Council of the European Union

Brussels, 17 March 2022
(OR. en)

7288/22

LIMITE

IXIM 55
JAI 359
UK 49

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Implementation of the Trade and Cooperation Agreement (TCA) between EU and UK / Part Three, Title II, Article 54 • Report on the ex ante evaluation of automated DNA data exchange / Evaluation visit (London, 24-25 November 2021)

Delegations find in annex to this note the report on the outcome of the evaluation visit regarding automated DNA data exchange in accordance with the Trade and Cooperation Agreement between the EU and the UK.

The report was drafted by the evaluation team following the evaluation visit carried out in London from 24 to 25 November 2021.

The report is a basic element for a Council Decision to continue beyond 30 June 2022 DNA data exchange between the law enforcement authorities in accordance with the relevant provisions of the Agreement.

Delegations are invited to take note of the report and to proceed to the preparation of the Council Decision mentioned above.

1. Introduction

The legal framework of the Trade and Cooperation Agreement[1] (TCA) between the European Union and the United Kingdom provides that the Union, by way of a Council Decision, may decide that the UK has met the required conditions for automated data exchange, in particular DNA data exchange, between the competent law enforcement authorities of the UK and the Member States of the European Union and authorise the transfer of personal data to the UK under the TCA. This Decision can be taken by 30 June 2022 at the latest[2]. Until then, DNA data exchange can be continued in line with Council Implementing Decision (EU) 2019/968.[3]

Prior to the adoption of the Council Decision provided for by the TCA, an evaluation of the implementation of the legal and technical provisions for DNA data exchange by the UK is to take place, on the basis of which the Council should take the decision. The competent Council Working Party on JHA Information Exchange (IXIM) defined the details of that evaluation. The evaluation team presents the outcome of the evaluation in this report, which sets out both the information received and the on-site findings during the visit.

---

1 Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L 149, 30.4.2021, p. 10.

2 The current bilateral connections with the UK concerning the automated search and comparison of DNA profiles and dactyloscopic data have been established when the UK was still an EU Member State. The connections were established in accordance with Council Decisions 2008/615/JHA and 2008/616/JHA, which form the 'Prüm' *acquis*. Within the legal framework of the TCA, the Union is to determine under Article 540(2) of the TCA the date or dates from which personal data may be supplied by Member States to the UK. Prior to that decision, an evaluation whether the UK meets the required conditions has to be carried out. Pending the outcome of the evaluation, Article 540(3) of the TCA provides that Member States may supply DNA and dactyloscopic data to the UK until 30 September 2021. The evaluation procedure was not concluded by that date. By virtue of Article 540(3) of the TCA, the Specialised Committee on Law Enforcement and Judicial Cooperation extended, once by a maximum of nine months, i.e. until 30 June 2022, the period to continue with relevant personal data supply to the UK.

3 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, OJ L 156/8, 13.6.2019

The ex ante evaluation was carried out on the premises of the Metropolitan Police Service (MPS) in London on 24 and 25 November 2021. The evaluation team under the lead of experts from the Austrian Criminal Intelligence Service (BK) was composed of participants from Austria, Germany, France and the European Commission. Furthermore, a representative from the General Secretariat of the Council of the EU attended the evaluation as observer.

In order to verify whether the required conditions for DNA data exchange were met, the evaluation team came into direct contact with the representatives from the UK Home Office, the Scottish Government, the Northern Ireland Executive, the Police Service of Northern Ireland and from the Metropolitan Police Service London, who are applying the current daily DNA data exchanges with connected EU Member States.

UK representatives provided comprehensive information on all relevant points enabling a thorough analysis of the amendments to the Prüm DNA implementation since the first evaluation in January 2017 and the supplementary evaluation in July 2018, and the experiences with this cooperation since July 2019 regarding the operative Prüm DNA data exchange.

Representatives from the Home Office, the Scottish Government, the Northern Ireland Executive, the Metropolitan Police Service (MPS) and the National Crime Agency (NCA) and relevant law enforcement authority (LEA) representatives took great interest in the work and the on-site findings of the evaluation team. The team received all requested information.

In addition, the team took into account both the evaluation, which was carried out in the framework of the 'Prüm Decisions'[4] and led to the adoption of Council Implementing Decision (EU) 2019/968, and lessons learned on DNA data exchange between the UK and other Prüm operative EU Member States since that Decision entered into force. This TCA report also takes into account that since the recommendations given in the 2018 evaluation report and following Council Implementing Decision (EU) 2019/968, the UK reviewed its policy regarding suspects' profiles and notified the European Union that it had decided to include suspects' profiles in its automated biometric data exchanges within the shareable Prüm dataset[5].

Finally, the evaluation team provided the UK with a draft version of this report on 20 January 2021 for comments, which were received 2 March 2022 and taken into account in this final version.

2. Participants in the evaluation and locations visited

The list of the evaluation team members is set out in Annex I.

The evaluation visit took place at the following location: Metropolitan Police Service (MPS), Directorate of Forensic Services, 109 Lambeth Road, London, SE1 7LP, UK.

The UK provided the evaluation team and the observers a visitor program before the evaluation visit in line with the TCA, Annex 39, Chapter 4, Article 3(2)

3. Questionnaire

The UK notified the EU secretariat of the Specialised Committee on Law Enforcement and Judicial Cooperation on 26 July 2021 that the UK has implemented the obligations imposed under Title II of Part Three of the Trade and Cooperation Agreement (TCA) in respect of DNA and dactyloscopic data. The UK also wishes to apply Part Three of the TCA to all Member States that have given the notifications referred to in Article 36(2) of Council Decision 2008/615/JHA.

---

4 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, *OJ L 210, 6.8.2008, p. 1–11 and* 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, *OJ L 210, 6.8.2008, p. 12–72.*

5 Prüm – Data Sharing Update: Written statement - HCWS290 UK Home Office Report to UK Parliament and Letter from the UK Ambassador to the EU on automated data exchange with regard to DNA data in the United Kingdom (ST 8879/20 UK 13 IXIM 62).

The UK made further declarations and designations in accordance with Article 22 of Chapter 0 of Annex 39 of the TCA and indicated its readiness to be evaluated for the exchange of DNA data between the UK and EU Member States.

Subsequent to that notification, the competent Working Party on JHA information exchange (IXIM) set up the relevant questionnaire on automated DNA data exchange. The UK's reply to the questionnaire was submitted to the relevant Council working parties (Working Party on UK and IXIM) on 11 November 2021 (13660/21 IXIM 219 UK 239). The UK representatives explained in detail all information set out in the reply during the evaluation visit.

The reply to the questionnaire (13660/21) is attached to this report as ANNEX III.

4. Test run / Pilot run

The UK is exchanging DNA data on the basis of Council Implementing Decision (EU) 2019/968 of 6 June 2019. The Prüm DNA data exchange is deemed successful at technical and operative[6] level since 2019.

In order to set up that data exchange, pilot and test runs were carried out in the supplementary 2018 Prüm DNA data exchange evaluation of the UK and reported in the *"Report of the supplementary evaluation visit from 01-02 August 2018 in London"* to DAPIX (doc. 11545/18 JAI 827 DAPIX 257 CRIMORG 110 ENFOPOL 418 ENFOCUSTOM 172). The first live operation between the UK and an EU Member State was established with Austria in July 2019. Since then, the UK, in agreement with the EU Member States concerned, has gone live with 13 EU Member States.

As the UK database stores millions of DNA profiles, the beginning of mass comparisons in line with Article 4 of Council Decision 2008/615/JHA already created thousands of DNA matches, particularly in cooperation with Member States with similarly large national DNA databases. The UK allocated a sufficient amount of human resources to check and confirm these hits. The current UK cooperation in the DNA area with 13 EU Member States has already led to the effective investigation of thousands of criminal offences both in the UK and in the EU Member States, and is set out in more detail in the report hereunder.

[6] The operative status refers to the actual exchanges of data with connected EU Member States.

The following Member States currently exchange Prüm DNA data with the UK:

EU Member State	**Connected since**
Austria	08 July 2019
Germany	01 August 2019
Netherlands	17 September 2019
Spain	19 September 2019
France	03 October 2019
Romania	20 December 2019
Poland	30 December 2019
Czech Republic	14 February 2020
Ireland	19 March 2020
Latvia	28 August 2020
Sweden	23 October 2020
Belgium	24 December 2020
Malta	23 August 2021

Article 4 of Chapter 4 of Annex 39 to the TCA provides that the outcome of the 2018 evaluation should be taken into consideration in the context of the current ex ante evaluation. In agreement with IXIM, which decided on 9 November 2021 that no pilot run prior to the current evaluation and supplementary to the 2018 evaluation was required, a pilot run was not carried out.

5. Focal points

The following part of the report draws on the main aspects of the Prüm implementation by the UK Law Enforcement Authorities (LEA).

5.1 General Overview – UK system landscape and responsibilities – technical system architecture overview

The UK Home Office provides both the central Police National Computer (PNC) and the central national biometric databases linked to it, which operate in form of subsystems of the PNC for all national law enforcement authorities. Law enforcement data of England & Wales, Scotland and Northern Ireland are stored both on regional databases and, by means of duplication storage procedures, in the national PNC. They are linked from the PNC with unique numbers to the biometric data stored in the national AFIS IDENT1 and the national DNA database (NDNAD).

The UK Home Office is the data processor and owns and operates the UK biometric systems, such as the national central DNA database for LEA. The data owner and data controller are the national LEA. HOB ensures also via the Biometric Service Gateway (BSG) the data transfer between system users and partners. This includes also the MPS, which is the operator for international classical DNA cooperation and acts as the Prüm 1st step national contact point (NCP) for the current online Prüm DNA network with the EU Member States.

UK biometric systems are also used to distinguish between suspects and witnesses, and to exclude innocent people through matching latent marks found at crime scenes or elsewhere by linking such marks to known persons. NDNAD and IDENT1 are therefore closely coupled to the UK Criminal History System (PNC) that is the main criminal and arrest history database of identity information on offenders. PNC is from a technical point of view also the "IT master system" of the IDENT1 and NDNAD.

The Metropolitan Police Service (MPS) Forensic Service ensures the international exchange of dactyloscopic data and DNA data via the connection to the Prüm AFIS and Prüm DNA databases of the EU Member States. It is accountable to the Forensic Information Databases Strategy Board for ensuring the efficient and effective provision of the database infrastructure, information, and services.

5.2 Technical aspects related to United Kingdom and for international Prüm data exchange

5.2.1 TESTA ng Network

The Prüm communication works via the TESTA.ng network and in an encrypted way in operative cooperation with 13 EU Member States.

The main technical features related to the Prüm exchange are:

- The email server transmits the data through the TESTA.ng network in encrypted form;
- The Prüm features are only available at central level, located at the MPS in London;
- Demographic personal data are not transmitted in Prüm transactions;
- "Article 3"- searches of new DNA profiles will be controlled and launched on a daily basis by the Forensic Service MPS London in accordance with best practice recommendations.

DELETED

DELETED

DELETED

DELETED

DELETED

DELETED

5.2.4 NDNAD / IDENT1 and its relationship to the UK Criminal History System

To maintain the arrest history and the identity of offenders, NDNAD and the national AFIS IDENT1 are constructed as a subsystem to the UK Criminal History System on the PNC (Police National Computer). Each arrest event has a record on the UK PNC with a unique Arrest/Summons number entry. The linkage between NDNAD, IDENT1 and PNC ensures the proper retention of the whole criminal history data, including fingerprint data, as UK retention laws can be easily applied to fingerprints obtained for law enforcement purposes.

5.2.5 NDNAD / IDENT1 and its relation to the UK Forensic Information Database Services FINDS

The UK Forensic Information Database Services Organization (FINDS), under the responsibility of the UK Home Office, processes biometric data to provide forensic matches, which contributes to solving crime, including the facility to provide 24/7 support to the investigation of urgent crimes, most of which relate to serious offences. FINDS ensures that the records on NDNAD (and in other biometric systems) are accurate in order to support the criminal justice system and data protection principles. It investigates and corrects all data errors on NDNAD on behalf of the data owners.

It ensures that the database and its supporting policies are compatible with the current technology and developed to accommodate emerging technological advances and it contributes to wider business change within the forensic community by supporting the Home Office Biometrics Programme and the Transforming Forensics Programme and any other initiatives that require the skills and experience of the unit. Moreover, it supports the responsibilities defined within the Strategy Board governance rules.

5.3 Data retention

As an overarching principle applying across the entire United Kingdom, according to Section 39 of the Data Protection Act 2018, it is prohibited to keep personal data processed for any of the law enforcement purposes for longer than is necessary in relation to the purpose for which it is processed. The United Kingdom legal regime requires that appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes. Further rules on practices related to retention of personal data and the applicable time limits have been set out in the relevant legislation and guidance governing the powers and functioning of the police, and in localised rules in the devolved nations.

The UK Protection of Freedoms Act 2012 (PoFA) specifies the retention periods for fingerprints and DNA profiles stored in the PNC and biometric subsystems in England and Wales. DNA and fingerprint provisions are the same and are set out in the tables below. The Act strikes a balance between protecting the freedoms of those who are innocent of any offence whilst ensuring that the police continues to have the capability to protect the public and bring criminals to justice.

Separate legislation governs data retention in Northern Ireland and Scotland. The criminal history data and associated biometric data of Scotland and Northern Ireland are transferred from their national criminal history system (CHS and Niche respectively) databases to the PNC and the national biometric databases, too, and are thus fully available for Prüm cooperation with connected EU Member States.

There are only minor differences between the legal requirements for the collection of biometric data and the permissible storage period of biometric data in the respective legal systems in England and Wales, Northern Ireland and Scotland

In Scotland, biometric data collection and storage principles are regulated by the Criminal Procedure (Scotland) Act 1995. In Northern Ireland, biometric data collection and storage principles are regulated by the Police and Criminal Evidence (NI) Order 1989. The legislation provides for taking and sharing fingerprints and DNA profiles for the purpose for preventing and detecting crime.

As mentioned earlier, UK legislation does not define the term "suspect", but it is broadly understood to mean an individual arrested for, or charged with, but not yet convicted of a criminal offence. This allows for data acquisition and storage of fingerprints and DNA profiles. These data are also stored in the national UK PNC and IDENT1 AFIS and NDNA database as long as they do not need to be deleted. The data of arrested persons is also made available for both Scotland and Northern Ireland for the purpose of Prüm cross-checking since September 2020.

Deletion from the biometric databases is fully automated from PNC, in line with the PoFA and judicial case outcomes. FINDS runs an annual comparison exercise to ensure data integrity. The datasets shared by Northern Irish and Scottish authorities are checked regularly, before and after sharing with central UK processors. Data retention and deletion is governed by their respective legislation.

Approximately 98 per cent of individuals registered on Police National Computer (PNC) for which the UK holds biometric samples have a conviction.

Example of Retention rules for Convictions in England and Wales:

Situation	**Fingerprint and DNA Retention**
Any age convicted (including given a caution or youth caution) for a recordable qualifying offence	Indefinite
Adult convicted (including given a caution) for a recordable minor offence	Indefinite
Under 18 convicted (including given a youth caution) of a recordable minor offence	1st conviction: 5 years (plus length of any prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Data retention for Non-convictions:

Situation	**Fingerprint and DNA Retention**
Any age charged with but not convicted for a recordable qualifying offence	3 years plus a 2-year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for but not charged with a qualifying offence	3 years if granted by the Biometrics Commissioner plus a 2-year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for or charged with a minor offence	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Adult given a Penalty Notice for Disorder	2 years

5.4 Data protection and data responsibility

The Forensic Information Databases Strategy Board was given a legislative footing introduced in the PoFA 2012. It is responsible for the overall strategic management of the databases, including IDENT1. It takes strategic decisions to balance the freedoms of the individual whilst making the tool operationally effective. It has a parliamentary accountability through PoFA 2012 for NDNAD and IDENT1.

The Strategy Board comprises representatives of the National Police Chiefs Council, the Home Office, the Biometrics and Forensics Ethics Group, the Association of Police and Crime Commissioners, the Forensic Science Regulator (or representative), the Information Commissioner's Office, the Biometrics Commissioner (or representative), representatives from the police and devolved administrations of Scotland and Northern Ireland and such other members who may be invited.

The data by FINDS is owned by the Police (represented by the National Police Chiefs Council). The data held on IDENT1 is the property of the individual police forces – each Chief Constable is a data controller. The chair of the Strategy Board acts as joint data controller. The Home Office and each Forensic Service Provider (organizations granted permission by the Forensic Information Databases Strategy Board to provide forensic services to Law Enforcement Agencies) are data processors, whereby every organization has to have a data protection officer.

Prior to the United Kingdom's withdrawal from the EU, and during the transition period, the UK data protection legislation consisted of the relevant EU data protection legislation[7] and the UK Data Protection Act (DPA) 2018[8], enacted on 25th May 2018, which provided national rules, where allowed by Regulation (EU) 2016/679, specifying and restricting the application of the rules of Regulation (EU) 2016/679 and transposed Directive (EU) 2016/680.

To prepare for the exit from the EU, the Government of the United Kingdom enacted the European Union (Withdrawal) Act 2018[9], which incorporated directly applicable Union legislation into the law of the United Kingdom and provided that so-called "retained EU law" (which includes Regulation (EU) 2016/679 in its entirety; i.e. 'UK GDPR') and "EU-derived domestic legislation" (including Part 3 of the DPA 2018 transposing Directive (EU) 2016/680; i.e. 'UK LED'), continue to have effect after the end of the transition period.

---

7 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) (Text with EEA relevance) *OJ L 119, 4.5.2016, p. 1–88;* 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, *OJ L 119, 4.5.2016, p. 89–131*. also referred to as 'Law Enforcement Directive' or LED

8 Data Protection Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/12/contents

9 European Union Withdrawal Act 2018, available at the following link: https://www.legislation.gov.uk/ukpga/2018/16/contents

The UK GDPR and DPA 2018 together make up the UK 'data protection legislation':

- Part 2 covers General processing
- Part 3 covers Law Enforcement processing
- Part 4 covers Intelligence Services processing

Furthermore, the United Kingdom law enforcement agencies must ensure compliance with the Council of Europe's European Convention on Human Rights and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[10].

With regards data processing in the law enforcement sector, on 28 June 2021, the Commission adopted a Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom (Commission's UK adequacy decision under the Law Enforcement Directive)[11], noting that the UK ensures an adequate level of protection for personal data transferred from the European Union to the UK public authorities responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Commission continuously monitors the application of the legal framework upon which this Decision is based, with a view to assessing whether the United Kingdom continues to ensure an adequate level of protection of personal data.

On 10 September 2021, the UK Government launched a consultation outlining its proposals to reform the UK's data protection and privacy regime, following its departure from the European Union. The consultation ended on 19 November 2021.

10 The UK also signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108+) in 2018.

11 Commission Implementing Decision of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (C(2021) 4801 final) (Final act signed 28 June 2021).

The present report is based on current UK data protection legislation; not on the potentially envisaged reforms. At the moment of conclusion of this evaluation report, the UK Government's intentions in this regard are not clear yet[12]. During the visit the UK reiterated that it would seek to build on its current high data protection standards and practices. Any changes to this legislation resulting from the UK's reform exercise could lead to a reassessment of the Commission's adequacy Decision. In line with Article 3(4) of the Commission's UK adequacy decision under the Law Enforcement Directive, where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent United Kingdom authorities and may suspend, repeal or amend the decision. Pursuant to Article 693(2) of the TCA, serious and systemic deficiencies as regards the protection of personal data, including where those deficiencies have led to a relevant adequacy decision ceasing to apply, entitles the other Party to suspend Part Three or Titles thereof.

6. DNA examination accreditation and Forensic Policy

All forensic services within the MPS that fall within the Codes of Practice and Conduct of the Forensic Science Regulator are delivered through a single corporate Quality Management System that is accredited to the international standards ISO/IEC 17025:2017[13] and ISO/IEC 9001, subject to external third party accreditation and operated by the Directorate of Forensic Services.

The UK national legal framework is set out in the Accreditation of Forensic Service Providers Regulations 2018 and the UK Forensic Science Regulator Act 2021. That legislation implements international ISO/IEC 17025 quality standards and additional UK specific requirements, which are regulated in forensic details in the International Forensic Guidance (ILAC G19) and in UK Forensic Codes of Practice and Conduct with Appendices.

The Director of Forensic Services will on behalf of the Metropolitan Police Commissioner be the Senior Accountable Person for ensuring that the MPS meets the quality standards set by the Forensic Science Regulator and that all forensic staff who give evidence as an expert witness comply with their duty under the Criminal Procedure Rules.

---

12 The Commission has been informed that, in response to the consultation, the UK Government intends to publish a policy document and a draft bill when parliamentary time allows.

13 https://www.ukas.com/wp-content/uploads/schedule_uploads/00002/4309Testing-Multiple.pdf

The UK therefore fulfils all quality assurance requirements of Council Framework Decision 2009/905/JHA on Accreditation of forensic service providers carrying out laboratory activities.

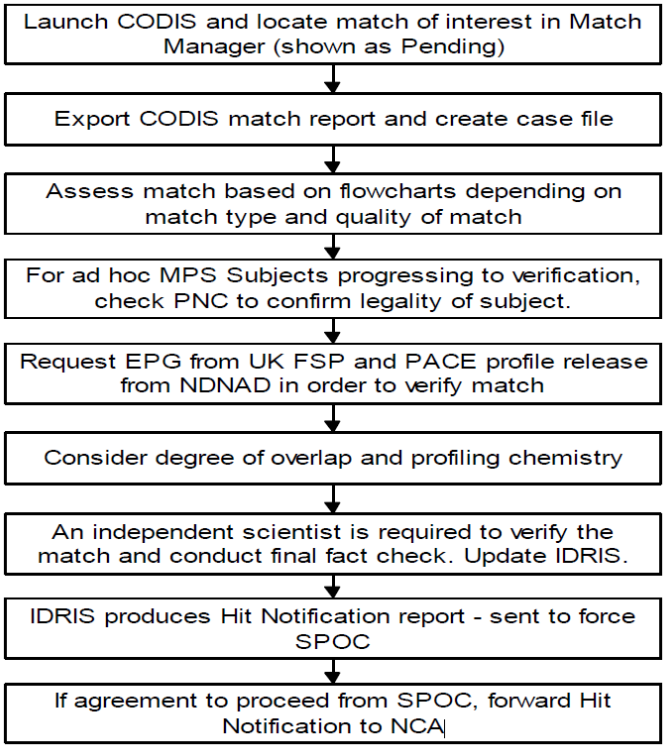

Figure 03: Overview MPS Scientific verification Prüm DNA hits

DELETED

DELETED

DELETED

DELETED

DELETED

8. Operative experiences made by UK and EU Member States in Prüm DNA data exchange

Based on the outcome of the ex ante evaluation, the implementation of the automated comparison of DNA-profiles and the related information flow can be considered as successfully concluded in the UK, both at legal and at technical level.

Since its launch with 13 EU Member States, the cooperation resulted in total in 13,169 Prüm hits regarding crimes under investigation in the UK and 44,892 regarding crimes under investigation in the EU Member States. Each month, about 1.500 Prüm hits lead to criminal investigations and clarification of crimes committed by internationally active criminals (active in minimum in two EU Member States).

Hereunder, see an overview provided from UK to Prüm DNA hits and an excerpt of November 2021 results before Prüm TCA evaluation with connected EU Member States.

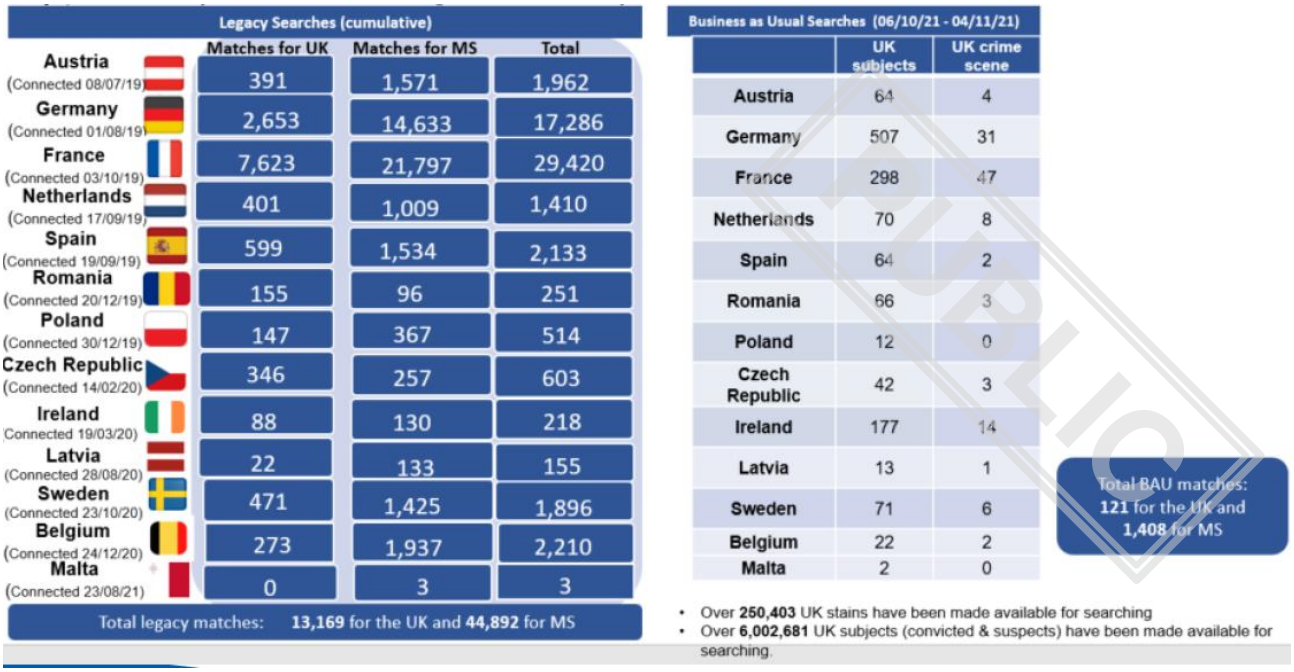

Figure 06: Overview Prüm 1 step hits UK – operative EU partner states with November 2021

Recommendations given to the UK authorities

The UK connected to a relatively high number of Prüm operational Member States. This is of great importance, especially in view of the size of the DNA database in the UK, which, as mentioned above, has led to thousands of hits from the moment the first connections were established.

The UK has implemented the requirements of Council Implementing Decision (EU) 2019/968 and completed by 15 June 2020 a review of its policy of excluding suspects' profiles from automated DNA data exchange. Following this review, the UK informed the European Commission on 15 June 2020 that it made the decision to include suspects' profiles in its automated biometric data exchanges with connected EU Member States.

Whilst therefore none of the points raised below impact on the positive outcome of the ex ante evaluation, they capture some broader observations made by the experts during the visit and forwarded for consideration to the UK. They have been included in this report not only for reason of completeness but also and more importantly for highlighting the potential for further increase in efficiency and reduction of workload.

9.1 Providing statistics on the automated data exchange

Pursuant to Article 24(2) of Annex 39 of the TCA, the UK shall compile statistics on the results of the automated data exchange and forward these annually to the Specialised Committee on Law Enforcement and Judicial Cooperation. The evaluation team therefore encourages the UK to support the compilation on statistics by providing all the necessary information.

9.2 Waiver of attachment of the Interpol form after Prüm less than 10 loci hit follow up correspondence

It is recommended that the UK waives the use of the Interpol DNA form by EU Member States when handling Prüm DNA follow-up communication after Prüm DNA hits with less than 10 loci in order to reduce unnecessary workload.

9.3: Waiver on systematic checks for hits of 6 loci with mismatch

It is recommended that the UK evaluates the seriousness of a crime before requesting an EU member state to perform a verification of a hit on 6 loci with mismatch.

10. Conclusions

Based on the outcome of the ex ante evaluation, the implementation of the automated DNA data application and the related automated DNA data information flow can be considered as successfully concluded in the UK, both at legal and at technical level.

The evaluation team proposes that the Working Party on Information Exchange and Information Management (IXIM) informs the Council that for the purposes of the automated exchange of DNA data, the UK has satisfactorily implemented the provisions pursuant to the TCA, Part Three, Title II and the respective Annex 39.

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 39)