of DNA, fingerprint and vehicle registration data. The Prüm-like agreement is accompanied by a memorandum of understanding that outlines the key elements of the

[218] 'What the Schrems II Ruling Means for Brexit' (*After Brexit*, 16 July 2020) https://afterbrexit.tech/opinions/what-the-schrems-ii-ruling-means-for-brexit/.

[219] David Davis, 'Facial Recognition Technology Threatens to End All Individual Privacy' (*The Guardian*, 20 September 2019) https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy; Owen Bowcott, 'UK's Facial Recognition Technology 'Breaches Privacy Rights' (*The Guardian*, 23 June 2020) https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights.

[220] Joint Action Plan on Counter-Terrorism for the Western Balkans (5 October 2018).

[221] Commission, 'A credible enlargement perspective for and enhanced EU engagement with the Western Balkans' COM(2018) 65 final, 10.

commitment by the Contracting Parties and further consolidates an effective and sustainable development of the new framework.[222] The first signatories at that time included a mixture between EU Member States (Bulgaria, Austria, Romania, Slovenia and Hungary) and third countries (Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Moldova and Serbia). The aim of the agreement is on the one hand to enhance cooperation years before all the non-EU contracting parties accede the EU and on the other hand, to contribute to EU accession efforts of those countries, as Prüm readiness constitutes a precondition for closing the negotiations on Chapter 24. Other EU Member States may connect as well; according to Article 23(2) of the Agreement, '[o]nce a positive evaluation of a Party in the context of this Agreement (Article 21) or the European Union has been made, the respective Party is entitled to apply this Agreement immediately in relation to all other Parties which also have been evaluated positive'. In that respect, Toom, Granja and Ludwig are concerned about the emergence of Prüm as an 'aspirational regime', in constant development, which is 'based on an overall lack of available, relevant, accurate and comparable data' to concretely enable the objective, independent and systematic analysis of the Prüm's contribution to its stated purposes.[223]

It must be noted that the third countries involved in this agreement are in an accession trajectory and therefore beginning their connection with Prüm is indeed within their obligations for accession. Thus, as long as the relevant data protection rules are respected and the degree of their connection with the EU remains high, this way forward seems to make sense. However, concerns are raised as to whether such cooperation may take place without the EU involvement. In this regard, in October 2019, the Commission decided to launch infringement procedures by sending letters of formal notice to Austria, Bulgaria, Hungary and Romania for signing the agreement.[224] The Commission considers that the agreement is in breach of EU exclusive competence in the area under Articles 3(2) TFEU, particularly because the exchange of such data between the Member States is covered by the Prüm Decisions. The Member States concerned had two months to reply to the arguments raised by the Commission, however, at the time of writing, the case remains active, without any progress made in 2020. It is noteworthy that the evaluation prior to allowing automated exchange (on the basis of evaluation visits, pilot runs, replies to questionnaire) will be conducted by the contracting parties themselves. As a result, the role of EU institutions (the Council adopting an Implementing Decision with the Parliament being consulted) may be marginalised, as such evaluations will have already taken place prior to the formal accession of those states to the EU. Nevertheless, on the South-East Europe front, informal negotiations to amend the agreement are underway.[225]

Similar to that initiative, but not within the remits of the Prüm Decisions, are the bilateral agreements that many EU Member States (as well as other countries) have made to connect their databases with the US Combined DNA Index System (CODIS). In particular, in 2014, Belgium, Austria, Switzerland, Czech Republic, Germany, Netherlands, Finland, Spain, Estonia, Greece, Denmark and South Korea made such arrangements with the US, but DNA has thus far not been exchanged.[226]

---

[222] Agreement between the Parties to the Police Cooperation Convention for Southeast Europe on the Automated Exchange of DNA Data, Dactyloscopic Data and Vehicle Registration Data and its Implementing Agreement (13 September 2018).

[223] Toom, Granja and Ludwig (n 122).

[224] Commission, 'October Infringements Package: Key Decisions' (13 October 2019) INF19/5950 https://ec.europa.eu/commission/presscorner/detail/EN/INF_19_5950.

[225] Police Cooperation Convention for Southeast Europe, 'Informal Negotiations to Amend the PCC Prüm Agreement' (27 May 2020) https://www.pccseesecretariat.si/index.php?page=news&item=7&id=997&type=arhiv.

[226] Toom, Granja and Ludwig (n 122) 55.

3. THE API DIRECTIVE

3.1. An outline of the API Directive

Advance Passenger Information (API) concerns the information of an air passenger taken at check-in at the airport or at the time of online check-in, and includes biographic data of the passenger and some flight-related information. Council Directive 2004/82/EC (API Directive) regulates the collection and transmission of API data in the 32 participating countries, including the UK and the four Schengen Associated States. It obliges air carriers to transmit upon request passenger data to the Member State of destination prior to the take off of the flight, or shortly after if that flight is inbound from a third country. [227] The principal objective of the API Directive is to improve border control and combat irregular migration,[228] but the Directive allows the use of API data for law enforcement purposes on the basis of national law.[229] The Directive only sets minimum standards for the Member States to request API data and Member States are free to also request similar data from other transport carriers, such as maritime or rail transport carriers.[230]

In the meantime, Directive 2016/681 was adopted concerning the use of Passenger Name Record (PNR) data for law enforcement purposes, which also requires the transfer of API data, if collected as part of PNR data by air carriers.[231] However, whereas the primary purpose of the API Directive is border control and the fight against irregular migration, the PNR Directive is the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[232] Therefore, the linkage between the two instruments is strong.

On 5 September 2006, the deadline for transposing the API Directive expired and an evaluation report in that respect was released in 2012.[233] In February 2020, a second evaluation report, conducted by ICF in cooperation with Unisys, was released with the aim of providing an updated assessment of the implementation, relevance, effectiveness, coherence and EU added value of the Directive 15 years after its adoption.[234] Furthermore, at the time of writing, an impact assessment for a revised API Directive is undertaken by ICF.

3.2. The state of implementation

In 2019, when the study was carried out, 25 out of the 32 Member States had functioning API systems in place, two Member States were in pilot phase[235] and another four were planning to introduce an API system by 2020.[236] Overall, whereas the study concludes that the API Directive has been adequately transposed, a series of articles have flagged conformity assessment issues, particularly:

[227] API Directive, art 3.

[228] Ibid, art 1.

[229] Ibid, art 6(1) last subparagraph.

[230] Ibid, recital 8.

[231] See (n 15).

[232] Ibid, Annex I.

[233] Commission, 'Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82' (17 September 2012).

[234] Commission, 'Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data' (February 2020).

[235] These are: Belgium and Slovakia.

[236] These are: Cyprus, Greece, Iceland, Norway.

- Article 1, on 'Objectives', whereby half of the Member States have gone beyond those two requirements;[237]
- Article 2, on 'Definitions', with 13 Member States not having transposed one or more definitions;[238] and
- Article 6, on 'Data Processing'. This article imposes the obligation for carriers to transmit the data for border control and irregular migration and sets out the rules applicable to the processing of the API data collected, including data protection safeguards.[239] It also allows Member States to use API data for law enforcement purposes. For more than half of the Member States, the transposition is problematic.[240]

Overall, Slovenia is the only Member State to be in full conformity with the Directive.[241] However, significant discrepancies are observed as a result of the adoption of new legislation on border management, such as the legal instruments on EU information systems, passenger information (particularly the PNR Directive) and EU data protection law.

3.3. The use of API data for law enforcement purposes

Of particular importance for the purposes of this in-depth analysis are the findings of the study concerning the use of API data for law enforcement purposes. As mentioned above, Article 6(1) last subparagraph foresees the possibility of using API data for law enforcement purposes, when the use of such data is authorised by national law, but implementation of this option is left at Member States' discretion. Almost all Member States have made use of this discretion, with the Netherlands and Slovenia being the only two Member States that have not taken up that option.[242] Overall, the study found that 29 Member States collect API data with the aim of combating irregular immigration (with the exception of Bulgaria and Sweden), 29 collect API data for improving border control purposes (with the exception of Bulgaria and Hungary, in 21 Member States API data are being used for the purposes of law enforcement[243] and in 15 for fight against terrorism.[244] No Member State has provided the rationale behind its choice.[245] Member States are using API data for law enforcement purposes in different ways: to match API data against national counter-terrorism and counter-organised crime databases; comparing API data against the SIS, including alerts on discreet checks; matching against foreign counter-terrorism databases;[246] and processing of API data jointly with PNR to match risk profiles and criteria for the purposes of identifying possible criminal behaviour or participation in terrorist acts - in this process, the API data is primarily used to verify the PNR-based analysis and profiling. The API data is rarely, if at all, used to match pre-defined risk profiles.[247]

---

[237] Commission, 'Study on Advance Passenger Information (API) (n 234) 30-31.

[238] Ibid.

[239] These are: that the collected data in a temporary file (Article 6 (1) second subparagraph; 2) that the authorities to delete the data within 24 hours after transmission (Article 6(1) third sub-paragraph; that carriers must delete data within 24 hours of the arrival of the means of transport (Article 6(1)fourth sub-paragraph; and the right to information enjoyed by passengers (Article 6(2)).

[240] Commission, 'Study on Advance Passenger Information (API) (n 234) 33-34.

[241] Ibid, 30.

[242] Ibid, 35.

[243] Ibid, 183. These are: Austria, Belgium, Switzerland, Czech Republic, Denmark, Estonia, Greece, Spain, France, Croatia, Latvia, Lithuania, Slovakia, UK, Romania, Finland, Iceland, Germany, Cyprus and Luxemburg.

[244] Ibid. These are Austria, Belgium, Czech Republic, Denmark, Estonia, Greece, France, Croatia, Latvia, Lithuania, Sweden, Slovakia, UK, Germany and Cyprus.

[245] Ibid, 35.

[246] Ibid, 73. Two Member States (Bulgaria and Italy) have reported on such use, although others are likely to match data against major databases maintained by the United States as well.

[247] Ibid, 73.

The use of API data for law enforcement purposes has proved to be one of the most problematic issues of the Directive; In addition to the prescriptions of that Directive, the PNR Directive has established the obligation for air carriers to transmit API data, as well as flight reservation data, where API data are collected in the normal course of their business. As a result, the processing of API data at EU level is governed by two separate instruments. In practice, this means that where API data is collected by the authorities within the framework of the PNR Directive, it must be treated as PNR data. In practice, API data has enhanced the reliability of PNR data, due to its 'typically verified nature' when collected through MRZ (Machine-Readable Zone). In turn, with the discretionary nature of the clause of the API Directive several discrepancies between the two legal instruments are created, causing incoherence with regard to the applicable data protection safeguards and operational challenges at practical level.

In particular, **the API Directive lacks a definition of what 'law enforcement' purposes may encompass**; national implementation of this purpose at the national level varies from enhancing internal security and public order, to fight against terrorism and national security.[248] The following examples are illustrative of the convoluted landscape: in Cyprus, API data may also be used to investigate offences leading to imprisonment sentence of one year or more (three years or more in Slovakia). In the case of Austria, API data may be transmitted to another security authority in case of suspicion of a criminal offence. In the UK, the national transposing regulation goes beyond the objectives of the API Directive by including law enforcement and intelligence as one of the ultimate goals.[249] These examples denote an understanding of the concept of law enforcement that is wider than the material scope of the PNR Directive,[250] which involves the use of data for the prevention, detention, investigation and prosecution of terrorist offences, as defined in Directive 2017/541[251] and serious crime, as listed in Annex II of the PNR Directive, that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State.[252]

Another source of contradiction is that **the API data elements do not entirely match** in both Directives. In particular, the API Directive provides a non-exhaustive list of data elements, which leaves each Member States the right to request additional data in line with national legislation.[253] PNR Directive provides for different API data elements than API Directive, stating '(a)ny advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)'. For example, gender is not a mandatory API data element included in the API Directive.[254]

Additionally, **the two instruments do not apply to the same type of flights**; in some Member States air carriers have the obligation to send PNR data (and API data if available) for intra-Schengen flights, while the API Directive does not prescribe the collection of API data for such flights.[255]

Importantly, in relation to the **data retention period**, Article 6(1) third sub-paragraph of the API Directive prescribes that API data should be deleted within 24 hours after transmission, 'unless the data

[248] Ibid, 56.

[249] Ibid, 182.

[250] Ibid, 62.

[251] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

[252] PNR Directive, art 3(9).

[253] API Directive, art 3(2).

[254] Commission, 'Study on Advance Passenger Information (API) (n 234) 62.

[255] Ibid.

are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders'.[256] However, no requirements on the data retention period are foreseen for the use of API data for law enforcement purposes and this issue is left for determination in national laws. Therefore, the Directive is unclear as to whether the 24-hour limitation should also be applicable when processing of API data for law enforcement purposes, or whether the retention period should be different if data is used for a different purpose. In practice however, a majority of Member States apply the provisions of the PNR Directive, (also due to the joint collection of API and PNR data)[257] according to which API data can be stored by national authorities for a period of five years after the transfer when they are collected as part of PNR data.[258]

The evaluation study concludes that there is need for more clarity and coherence in relation to the law enforcement scope of the API Directive when implemented in conjunction with the PNR Directive. In order to reconcile these two instruments the study proposed the establishment of what is referred to as the 'single window' model to receive both API and PNR data,[259] as well as 'targeting centres' to receive all forms of passenger data in one single entry point. Through a 'targeting centre' a Member State may conduct risk assessment of travellers based on personal data stemming from different sources (such as EU information systems and API data) through 'tactical risk analysis' in order to detect unknown persons of interest before they come to the border.[260] This border control approach is already followed by the US and Canada, but there these capacities in Europe are not as widespread (with the UK being one such example).[261]

The study notes that 13 Member States use the 'single window' model, according to which API data are sent to the Passenger Information Unit (PIU) by the push method, which typically acts as the targeting centre.[262] For example, in Ireland the PIU is the targeting centre for both API and PNR data; whereas API data is checked against immigration control information systems, PNR data is checked for threats related to terrorism and serious crime. In the Netherlands, API data is processed by the border authorities, while PNR data by the PIU.

Overall, these efforts to create the conditions of convergence between the two Directives are underpinned by a key question: does it make sense to keep API and PNR data streams separate, or do the different purposes to use the data and the authorities involved necessitate a distinction between the two instruments? Whereas it is true that the passenger information landscape has changed significantly, thus numerous inconsistencies among these legal instruments exist and detailed rules on personal data protection are missing, it must be emphasised that the PNR framework is currently under scrutiny by the CJEU; on the one hand, Opinion 1/15 struck down the draft EU-Canada Agreement on the transfer and use of PNR data to prevent and combat terrorism and other serious transnational crime.[263] On the other hand, 31 October 2019 the Belgian Constitutional Court referred to the CJEU submitted before the Court a series of questions for preliminary ruling regarding the compatibility of

[256] This provision has not been implemented correctly. On its implementation see ibid, 34-35.

[257] Data so far indicates that 14 Member States process PNR and API data (as collected as part of PNR) together, while 15 do not. Ibid, 70.

[258] Ibid, 51.

[259] According to ICAO93, the single window concept should apply to each form of passenger data that an airline is obliged to transmit to the requesting authority, i.e. Advance Passenger Information (API), interactive API (iAPI) and/or Passenger Name Record (PNR).

[260] Commission, 'Study on Advance Passenger Information (API) (n 234) 39.

[261] Ibid.

[262] Ibid. The study acknowledges that the set up varies across Member States.

[263] Opinion 1/15 (n 134).

the PNR Directive with the rights to respect for private life and protection of personal data.[264] On 20 January 2020, another request for reference ruling was filed by the District Court of Cologne.[265] Therefore, a revision of the API Directive to match the PNR Directive may be premature.

3.4. Interoperability of API data with EU information systems?

With API data deemed as an important tool for facilitating border control as it allows for faster clearance of passengers, another key question emerges: what is the role of API data in the emerging interoperability framework? In its Communication on Stronger and Smarter Information Systems for Borders and Security, the Commission emphasised that in line with existing best practice, Member States should increase the added value of API by establishing automated cross-checking against SIS and Interpol's Stolen and Lost Travel Documents (SLTD) database.[266]

The API evaluation report briefly mentions that with the introduction of the ESP, via which API data could be matched against multiple databases, the potential for countering terrorist threats may grow.[267] However, no further remarks are made in that respect. Furthermore, the report finds that API data will play a central role in interoperability, as implemented by the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS). In particular, Member States currently receive API data in a batch format exchanged directly between the airline and the Member State. However, upon establishing the EES and the consequent abolition of stamping, carriers will no longer be able to know whether a visa was used or not by a third-country national. In that respect, a 'carrier gateway' will be set up and carriers will have to consult the EES to verify whether third-country nationals holding a Schengen visa for one or two entries will have already used the number of entries authorised by their visa. Similarly, when the ETIAS becomes operational, carriers will similarly have to verify the status, including the validity of an ETIAS travel authorisation.[268] The aforementioned developments will require several changes at technical level as to how API data is collected and the industry-recommended technology for facilitating this is an interactive API (iAPI), so that API data will be sent once through a single point (the carrier gateway) to different destinations, both centralised systems and national systems.[269] However, though the development of iAPI is supported by representatives from the EU institutions and industry associations, several Member States are sceptical due to the number of expected implementing challenges, such as the lack of financial resources and insufficient analytical and processing capacity.[270] It must be noted that these considerations are in line with the conclusions of the HLEG that has stressed that in the future, interactive API data will be necessary to enable carriers to check a travel authorisation and to check remaining authorised stay.[271] The HLEG further pointed out that Member States could opt, on a voluntary basis, for a single router or

[264] Case C-817/19 *ASBL 'Ligue des Droits Humains'* (pending).

[265] Case C-222/20 *Bundesrepublik Deutschland* (pending).

[266] Commission, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205 final.

[267] Commission, 'Study on Advance Passenger Information (API) (n 234) 75.

[268] For both systems, such checks will be carried out through the introduction of the Interactive Query. See Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L 327/20, art 13; Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L 236/1, art 45.

[269] Commission, 'Study on Advance Passenger Information (API) (n 234) 61.

[270] Ibid, 62.

[271] HLEG, 'Final report' (n 164) 39.

hub (an API hub), perhaps hosted by eu-LISA, that could collect such data from carriers and transfer them to the relevant central and national entities.[272]

[272] Ibid.

4. POLICY RECOMMENDATIONS

Based on the analysis presented in this study, this section lays down key policy recommendations, so as to inform the EU legislature when revising the Prüm rules and the API Directive.

4.1. Recommendations concerning the Prüm framework

- With respect to the Prüm framework, the study has demonstrated that the implementation is currently in its final stages, with few Member States currently non-operational. However, the degree of operational connectivity among operational Member States varies significantly. As a result, law enforcement authorities in certain Member States perhaps are not able to contribute to the debate about a possible revision of the Prüm system due to lack of first-hand experience. Therefore, **any revision of the legal framework should take place after the implementation of the Prüm rules is complete,** so that all participating countries can provide valuable input. In any case, considering the intergovernmental origins of Prüm, a revised legal framework will enable the **Parliament to fully participate** in the legislative process as co-legislator and scrutinise the proposed legislation.
- In relation to the possible reforms of the Prüm framework, as suggested by the feasibility study, it is evident that fundamental rights concerns, particularly with regard to the rights to respect for private life and protection of personal data and non-discrimination, are at the heart of the analysis. Therefore, before the adoption of legislative proposals, **Impact Assessments must be carried out** with the aim of evaluating the impact of different options to the fundamental rights of individuals. The feasibility study touches upon certain legal and data protection issues, but these are insufficient. Legislative action should not merely be driven by the possibilities offered by the evolution of technology; compliance with the fundamental rights enshrined in the Charter must be ensured. Central in that respect are the principles of necessity and proportionality. An Impact Assessment should provide as much information as possible on the practical effectiveness of the system and its use at the national level; as indicated in this study, the number of requests, the number of hits and the number of convictions are fundamentally different issues.
- In particular, the study highlighted that the next generation Prüm foresees an expanded personal and material scope of the rules to enable automated searches of data related to missing persons and unidentified deceased persons. Rectifying the fragmented legal framework stemming from different national rules is a welcome approach. However, **by processing data concerning missing persons, who may be vulnerable, within the same legal framework that enables searches of information on convicted criminals, additional safeguards are required** in relation to the retention of such data and the authorities' rights to launch searches, considering that different bodies may handle those cases in comparison to open criminal investigations. Finding missing persons and the identification of deceased persons are purposes which are not always linked with criminal law purposes. **Segregating the different types of data exchanges** concerning missing and deceased persons from those related to criminals should be considered as an option.
- The possibility of affording protection to the rights of **deceased persons**, as for example deceased persons do not fall within the scope of EU data protection law, should also be discussed.
- **Ensuring high data quality** should be a top priority due to the danger of false positive matches, particularly with the gradual development of national databases and the large volumes of data stored. Therefore implementing technical standards that will result in improving the quality of fingerprints is necessary. In order to improve the quality of DNA matches (hits) increasing the number of loci for a DNA match should be considered. However, allowing flexibility to Member

States to define an alternative threshold level to be used by establishing different matching requirements as part of bilateral agreements with other Member States needs careful assessment. This is because providing flexibility may render the rule non-applicable and thus ineffective. If a flexible approach is preferred, then the EU legislature could carve out specific criteria, for example maintaining the six or seven loci in relation to the most serious offences.[273]

- **It must be ensured that hits are followed-up** in accordance with Decision 2008/616/JHA, so as to ensure that these are weeded out rigorously and avoid wrongful incrimination.
- Though Chapter 4 of Decision 2008/616/JHA foresees the **production of statistical data, that information is not generally publicly available**.[274] As a result, the effectiveness, transparency and accountability of the Prüm framework are called into question.
- The imposition of **reporting duties** on usage is welcome; it should be considered whether reporting duties on accuracy could be embedded through a flexible approach.
- With respect to automated searches of vehicle data, it must be noted that any amendments must be informed by the principles of necessity, proportionality and data minimisation. Particularly, in relation to the creation of an **index, a series of considerations must be taken into account,** *inter alia*, the necessity of its establishment, the elements that should be included to identify a very limited number of vehicles, the retention period, the conditions for access by requesting officers to the index, the keeping of logs of using the index and the content to which access is provided.
- As for streamlining the follow-up procedure, **any automation in follow-up requests and retrievals of the minimum data set will significantly benefit law enforcement authorities, as at present cooperation is time-consuming and cumbersome. However, automation should be possibly reserved only in cases where the possibility of error remains marginal. Facilitation of MLA requests could also take place by imposing specific timeframes for replying to incoming requests.** Even in those cases, it is useful to allow discretion for Member States to maintain manual authorisation, perhaps within a specific limited timeframe, particularly in cases of concerns that the personal data in another Member State's fingerprint database may not be trustworthy. Furthermore, it will be useful in a forthcoming impact assessment to have information as to how often such searches take place, in order to determine in approximately how many cases time will be saved through the proposed new step. This will primarily be the case when a suspect or criminal is under investigation and known to the law enforcement authorities, but it will be important to have a clear view as to how often such automated retrievals could take place, and thus it will be a useful and effective amendment. Otherwise, it is feared that in the future the high threshold foreseen in this reform will be lowered to allow automated retrievals in other cases as well, without due regard to the principle of data quality and the prescriptions of Opinion 1/15.
- With the introduction of automated searches on facial images, certain Member States will be required to set up dedicated databases without domestic scrutiny. More information on the number of Member States and the overall current state of play is required in that respect. Importantly, a possible revision will have to take into account the **acute fundamental rights implications of searches by facial images**. Contemporary research demonstrates that such searches are likely difficult due to an adequate quality of such images. If this option goes forward, **the sources of facial images require clarity and data protection safeguards must be**

[273] Toom (n 35) 44.

[274] See Council, Document 14103/11 (18 November 2011).

embedded so that the quality of facial images is high enough to prevent the risk of increased false matches, which may lead to discriminatory practices. The specific purposes for searching facial images should also be circumscribed so as to **prevent wide-ranging surveillance practices at the national level**. **Separation of images on the basis of their sources and their quality** (mug-shots v probe images) should be considered as well.

- **The privacy and data protection implications of creating index databases containing an extract of police records should be assessed,** including their necessity and added value, particularly in view of the work of Europol and the possibilities offered by the Swedish Initiative. Of particular importance are a definition of what constitutes a police record; the amount of information included in the index; the retention period of a police record; the purposes for which it may be used; and the authorities that could access such an index.
- **Embedding interoperability solutions should not be decided before the introduction of interoperability in 2023 and assessing its effectiveness**. There are significant differences between centralised information systems and decentralised exchange mechanisms, such as Prüm framework and there are significant differences between the purposes of centralised information systems and the possibilities offered by Prüm. The necessity and proportionality of enabling interoperability of Prüm data with other data present in EU-wide databases should be assessed, as well as discrimination concerns. Possible overlaps should be avoided. It is also to be considered whether a central Prüm router is necessary if the bilateral connections among national databases are already in their final stages.
- The possibility of giving **Europol** a role in the Prüm system raises a series of issues such as the **protection of biometric data by Europol and the need for restrictions on onward transfers to third countries.**
- **The inclusion of Interpol as a Prüm actor** must ensure that no transfer of personal data to third countries takes place unless the Commission has adopted an adequacy decision ensuring the adequate level of personal data protection in that country.
- A revised Prüm framework should provide for **updated data protection rules** in line with the modernised EU data protection legal framework, particularly the Law Enforcement Directive.
- With the forthcoming end of the transitional period on 31 December 2020, after which the UK will become a third country, a new partnership agreement will possibly reconfigure the EU-UK relationship. **The UK's efforts to implement Prüm suggest that this avenue for information exchange among law enforcement authorities constitutes a priority**. However, the study provided a series of important issues that undermine trust to the UK and which have to be taken into account in the Commission's assessment of whether the UK offers an adequate - essentially equivalent - level of personal data protection. Close monitoring of the UK's compliance with the ECHR and possible significant deviations from the EU data protection regime is recommended. A partial adequacy decision or information exchanges via Interpol are also possible options in case the UK does not secure an adequacy decision.
- Finally, as for the **possibility of opening up Prüm to** third countries, particularly the **Western Balkans,** it must be emphasised that any automated searches of DNA analysis files, fingerprint data and VRD must take place in line with EU data protection law. Consequently, this option could be possible only if there is sufficient integration and link with the EU so that personal data is protected in an essentially equivalent way. The involvement of the EU in this process, however, is hereby emphasised.

4.2. Recommendations concerning the API Directive

- With respect to the API Directive, it is true that the passenger information landscape is convoluted in the aftermath of the adoption of the PNR Directive. The evaluation report confirms a series of discrepancies in the national legislations, including on the retention period, the categories of data forming part of API data and the application of the API Directive to internal flights. On the one hand, clarity and coherence between these two EU legal instruments, which are strongly linked, is necessary, **so that the treatment of API data when used in the law enforcement context is aligned with the prescriptions of the PNR system**. On the other hand, it must be emphasised that any revision of the API Directive should not be premature: it is recalled that PNR Directive is under scrutiny by the CJEU and judging from Opinion 1/15, it is possible that the PNR Directive will have to be revised. Furthermore, it must be stressed that despite the close link between the two instruments, their objectives are distinct and, therefore, due regard to these differences must be ensured.
- Neither a transplantation of the prescriptions of the PNR Directive to the API Directive, nor **expanding the material scope of the API Directive** to other means of transport are proportionate ways forward. Particularly the latter possibility may pre-empt the subsequent expansion of the PNR Directive to that direction. In addition, the correction of possible erroneous transposition of the PNR Directive must also be taken into account.
- As mentioned above, the **implementation of an iAPI** that will be introduced with the **EES** and the **ETIAS** is met with scepticism. Therefore, extending the **interoperability components** to the API Directive should be left for future determination, after the setting up of those information systems.

REFERENCES

- Amankwa, A.O. and McCartney, C. 'The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012' (2018) 284 *Forensic Science International* 117.
- Balzacq, T. and Hadfield, A., 'Differentiation and Trust: Prum and the Institutional Design of EU Internal Security' (2012) 47(4) *Cooperation and Conflict* 539.
- Balzacq, T. et al., 'Security and the Two-Level Game: The Treaty of Prum, the EU and the Management of Threats' (CEPS Working Document no 234, 2006).
- Balzacq et al., 'The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security' in Thierry Balzacq and Sergio Carrera (eds), *Security versus Freedom? A Challenge for Europe's Future* (Ashgate 2006).
- Bellanova, R.. 'The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?' in Elspeth Guild and Florian Geyer (eds), *Security Versus Justice? Police and Judicial Cooperation in the European Union* (Ashgate 2008) 212.
- Bowcott, O., 'UK's Facial Recognition Technology 'Breaches Privacy Rights' (*The Guardian*, 23 June 2020) https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights.
- Campbell, Z. and Jones, C., 'Leakeed Reports Show EU Police Are Planning a Pan-European Network of Facial Recognition Databases' (*The Intercept*, 21 February 2020) https://theintercept.com/2020/02/21/eu-facial-recognition-database/.
- Commission, 'The EU Security Union Strategy' (Communication) COM(2020) 605 final.
- _____, 'Study on the feasibility of improving information exchange under the Prüm Decisions (May 2020).
- _____, 'Study on Advance Passenger Information (API) - Evaluation of Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data' (February 2020).
- _____, 'October Infringements Package: Key Decisions' (13 October 2019) INF19/5950 https://ec.europa.eu/commission/presscorner/detail/EN/INF_19_5950.
- _____, 'A credible enlargement perspective for and enhanced EU engagement with the Western Balkans' COM(2018) 65final.
- _____, 'Ninth progress report towards an effective and genuine Security Union' COM(2017) 407 final.
- _____, 'Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union' (Communication) COM(2016) 230 final.
- _____, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205 final.
- _____, 'The European Agenda on Security' (Communication) COM(2015) 185 final.
- _____, 'The implementation of 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 (the "Prüm Decision")' (Report) COM(2012) 732 final.

- _____, 'Study on possible ways to enhance efficiency in the exchange of police records between the Member States by setting up a European police records index system' (October 2012).
- _____, 'Evaluation on the implementation and functioning of the obligation of carriers to communicate passenger data set up by Directive 2004/82' (17 September 2012).
- Council, Document 10119/20 (14 August 2020).
- _____, Document 5197/1/20 REV 1 (25 June 2020).
- _____, Document 8879/20 (19 June 2020).
- _____, Document 5197/20 (21 February 2020).
- _____, Document 14755/19 (2-3 December 2019).
- _____, Document 14744/19 (2 December 2019).
- _____, Document 13356/19 (30 October 2019, not publicly available).
- _____, Document 12511/19 (8 October 2019) not publicly available but retrieved in https://www.statewatch.org/media/documents/news/2019/nov/eu-council-uk-prum-fingerprints-report-12511-19.pdf.
- _____, Document 11434/19 (6 September 2019).
- _____, Document 10581/19 (27 June 2019).
- _____, Document 11227/18 (17 July 2018).
- _____, Document 9368/1/16 REV 1 (6 June 2016).
- _____, Document 9798/15 (15 June 2015).
- _____, Document 12750/13 (26 July 2013).
- _____, Document 17761/11 (5 December 2011).
- _____, Document 14103/11 (18 November 2011).
- _____, Document 13903/11 (8 September 2011).
- _____, Document 5842/2/10 (23 February 2010).
- _____, Document 5922/07 (15 February 2007).
- _____, Document 10900/05 (7 July 2005).
- Davis, D., 'Facial Recognition Technology Threatens to End All Individual Privacy' (*The Guardian*, 20 September 2019) https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy.
- De Hert, P., 'Division of Competences between National and European Levels with Regard to Justice and Home Affairs' in Malcom Anderson and Joanna Apap (eds), *Police and Justice Cooperation in the new European Borders* (Kluwer Law International 2002).
- European Council, The Hague Programme: strengthening freedom, security and justice in the European Union [2005] OJ C53/1.
- European Data Protection Board (EDPB), 'EDPB response to MEPs Sophie in't Veld and Moritz Körner n the US-UK agreement under the US Cloud Act' (15 June 2020).

- European Data Protection Supervisor (EDPS), 'Opinion 02/2020 – EDPS Opinion on the opening of negotiation for a new partnership with the UK' (February 2020).
- _____, 'Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM)2005) 490 final)' (2006).
- Genewatch, 'Parliamentary vote on the Prüm Decisions: Sharing DNA profiles and fingerprints across the EU requires further safeguards' (2015).
- Grother, P., Ngan, M. and Hanaoka, K., 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects' (National Institute of Standards and Technology, 2019).
- High-level expert group on information systems and interoperability (HLEG), 'Final report' (May 2017).
- House of Lords European Union Committee, 'Prüm: An Effective Weapon Against Terrorism and Crime?' (18th Report, session 2006-07, HL Paper 90).
- Jones, C., '"Complex, Technologically Fraught and Expensive" - The Problematic Implementation of the Prüm Decision' (Statewatch, 2012).
- Machado, H. and Granja, R., 'Ethics in Transnational Forensic DNA Data Exchange in the EU: Constructing Boundaries and Managing Controversies' (2018) 27(2) *Science as Culture* 242.
- McCartney, C., 'Forensic DNA Sampling and the England and Wales National DNA Database: A Sceptical Approach' (2004) 12 *Critical Criminology* 157.
- Mitsilegas, V., *EU Criminal Law after Lisbon*, Hart, London, 2016.
- _____, *EU Criminal Law*, Hart, London, 2009.
- _____, 'European Criminal Law after Brexit' (2017) 28 *Criminal Law Forum* 219.
- _____, 'What Are the Main Obstacles to Police Co-Operation in the EU?' (Briefing Paper for European Parliament LIBE Committee, IP/C/LIBE/FWC/2005-24, 2006). reproduced in Didier Bigo and Anastassia Tsoukala (eds), *Controlling Security* (Centre d'études sur les conflits/l'Harmattan 2008).
- Mitsilegas, V. and Vavoula, N., 'European Union Criminal Law' in Herwig Hofmann et al. (eds), *Specialized Administrative Law of the European Union - A Sectoral Treatment*, Oxford University Press, Oxford, 2018.
- Nielsen, N., 'MEPs Slam UK for Violating EU Police Database' (*EUobserver*, 10 January 2020) https://euobserver.com/justice/147084.
- _____, 'UK Taking 'Steps' after Illegal Copying of EU Schengen Data' (*EUobserver*, 25 July 2019) https://euobserver.com/justice/145530.
- _____, 'UK Unlawfully Copying Data from EU Police System' (*EUobserver*, 28 May 2018) https://euobserver.com/justice/141919.
- Parliament, 'European Parliament recommendation of 18 June 2020 on the negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland (2020/2023(INI))' (18 June 2020).
- _____, 'Report on the draft Council implementing decision on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom (14247/2019 – C9-0198/2019 – 2019/0819(CNS)) (8 May 2020)'.

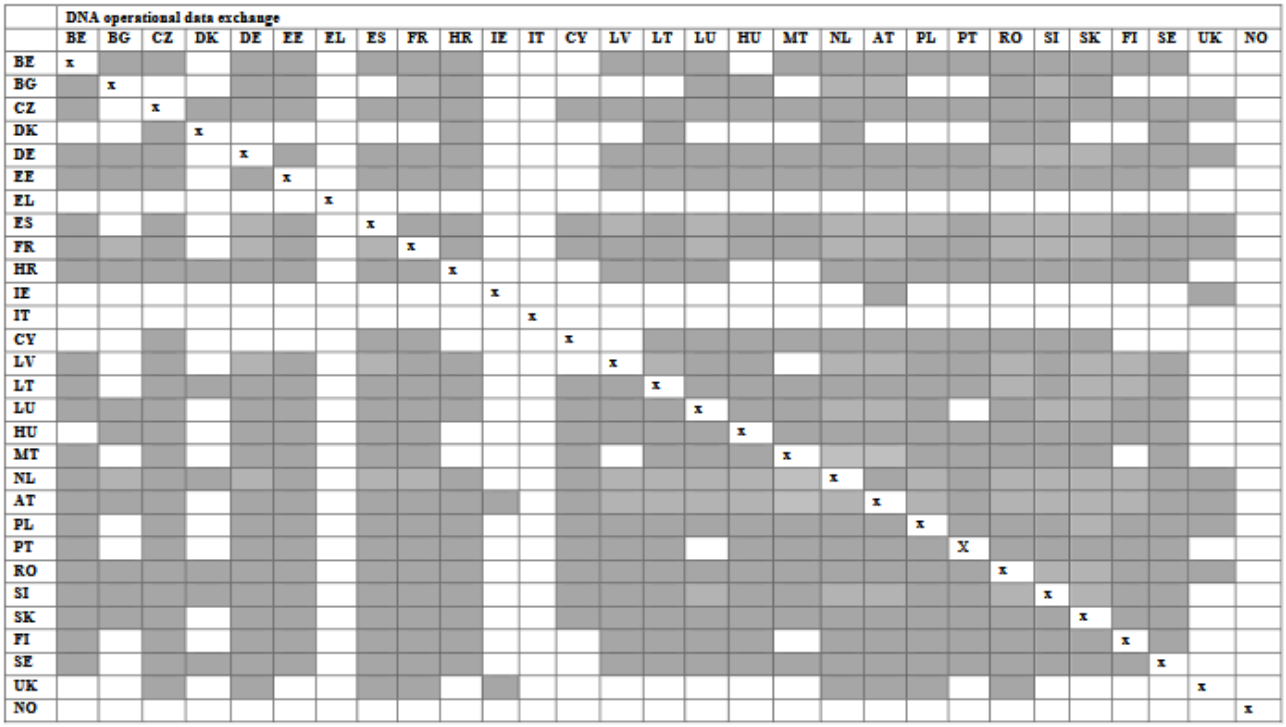
- _____, 'European Parliament legislative resolution of 13 May 2020 on the draft Council implementing decision on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom (14247/2019 – C9-0198/2019 – 2019/0819(CNS))' (13 May 2020).
- Police Cooperation Convention for Southeast Europe, 'Informal Negotiations to Amend the PCC Prüm Agreement' (27 May 2020) https://www.pccseesecretariat.si/index.php?page=news&item=7&id=997&type=arhiv.
- Prainsack, B and Toom, V., 'Performing the Union: The Prüm Decision and the European Dream' (2013) 44(1) *Studies in History and Philosophy of Biological and Biomedical Sciences* 71.
- _____, 'The Prüm Regime: Situated Dis/empowerment in Transnational DNA Profile Exchange' (2010) 50(6) *British Journal of Criminology* 1117.
- Rankin, J., 'UK Agrees to Share Suspects' DNA with EU Crime-Fighting System' (*The Guardian*, 15 June 2020) https://www.theguardian.com/politics/2020/jun/15/britain-agrees-share-suspects-dna-eu-crime-fighting-system.
- Santos, F., Machado, H. and Silva, S., 'Forensic DNA Databases in European Countries: Is Size Linked to Performance?' (2013) 9(1) *Life Science, Society and Policy* 12.
- Taverne, M. and Broeders T., *The Light's at the End of the Funnel! Evaluating the Effectiveness of the Transanational Exchange of DNA Profiles Between the Netherlands and Other Prüm Countries*, Paris Legal Publishers, Zutphen 2015.
- Toom, V., 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision' (Study for the LIBE Committee, PE 604.971, 2018).
- 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' (2019) 41 *Forensic Science International: Genetics* 50.
- UK Government, Department for Digital, Culture, Media and Sport and The Rt Hon Oliver Dowden CBE MP, 'Digital Secretary's closing speech to the UK Tech Cluster Group' (23 June 2020) https://www.gov.uk/government/speeches/digital-secretarys-closing-speech-to-the-uk-tech-cluster-group.
- UK Government, Department for Digital, Culture, Media and Sport, 'Explanatory framework for adequacy discussions' (13 March 2020) https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions.
- UK Government, 'The Future Relationship with the EU – The UK's Approach to Negotiations' (February 2020).
- UK Parliament, 'Prüm – Data Sharing Update: Written statement - HCWS290' (15 June 2020).
- _____, 'UK / EU relations: Written statement - HCWS86' (3 February 2020).
- Van der Beek, K., 'Forensic DNA Profiles Crossing Borders in Europe (Implementation of the Treaty of Prüm)' (2011) https://worldwide.promega.com/resources/profiles-in-dna/2011/forensic-dna-profiles-crossing-borders-in-europe/.
- Van der Beek, K., Kloosterman, A. and Sjerps, M., 'De Detectie van Vals Positieve en de Preventie van Vals Negatieve Matches bij Grootschalige DNA-Databankvergelijkingen' (2011) 6 *Expertise en Recht*,

- Vavoula, N., 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?' (2020) 26(1) *European Public Law* 131.
- Wieczorek, I., *The Legitimacy of EU Criminal Law* (Hart 2020).
- Williams, R and Johnson, P., *Genetic Policing: The Use of DNA in Criminal Investigations,* Willan Publishing, London, 2008.
- 'What the Schrems II Ruling Means for Brexit' (*After Brexit*, 16 July 2020) https://afterbrexit.tech/opinions/what-the-schrems-ii-ruling-means-for-brexit/.
- 'Europol: plans afoot to legalise unlawful acts' (*Statewatch*, 6 July 2020) https://www.statewatch.org/news/2020/july/europol-plans-afoot-to-legalise-unlawful-acts/.
- 'EDPB Casts Doubt over GDPR Adequacy Decision for the UK' (*Finextra*, 17 June 2020) https://www.finextra.com/newsarticle/36043/edpb-casts-doubt-over-gdpr-adequacy-decision-for-the-uk.
- 'UK and EU Law Enforcement Boost Co-Operation on DNA Databases' (*UK Government*, 13 June 2019) https://www.gov.uk/government/news/uk-and-eu-law-enforcement-boost-co-operation-on-dna-databases.

Case law:

- Case C-222/20 *Bundesrepublik Deutschland* (pending).
- Case C-623/17 *Privacy International* ECLI:EU:C:2020:5, Opinion of Advocate General Campos Sánchez-Bordona delivered on 15 January 2020.
- Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559.
- Opinion 1/15, ECLI:EU:C:2017:592.
- Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.
- Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* (C-698/15) ECLI:EU:C:2016:970.
- *Big Brother Watch v UK* (Appl. Nos 58170/13, 62322/14 and 24960/15).
- *S and Marper v UK* (2009) 48 EHRR 50.
- *Peck v UK* (2003) 36 EHRR 41.
- *Gaughran v UK* (Appl. No. 45245/15).

ANNEX I: DNA OPERATIONAL DATA EXCHANGE



	DNA operational data exchange																												
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						X							
RO																							x						
SI																								x					
SK																									x				
FI																		x								x			
SE																											x		
UK																												x	
NO																													x

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) 20.

ANNEX II: CATEGORIES OF NATIONAL DNA ANALYSIS FILES

National DNA analysis files to which Member States allow each other access for automated searching pursuant to 2008/615/JHA, Art 3(1)

MS	Notification of DNA files	Convicted	Suspects	Crime stains	Victims	Unidentified Persons	Unidentified Human Remains	Missing Persons	Relatives of Missing Persons	Others
BE	7655/12	X	X	X			X	X		
BG	6643/12	X	X	X			X			
CZ	13903/11	X	X	X		X	X	X		X
DK	9757/1/15	X	X	X			X	X		
DE	10271/11*	X	X	X						
EE	8745/12	X	X	X		X	X	X		
IE	9309/18	X	X	X						
EL	7115/14+11912/16		X	X						
ES	6946/10	X	X	X		X	X			X
FR	18714/11	X	X	X		X	X			
HR	5379/18	X	X	X		X		X		
IT	9722/1/19	X	X	X			X	X		
CY	16029/11	X		X		X	X			
LV	10849/11	X	X	X		X		X		
LT	13246/11	X	X	X		X				
LU	13449/10	X	X	X						
HU	11355/12	X	X	X			X			
MT	5728/13	X	X	X	X	X	X	X	X	
NL	6034/13	X	X	X		X	X	X		
AT	5864/10 ADD 1*	X	X	X		X	X	X		
PL	11184/12		X	X		X	X	X		
PT	9853/17	X		X						
RO	7043/12	X	X	X		X	X	X		
SI	8511/11*		X	X			X	X		
SK	14459/10	X	X	X	X	X	X	X		
FI	6753/12	X	X	X						
SE	5466/13	X	X	X						
UK	6188/17	X	X	X			X			
NO		X	X	X						

* = DNA analysis files not specified in notification

5197/1/20 REV 1 GB/mr 21
ANNEX 3 bis JAI.1 **LIMITE** **EN**

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) 21.

ANNEX III: FINGERPRINT OPERATIONAL DATA EXCHANGE

	FP operational data exchange																												
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	
NO																													

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) 27.

ANNEX IV: NATIONAL AFIS REPOSITORIES

National AFIS repositories to which Member States allow each other access for automated searching pursuant to 2008/615/JHA, Art. 9

MS	Convicted	Suspects	Victims	Crime scene	Unidentified Human Remains	Missing Persons	Relatives of Missing Persons	Others
BE	x	x		x				
BG	x	x		x				
CZ	x	x		x	x	x	x	x
DK	x	x		x	x			x
DE	x	x		x	x			
EE	x	x		x				x
IE	x	x		x				
EL								
ES	x	x		x				
FR	x	x		X	x	end of 2020		
HR	x	x		x	x			
IT								
CY	x	x		x	x	x		
LV	x	x		x	x			
LT	x	x		x	x			x
LU	x	x		x	x	x		
HU	x	x		x				
MT								
NL	x	x	crime related	x	crime related			
AT	x	x		open crimes	x	crime related		
PL		x		x				x
PT	x	only accused		open crimes	x	crime related		
RO	x			x	x	x		
SI		x		x				
SK	x	x		x				
FI	x			x				
SE	x	x		x				
UK	x	x						
NO	x	x	x	x	x	x	x	Foreigners

5197/1/20 REV 1 GB/mr 28
ANNEX 4 bis JAI.1 **LIMITE** **EN**

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) 28.

ANNEX V: VRD OPERATIONAL DATA EXCHANGE

	VRD operational data exchange																												
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	
NO																													x

Source: Council. Document 5197/1/20 REV 1 (24 June 2020) 36.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, aims to provide background information and policy recommendations concerning police information exchange and in particular the future developments regarding Prüm and the API Directive (Directive 2004/82/EC).

PE 658.542
IP/C/LIBE/IC/2020-095

Print ISBN 978-92-846-7118-2 | doi:10.2861/70848 | QA-02-20-701-EN-C
PDF ISBN 978-92-846-7119-9 | doi:10.2861/6059 | QA-02-20-701-EN-N