Council of the European Union

Brussels, 17 March 2022
(OR. en)

7286/22

LIMITE

IXIM 54
JAI 358
UK 48

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 540 – Report on the ex ante evaluation of automated dactyloscopic data exchange / Evaluation visit (London, 24-25 November 2021)

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (26.06.2024)

Delegations find in annex to this note the report on the outcome of the evaluation visit regarding automated dactyloscopic 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 dactyloscopic 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.

ANNEX

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 dactyloscopic 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, dactyloscopic data exchange can be continued in line with Council Implementing Decision (EU) 2020/1188.[3]

---

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) 2020/1188 of 6 August 2020 on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom, OJ L 265, 12.8.2020, p. 1, and Corrigendum to 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, OJ L 266 I, 13.8.2020, p. 7.

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 dactyloscopic 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.

The evaluation was carried out on the premises of the Metropolitan Police Service (MPS) in London on Wednesday, 24/25 November 2021. The evaluation team under the lead of experts from the German Federal Criminal Police Office (BKA) was composed of participants from Germany, Austria, 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 dactyloscopic data exchange were met, the evaluation team came into direct contact with the representatives from both the UK Home Office and from the Metropolitan Police, who are applying the current daily fingerprint data exchanges.

In addition, the team considered both the evaluation, which was carried out in the framework of the 'Prüm Decisions'[4] and lead to the adoption of Council Implementing Decision (EU) 2020/1188, and lessons learned on dactyloscopic data exchange between the UK and Germany since that Decision entered into force.

Finally, the evaluation team provided the UK with a draft version of this report on 17 December 2021 for comments, which were received on 2 March 2022 and considered in this version.

[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*

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, 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.

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 dactyloscopic data between the UK and EU Member States.

Subsequent to that notification, the competent working party (IXIM) set up the relevant questionnaires on automated dactyloscopic data exchange. The UK's reply to the questionnaire (13784/21 IXIM 223 UK244) was submitted to the relevant Council working parties, i.e. the Working Party on UK and the Working Party on JHA Information Exchange (IXIM), on 11 November 2021. The UK representatives explained in detail all information set out in the reply during the evaluation visit.

4. Test run / Pilot run

Since 5 October 2020, the UK is exchanging dactyloscopic data with Germany based on Council Implementing Decision (EU) 2020/1188. The data exchange is deemed successful at technical level. In order to set up that data exchange, pilot and test runs were carried out prior to the evaluation visit of 10/11 September 2019 (12511/19 DAPIX 273 CRIMORG 131 ENFOPOL 347 ENFOCUSTOM 159 JAI 986).

Article 4 of Chapter 4 of Annex 39 to the TCA provides that the outcome of the 2019 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 2019 evaluation was required, a pilot run was not carried out.

Furthermore, it should be noted that regular tests are run between the UK and the DE test systems to secure the proper functioning of the automated data exchange in the event of updates or patches in each automated fingerprint information system (AFIS).

5. Focal points

The following part of the report draws on the main aspects of the Prüm implementation by the UK Law enforcement authorities. Chapters 6.1 to 6.5 give an overall view on the UK national Forensic Information Database Services (FINDS), data processing, retention and protection. Chapters 5.6 to 5.8 describe the Prüm implementation in detail on the basis of information required from the UK administration to support a detailed ex ante evaluation.

5.1 General Overview – UK system landscape and responsibilities

The UK Home Office provides both the national PNC and national biometric databases, which are linked to the PNC and operate in form of subsystems of the PNC, to all national law enforcement authorities (LEA). The LEA data of England & Wales, Scotland and Northern Ireland are stored in the national PNC and linked to the national AFIS IDENT1 and the NDNAD.

The UK Home Office Biometrics (HOB) is the data processor and owns and operates the UK biometric systems, relevant for the operation of international dactyloscopic exchange, such as the national central AFIS for LEA. The data owner and the data controller are the national LEA. HOB also ensures the data transfer between system users and partners such as the national fingerprint bureaux. This also includes the MPS, which is the operator for classic international dactyloscopic fingerprint cooperation and acts as the Prüm 1st step national contact point (NCP) for the current online Prüm fingerprint network with the EU Member States.

HOB also provides the service management and technical support for UK biometric systems and has established the Prüm data exchange system.

At present, there are two separate significant fingerprint systems (AFIS) in the Home Office sector. 'IDENT1' is the name given to the AFIS supporting the LEA, while the Immigration and Asylum Biometrics System (IABS) supports the immigration sector. IDENT1 is used for verification and law enforcement purposes. The system is used by trained practitioners to verify the identity of up to a million people each year taken into custody and arrested or detained. It is also used to identify suspects, witnesses and exclude innocent people through matching latent marks found at crime scenes or elsewhere by linking such marks to known persons.

A discrete dataset is held within IDENT1 for national security purposes. IDENT1 is closely coupled to the UK Criminal History System (Police national computer - PNC) that is the main criminal and arrest history database of identity information on suspects and offenders. PNC is the IT master system of the IDENT1 AFIS and other linked via interfaces to other national biometric databases such as e.g. the NDNAD. Fingerprints are taken in every case of arrest to identify the subject.

IDENT1 comprises the UK National tenprint collection, which consists of fingerprint images obtained from people who have been arrested for a recordable, i.e. punishable with imprisonment,[5] offence (suspected and convicted persons) within any UK jurisdiction and unidentified finger marks obtained from scenes of crime. Police Elimination fingerprints, fingerprints from Volunteers and Vulnerable persons, and fingerprints relating to Counter Terrorism purposes are also stored on IDENT1 and available for non-routine searches.

The Metropolitan Police Service (MPS) Forensic Services 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 (cf. 5.2.5 of this report) and for ensuring the efficient and effective provision of the database infrastructure, information, and services.

See below the national LEA data transfer and database operating structure overview:

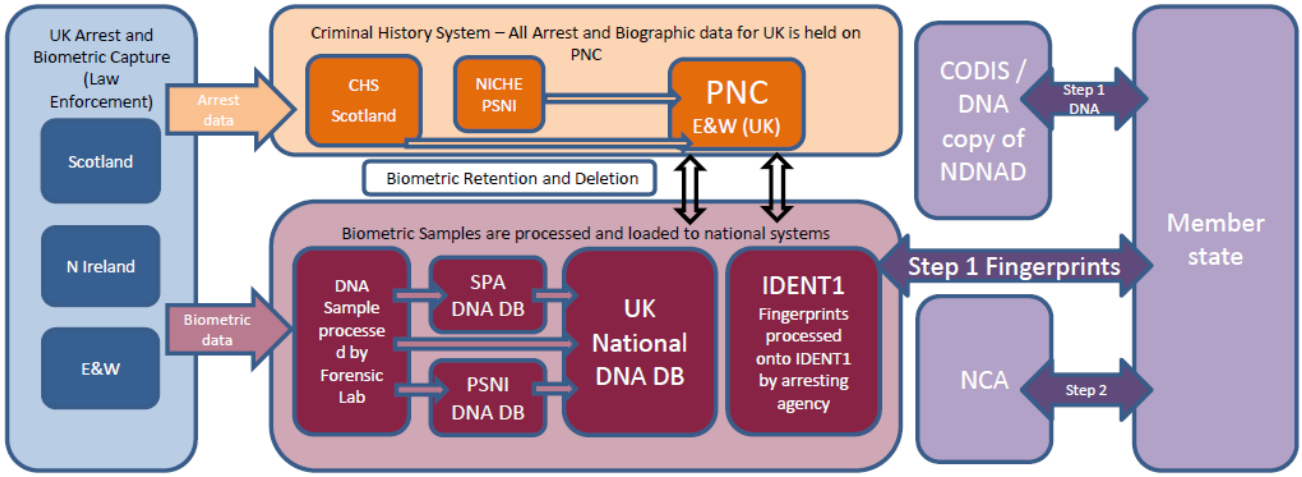

Figure 01: Overview UK Biometric Operating Model

[5] The purpose of the Police and Criminal Evidence Act (PACE) 1984, which incorporated the UK Protection of Freedoms Act 2012 (PoFA 2012), is to unify police powers under one code of practice and to balance carefully the rights of the individual against the powers of the police. PACE Code D concerns the main methods used by the police to identify people in connection with the investigation of offences and the keeping of accurate and reliable criminal records: Section 63 regulates the use of biometric samples for 'recordable' offences and section 118 PACE defines recordable offences as offences that are punishable with imprisonment. The concept of 'qualifying offence' distinguishes for the purposes of data retention between serious and less serious, i.e. minor offences. A list of qualifying offences is contained in section 65A(2) of PACE (as inserted by section 7 of the Crime and Security Act 2010 ("the 2010 Act")) and broadly covers serious violent, sexual and terrorist offences.

UK print sets from persons who are either suspected of having committed a criminal offence and the case is still pending, or who are convicted of a criminal offence are available for search (section 6.4) with the remaining UK data stock having separate governance and legislation.

To maintain public confidence in these services, the UK Home Office is responsible for continuously examining whether the system is run under the conditions set out in the respective UK legislation and is in line with UK governance. To ensure the integrity of data held in the systems, it has set up a data assurance strategy, which controls the access and the use of law enforcement fingerprint records. Under this strategy the Forensic Information Database Services ('FINDS', cf. chapter *5.2.2* of this document) is implemented. FINDS sets out the requirements for access and use of the national law enforcement fingerprint databases and services and maintains the data integrity between the systems.

5.2 Technical aspects related to the UK AFIS (IDENT1)

IDENT1 is physically run in two IT data centres and consists of more than 500 points of presence, among others 54 local bureau systems with 1,150 workstations attached.

Hosting and maintaining software applications and infrastructure falls into the responsibility of the Home Office (cf. chapter 6.2.3 of this document).

IDENT1 holds fingerprint data of 8 million convicted individuals and 200,000 fingerprint data of suspects, materializing in 27.9 million sets of ten prints and 13 million palm print pairs.
Furthermore, 1.7 million unresolved crime scene marks.

The following friction ridge data is stored and searchable on IDENT1 AFIS for the purposes of the automated data exchange:

- Tenprint rolled fingers
- Segmented plain (slap/flat) fingers
- Lower palm prints
- Writer's palm prints
- Latent finger marks
- Latent palm marks (lower palm or writers palm areas)

5.3 Organizational aspects

5.3.1 Service provider and stakeholders to IDENT1

The Home Office runs the immigration (IABS) and policing fingerprint databases (IDENT1). In doing so, its core objectives are to cut crime, prevent terrorism, control immigration and to support the UK's safeguarding agenda.

Concerning IDENT1, law enforcement agencies are responsible for

- loading print sets into the system obtained under UK legislation,
- searching latent marks recovered within their jurisdiction,
- loading unidentified latent marks into the national collection.

Law enforcement stakeholders to IDENT1 and their respective roles are:

Stakeholder	**Role**
Home Office Digital Data & Technology	IDENT1 Product management
UK Visas and Immigration	Cross reference law enforcement fingerprints for immigration decisions
Immigration Enforcement	
Crime and Policing Group	Develop policy for biometric retention
International Criminality Directorate	Develop policy for international law enforcement biometric exchange
Homeland Security Group	Biometric use for counter terrorism and national security
The Forensic Science Regulator	Setting standards for forensic processes
Home Office Science	Home Office oversight of the use of UK forensic databases
The Biometrics Commissioner	Independent oversight of the use and retention of biometric samples.
The Scottish Biometrics Commissioner	Independent oversight of the use and retention of biometric samples in Scotland

External stakeholders to IDENT1 are:

Stakeholder	**IDENT1 related Role**
National Crime Agency	Investigation and prevention of serious criminality across the UK, international exchange of biometric data.
National Police Chief's Council	Accountability for the IDENT1 law enforcement fingerprint data asset
Police & Crime Commissioners	Democratically elected Commissioner of a Police force ensuring police activity meets the needs of their electorate
The 43 Regional Police Forces of England & Wales	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
Police Service of Northern Ireland	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
The Northern Ireland Assembly	Setting legislation relating to the collection and retention of biometric samples collected for the investigation and prevention of crime in Northern Ireland
British Transport Police	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
HM Revenue and Customs	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
Police Scotland	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
Scottish Police Authority	Provide biometric services to Police Scotland and act as joint data controllers
The Scottish Government	Setting legislation relating to the collection and retention of biometric samples collected for the investigation and prevention of crime in Scotland

College of Policing	Setting the training standards and curriculum for Police Officers and Staff, specifically those involved in fingerprint processing and comparison
NPCC Criminal Records Office (ACRO)	UK central authority for international exchange of criminal records and provider of national criminal record management and subject access services

5.3.2 IDENT1 and its relationship to the UK Criminal History System

To maintain the arrest history and the identity of offenders, IDENT1 is constructed as a subsystem to the UK Criminal History System on the PNC (Police National Computer). Each arrest event is given a unique Arrest/Summons number entry (ASN) and recorded on the UK PNC. The linkage between 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.

5.3.3 IDENT1 and its relation to the UK Forensic Information Database Services

The UK Forensic Information Database Services organisation (FINDS), under the responsibility of the UK Home Office, operates and administers databases to provide forensic matches which contribute to solving crime. FINDS ensures that the records on IDENT1 (and in other systems) are accurate in order to support the criminal justice system in accordance with data protection principles. It investigates and corrects all data errors on IDENT1 on behalf of data owners.

It ensures that the database and its supporting policies are compatible with the current technology and developed to accommodate emerging technological advances. It contributes to wider business changes 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.

Figure 02: Overview FINDS responsibilities to IDENT1

5.4 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 retention periods for fingerprints and DNA profiles from England and Wales stored on the PNC and biometric subsystems are specified in the Protection of Freedoms Act 2012 (PoFA 2012). DNA and fingerprint provisions are the same and are given in the tables below. The Act strikes a balance between protecting the freedoms of those who are innocent whilst ensuring that the police continue 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 systems (CHS and Niche respectively) 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 regarding 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.

It should be noted that 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, and data held in certain circumstances following an acquittal verdict. This allows for data acquisition and storage of fingerprints and DNA profiles across the UK. These data are stored in the national UK PNC and IDENT1 AFIS and NDNA database as long as they do not need to be deleted. This arrest data 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 (UK national police information system) 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

5.5 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 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. 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. The overall process is shown in the diagram below.

Overall process, defining stakeholders, data ownership, authority, and lawful purpose*

	Collection (Unified Marks & Collection)	Analysis	Database Interactions	Investigation
Sample Source	• Arrestee / Detainee • Crime scenes	Not Applicable	• Crime stain records • Arrestee / Detainee	Not Applicable
Stakeholder / Actor	Law Enforcement Agency	Law Enforcement Agency Bureau	• Home Office • Metropolitan Police Service	Law Enforcement Agency
Data Ownership	Data Controller	Data Processor	Data Processor	Data Controller
Lawful Purpose	PACE	PACE (through contractual arrangements	• PACE • Statement of requirements	PACE
Jurisdictions	• England & Wales • Scotland • Northern Ireland	• England & Wales • Scotland • Northern Ireland	National	• England & Wales • Scotland • Northern Ireland

IDENT1
(Governance via FIND Strategy Board)

CRIME and SUBJECT INPUTS

Tenprint sets and unidentified marks from LEAs (and ACRO):
- England & Wales
- Scotland
- Northern Ireland

PNC link for demographics and deletions

Primary Purpose - Prevention and Detection of Crime

* Adapted for Prüm from Annexes in the "Forensic Information Databases Strategy Board Policy for Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data"

Figure 03: Overall UK Data Protection Processes

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[6] and the UK Data Protection Act (DPA) 2018[7], 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[8], 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.

The UK General Data Protection Regulation (UK GDPR) and UK Data Protection Act (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

---

6 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).

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

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

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)[9].

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, 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 legal framework and its application 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.

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[10]. 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.

---

9 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.

10 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.

5.6 1st step information exchange (AFIS-interconnection)

5.6.1 Technical Architecture

The UK technical solution for connecting to the Prüm network and for processing incoming and outgoing requests consists of four major systems, interconnected with IDENT1 AFIS.

a) UK Government E-Mail which is part of the UK governmental IT infrastructure, used for encrypted communication over TESTA NG with Prüm connected EU Member States.

b) The Prüm landing zone where messages from the Prüm connected EU Member States are received, signature validation, message decryption and anti-virus scanning is performed. Also, this gateway is responsible for transforming incoming requests from Prüm ICD complaint technical standard to the Home Office XML implementation of the NIST standard, HONE-1. IDENT1 receives HONE-1 and transforms it to its own internal IDENT1 standard.

c) The Biometric Services Gateway (BSG) where incoming messages are aggregated, queued and audited before processing through IDENT1 AFIS. For outgoing messages, message separation and transformation (to Binary) as well as message signing and encryption is performed by this part of the system. The data transformation is needed as, for example, some of the Prüm types of transactions (TOT) differ from the internal Home Office TOTs for processing in IDENT1. Nevertheless, all Prüm TOTs and the required areas of friction ridge detail, as defined in the Prüm ICD, are supported by the UK solution.

d) The Prüm Gatekeeper Service will authorize outgoing Prüm requests to ensure that the maximum allowable number for the target Member State is not breached (□ quota management).

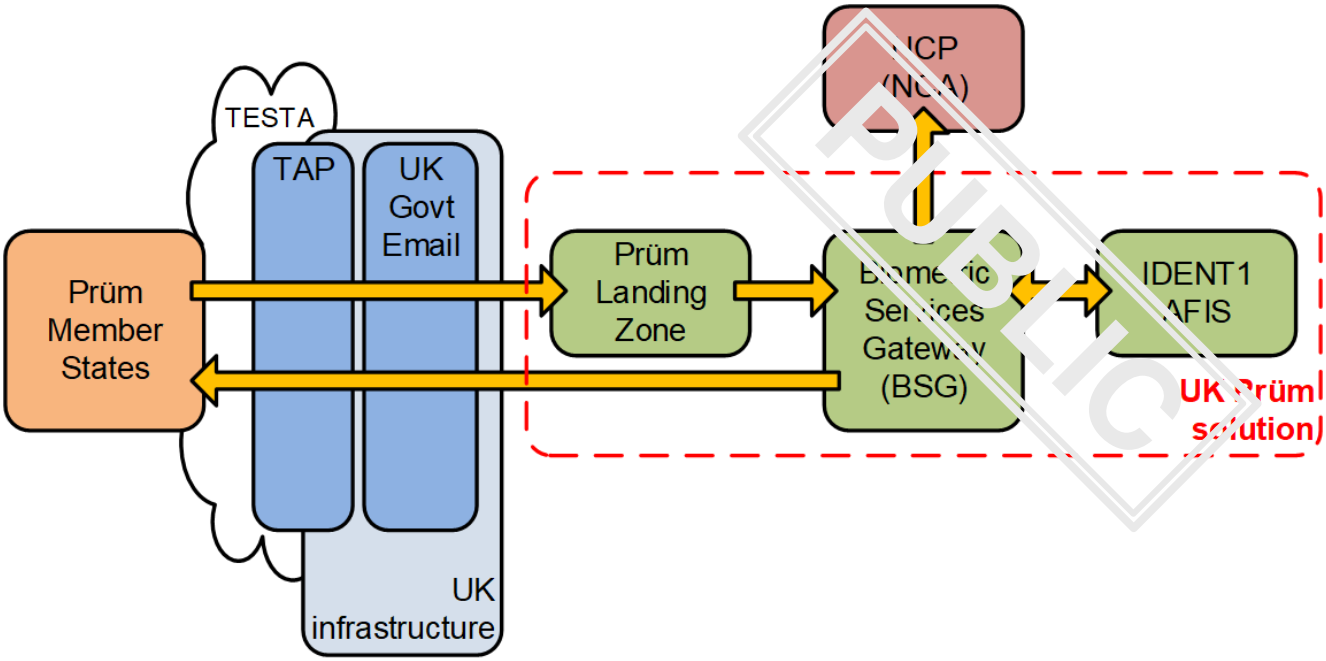

Figure 04: Overview UK Prüm technical solution

5.6.2 Prüm data processing and priority levels

The BSG and IDENT1 are designed to deal with volumes of transactions of many thousands per day pertaining to UK law enforcement processing, and deal with requests, in most cases, within a few minutes. Prüm transactions have been incorporated into this existing high-volume solution.

A high priority level can be set in an incoming Prüm request and the UK solution will accept this high priority request (as well as any priority code set in the Prüm NIST message). All Prüm requests will effectively be treated as high priority due to processing speeds that will be provided by the UK Home Office systems. Prüm requests will not be batched or placed in queues behind standard search requests to IDENT1 made from within the UK.

5.6.3 Auditing and logging

The UK Prüm implementation uses existing Audit functions in the BSG. The BSG is the primary audit store for Prüm messages and meets the Prüm logging requirements. All messages (in and out) are audited. Key identifiers are inserted into specific columns, to facilitate searching. Prüm entries are flagged to distinguish them from other audited messages.

All Base64 encoded images relating to original Prüm NIST records are hashed. A daily process runs to identify Prüm audit entries older than 24 months. At 24 months, the Type-2 is also hashed. The only audit remaining after 24 months is meta-data reflecting the fact that there was an exchange, but including no detail about that exchange.

The core AFIS has also been designed to meet Prüm requirements and ensure that business data in audited records are overwritten after 24 months.

5.6.4 Operational Security

The UK Home Office has adopted several processes to assure the Prüm Fingerprint service:

Physical security – Prüm services are hosted in secure locations in accordance with Police Assured Secure Facilities (PASF) requirements.

Personnel security – All support personnel hold national security vetting to Security Check (SC) and Non-Police Personnel Vetting Level 3 (NPPV3).

Independent IT health checks (ITHC) – All services are subject to independent ITHCs in accordance with The National Cyber Security Centre (NCSC) CHECK Scheme.

Monthly security reviews – A monthly operational security report is produced for discussion at a security working group (SWG) that focusses on any security incidents, vulnerabilities and status on remediation of technical debt (where applicable).

DELETED

5.7 Initiation of outgoing Prüm searches

The automated fingerprint data exchange is currently solely processed by the Metropolitan Police Service for all UK law enforcement authorities stakeholders. All outgoing search requests are authorized through the Prüm Gatekeeper function which consists of a dedicated application within the National Contact Point, which manages all UK searches and ensures quotas are not breached . Nevertheless, the UK plans to roll out the capabilities for the automated fingerprint searches to all national law enforcement authorities from 2022 onwards.

Incoming search results are processed by MPS as depicted in figure 05 and figure 06 below and in line with the Forensic Policy (cf. chapter 6.7.2 of this report).

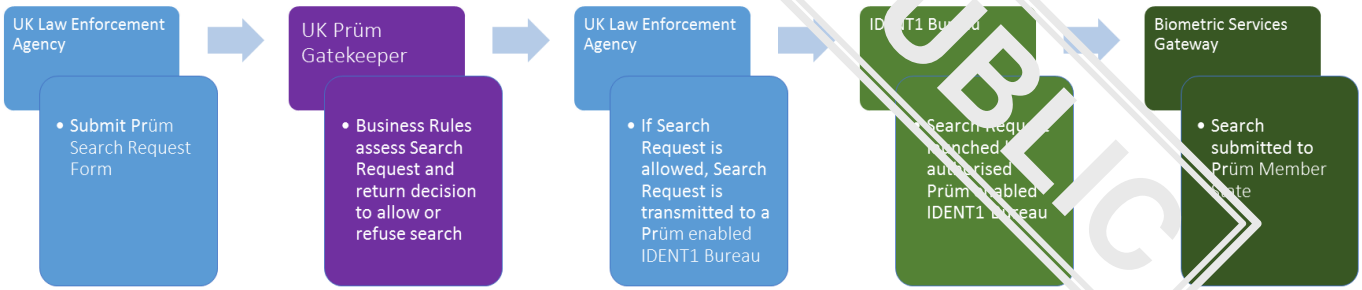

Figure 06: Flow chart – Prüm 1st step search initiation

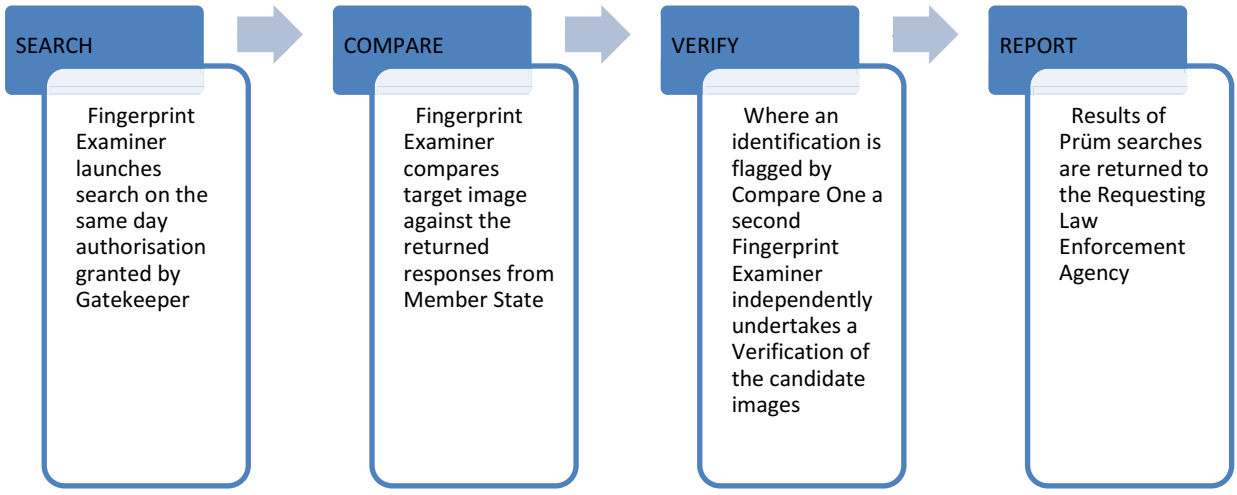

Figure 07: Flow chart – Prüm 1st step outgoing search verification

DELETED

6. Lessons learned

UK started the operational automated exchange of fingerprint data with DE on 5 October 2020. Since that point in time, the technical connection between both AFIS was operated with no unplanned downtimes or break downs. Some minor technical issues which all together occurred after updates and patches of each national AFIS were reported, analysed and patched immediately.

This shows especially the well-functioning of the above-mentioned service desk provided by UK to Prüm Member States.

In that context, it should also be highly noted that in the meantime UK took up the recommendation on providing data of "suspected" persons in the automated fingerprint exchange that was given during the first evaluation under the Prüm regime.

All Prüm transactions launched by DE so far were processed within minutes by IDENT1.

Since 5 October 2020, Germany sent 4.490 searches and in return retrieved 125 hits which lead to the respective numbers of person and latent identifications.

The future upkeeping of this important tool is therefore deemed to be a cornerstone in the field of practical law enforcement information exchange between the UK and DE.

DELETED

Conclusions

Based on the outcome of the ex ante evaluation, the implementation of the automated dactyloscopic data application and the related automated dactyloscopic 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 dactyloscopic 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 38)