14 August 2020

UKTF (2020) 18

Subject: 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

Origin: European Commission, Task Force for Relations with the United Kingdom

Remarks: This negotiating document was transmitted to the United Kingdom on 13 August 2020, following consultation with the European Parliament and Council. It was presented to the Council Working Party on the United Kingdom on Friday 17 July 2020.

Published on the UKTF website on Friday 14 August 2020

TITLE I: LAW ENFORCEMENT AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

Chapter one: General Provisions

Article LAW.GEN.1: Objective

1. The objective of this Title is to provide for law enforcement and judicial cooperation between, on the one hand, the Member States, Union institutions, bodies, offices and agencies and, on the other hand, the United Kingdom in relation to the prevention, investigation, detection and prosecution of criminal offences and to the prevention of and fight against money laundering and terrorist financing.

2. This Title shall only apply to law enforcement and judicial cooperation in criminal matters taking place exclusively between the Parties, and does not regulate situations arising within the Union, which remain defined by Union law.

Article LAW.GEN.2: Definitions

For the purposes of this Title, the following definitions apply:

(a) "State" means a Member State or the United Kingdom;

(b) "third State" means any State other than a State as defined in paragraph (a);

(c) "personal data" means any information relating to a data subject;

(d) "data subject" means an identified or identifiable natural person; an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(e) "special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

(f) "genetic data" means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(g) "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(h) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(i) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(j) "filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Article LAW.GEN.3: Protection of human rights and fundamental freedoms

Nothing in this Title shall have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in the European Convention on Human Rights, or, in case of the Union and its Member States, in the Charter of Fundamental Rights.

Article LAW.GEN.4: Protection of personal data

1. The provisions on the protection of personal data set out in this Title apply to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. Without prejudice to paragraph 3, any transfer of personal data to the United Kingdom under this Title, with the exception of any transfer of personal data under Chapter ten [AML], may only take place where the European Commission has decided in accordance with Article 36 of Directive (EU) 2016/680 that the United Kingdom or one or more relevant specified sectors within the United Kingdom ensures an adequate level of protection.

3. Transfers of Passenger Name Record under Chapter three [PNR] as well as any transfer of personal data under Chapter ten [AML] may only take place where the European Commission has decided in accordance with Article 45 of the General Data Protection Regulation (EU) 2016/679 that the United Kingdom or one or more relevant specified sectors within the United Kingdom ensures an adequate level of protection.

4. The United Kingdom shall ensure that the domestic independent authority responsible for data protection has the power to supervise compliance with and enforcement of the data protection safeguards under this Title. The United Kingdom shall by [XXXX] notify the Union of the supervisory authority or authorities responsible for overseeing the implementation of, and ensuring compliance with, this Title.

Chapter two: Exchanges of DNA, Fingerprints and vehicle registration data ("PRUM")

Article LAW.PRUM.5: Objective

The objective of this Chapter is to establish reciprocal cooperation between the competent law enforcement authorities of the United Kingdom, on the one hand, and the Member States, on the

other hand, on the automated transfer of DNA profiles, dactyloscopic data and certain domestic vehicle registration data.

Article LAW.PRUM.6: Definitions

For the purposes of this Chapter, the following definitions apply:

(a) “competent law enforcement authority” means a domestic police, customs or other authority that is authorised by domestic law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies, bodies or other units dealing especially with national security issues are not considered competent law enforcement authority for the purpose of this Chapter.

(b) “search” and ”comparison”, as referred to in Articles LAW.PRUM.8 [Automated searching of DNA profiles], LAW.PRUM.9 [Automated comparison of DNA profiles], LAW.PRUM.12 [Automated searching of dactyloscopic data], mean the procedures by which it is established whether there is a match between, respectively, DNA data or dactyloscopic data which have been communicated by one State and DNA data or dactyloscopic data stored in the databases of one, several, or all of the other States;

(c) “automated searching”, as referred to in Article LAW.PRUM.15 [Automated searching of vehicle registration data], means an online access procedure for consulting the databases of one, several, or all of the other States;

(d) “DNA profile” means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);

(e) “non-coding part of DNA” means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism;

(f) “DNA reference data” mean DNA profile and reference number;

(g) “reference DNA profile” means the DNA profile of an identified person;

(h) “unidentified DNA profile” means the DNA profile obtained from traces collected during the investigation of criminal offences and belonging to a person not yet identified;

(i) “note” means a State's marking on a DNA profile in its domestic database indicating that there has already been a match for that DNA profile on another State's search or comparison;

(j) “dactyloscopic data” mean fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database;

(k) “dactyloscopic reference data” mean dactyloscopic data and reference number;

(l) “vehicle registration data” mean the data-set as specified in Chapter 3 of the ANNEX LAW-1 to this Agreement;

(m) “individual case”, as referred to in Article LAW.PRUM.8(1) [Automated searching of DNA profiles], second sentence, Article LAW.PRUM.12 [Automated searching of dactyloscopic data], second sentence and Article LAW.PRUM.15(1) [Automated searching of vehicle registration data], means a single investigation or prosecution file. If such a file contains more than one DNA profile, or one piece of dactyloscopic data or vehicle registration data, they may be transmitted together as one request;

(n) “laboratory activity” means any measure taken in a laboratory when locating and recovering traces on items, as well as developing, analysing and interpreting forensic evidence regarding DNA profiles and dactyloscopic data, with a view to providing expert opinions or exchanging forensic evidence;

(o) “results of laboratory activities” means any analytical outputs and directly associated interpretation;

(p) “forensic service provider” means any organisation, public or private, that carries out forensic laboratory activities at the request of competent law enforcement or judicial authorities;

(q) “national accreditation body” means the sole body in a Member State that performs accreditation with authority derived from the State as referred to in Regulation (EC) No 765/2008.

Article LAW.PRUM.7: Establishment of domestic DNA analysis files

1. The States shall open and keep domestic DNA analysis files for the investigation of criminal offences.

2. For the purpose of implementing this Chapter, the States shall ensure the availability of DNA reference data from their domestic DNA analysis files as referred to in paragraph 1. DNA reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. DNA reference data shall not contain any data from which the data subject can be directly identified. DNA reference data relating to unidentified DNA profiles shall be recognisable as such.

3. The States shall declare the domestic DNA analysis files to which Article LAW.PRUM.7 [Establishment of domestic DNA analysis files] to Article LAW.PRUM.10 [Collection of cellular material and supply of DNA profiles] and 13 [national contact points], 14 [Supply of further personal data and other information] and 16 [Implementing measures] apply and the conditions for automated searching as referred to in Article LAW.PRUM.8(1) [Automated searching of DNA profiles].

Article LAW.PRUM.8: Automated searching of DNA profiles

1. For the investigation of criminal offences, States shall allow other States' national contact points as referred to in Article LAW.PRUM.13 [national contact points], access to the DNA reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting State's domestic law.

2. Should an automated search show that a DNA profile supplied matches DNA profiles entered in the requested State's searched file, the national contact point of the requesting State shall receive in an automated way the DNA reference data with which a match has been found. If no match can be found, automated notification of this shall be given.

Article LAW.PRUM.9: Automated comparison of DNA profiles

1. For the investigation of criminal offences, the States shall, in line with mutually accepted practical arrangements between the States concerned, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other domestic DNA analysis files' reference data. DNA profiles shall be supplied and compared in automated form. Unidentified DNA profiles shall be supplied for comparison only where provided for under the requesting State's domestic law.

2. Should a State, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied by another State match any of those in its DNA analysis files, it shall, without delay, supply that other State's national contact point with the DNA reference data with which a match has been found.

Article LAW.PRUM.10: Collection of cellular material and supply of DNA profiles

Where, in ongoing investigations or criminal proceedings, there is no DNA profile available for a particular individual present within a requested State's territory, the requested State shall provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained to the requesting State, if:

(a) the requesting State specifies the purpose for which this is required;

(b) the requesting State produces an investigation warrant or statement issued by the competent authority, as required under that State's domestic law, showing that the requirements for collecting and examining cellular material would be fulfilled if the individual concerned were present within the requesting State's territory; and

(c) under the requested State's law, the requirements for collecting and examining cellular material and for supplying the DNA profile obtained are fulfilled.

Article LAW.PRUM.11: Dactyloscopic data

For the purpose of implementing this Chapter, the States shall ensure the availability of dactyloscopic reference data from the file for the domestic automated fingerprint identification systems established for the prevention and investigation of criminal offences. Dactyloscopic reference data shall only include dactyloscopic data and a reference number. Dactyloscopic reference data shall not contain any data from which the data subject can be directly identified. Dactyloscopic reference data which is not attributed to any individual (unidentified dactyloscopic data) must be recognisable as such.

Article LAW.PRUM.12: Automated searching of dactyloscopic data

1. For the prevention and investigation of criminal offences, States shall allow other States' national contact points, as referred to in Article LAW.PRUM.13 [national contact points], access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Searches may be conducted only in individual cases and in compliance with the requesting State's domestic law.

2. The confirmation of a match of dactyloscopic data with reference data held by the requested State shall be carried out by the national contact point of the requesting State by means of the automated supply of the reference data required for a clear match.

Article LAW.PRUM.13: National contact points

1. For the purposes of the supply of data as referred to in Article LAW.PRUM.8 [Automated searching of DNA profiles], Article LAW.PRUM.9 [Automated comparison of DNA profiles] and Article LAW.PRUM.12 [Automated searching of dactyloscopic data], the States shall designate national contact points.

2. In respect of the Member States, national contact points designated for an according exchange of data within the Union shall be considered as national contact points for the purpose of this Chapter.

3. The powers of the national contact points shall be governed by the applicable domestic law.

Article LAW.PRUM.14: Supply of further personal data and other information

Should the procedure referred to in Article LAW.PRUM.8 [Automated searching of DNA profiles], Article LAW.PRUM.9 [Automated comparison of DNA profiles] and Article LAW.PRUM.12 [Automated searching of dactyloscopic data] show a match between DNA profiles or dactyloscopic data, the supply of further available personal data and other information relating to the reference data shall be governed by the domestic law, including the legal assistance rules, of the requested State.

Article LAW.PRUM.15: Automated searching of vehicle registration data

1. For the prevention and investigation of criminal offences and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the requesting State, as well as in maintaining public security, States shall allow other States' national contact points, as referred to in paragraph 2, access to the following domestic vehicle registration data, with the power to conduct automated searches in individual cases:

(a) data relating to owners or operators; and

(b) data relating to vehicles.

Searches may be conducted only with a full chassis number or a full registration number and in compliance with the requesting State's domestic law.

2. For the purposes of the supply of data as referred to in paragraph 1, the States shall designate a national contact point for incoming requests from other States. The powers of the national contact points shall be governed by the applicable domestic law.

Article LAW.PRUM.15a: Accreditation of forensic service providers carrying out laboratory activities

1. The United Kingdom shall ensure that their forensic service providers carrying out laboratory activities are accredited by a domestic accreditation body as complying with EN ISO/IEC 17025.

2. Each State shall ensure that the results of accredited forensic service providers carrying out laboratory activities in other States are recognised by its authorities responsible for the prevention, detection, and investigation of criminal offences as being equally reliable as the results of domestic forensic service providers carrying out laboratory activities accredited to EN ISO/IEC 17025.

3. The competent authorities of the United Kingdom shall not carry out searches and automated comparison according to Article LAW.PRUM.8 [Automated searching of DNA profiles], Article LAW.PRUM.9 [Automated comparison of DNA profiles] and LAW.PRUM.12 [Automated searching of dactyloscopic data] before the United Kingdom has transposed and applied the measures referred to in paragraph 1.

4. Paragraphs 1 and 2 do not affect domestic rules on the judicial assessment of evidence.

5. The United Kingdom shall communicate to the Specialised Committee on Law Enforcement and Judicial Cooperation the text of the main provisions adopted to implement and apply the provisions of this Article.

Article LAW.PRUM.16: Implementing measures

1. States shall make all categories of data available for searching and comparison to domestic competent authorities equally to the competent authorities of other States for the purposes covered in this Chapter.

2. For the purpose of implementing the procedures referred to in Article LAW.PRUM.8 [Automated searching of DNA profiles], Article LAW.PRUM.9 [Automated comparison of DNA profiles], Article LAW.PRUM.12 [Automated searching of dactyloscopic data] and Article LAW.PRUM.15 [Automated searching of vehicle registration data], technical and procedural specifications are laid down in the in ANNEX LAW-1.

3. The declarations made by Member States in accordance with Council Decisions 2008/615/JHA and 2008/616/JHA shall also apply in their relations with the United Kingdom.

Article LAW.PRUM.17: Ex ante evaluation

1. In order to verify whether the United Kingdom has fulfilled the conditions as set out in ANNEX LAW-1, an evaluation visit and a pilot run shall be carried out in respect of and under conditions and arrangements acceptable to the United Kingdom.

2. On the basis of an overall evaluation report and following the same steps as for the launching of automated data exchanges in Member States the Union shall determine the date or dates as from

which personal data may be supplied by Member States to the United Kingdom pursuant to this Chapter.

Chapter three: Transfer and processing of passenger name record data (PNR)

Article LAW.PNR.18: Scope

1. This Chapter lays down rules under which passenger name records (PNR) data may be transferred to, processed and used by the United Kingdom Competent Authorities for flights between the Union and the United Kingdom, and sets forth the specific safeguards in this regard.

2. This Chapter shall apply to air carriers operating passenger flights between the Union and the United Kingdom.

3. This Chapter shall also apply to carriers incorporating or storing data in the Union and operating passenger flights to or from the United Kingdom.

Article LAW.PNR.19: Definitions

For the purposes of this Chapter, the following definitions shall apply:

(a) "air carrier" means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air between the United Kingdom and the Union;

(b) "Passenger Name Record" ("PNR") means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities. Specifically, as used in this Chapter, PNR data consists of the elements set out in the ANNEX LAW-2;

(c) "The United Kingdom Competent Authority" means the United Kingdom authority responsible for receiving and processing PNR data under this Agreement;

Article LAW.PNR.20 Purposes of the use of PNR data

1. The United Kingdom shall ensure that PNR data received pursuant to this Chapter is processed strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime and to oversee the processing of PNR data within the terms set out in this Agreement.

2. For the purposes of this Chapter, a "terrorist offence" is an intentional act referred to in Articles 3 to 14 of EU Directive 2017/541/EU 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.

3. Serious crime means the offences listed in ANNEX LAW-3 that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under domestic law.

4. In exceptional cases, the United Kingdom Competent Authority may process PNR data where necessary to protect the vital interests of any individual, such as:

(a) a risk of death or serious injury; or

(b) a significant public health risk, in particular as required by internationally recognised standards.

5. The United Kingdom Competent Authority may also process PNR data on a case-by-case basis where the disclosure of relevant PNR data is compelled by a United Kingdom court or administrative tribunal in a proceeding directly related to a purpose under paragraph 1.

Article LAW.PNR.21: Ensuring PNR data is provided

1. The Union shall ensure that air carriers are not prevented from transferring PNR data to the United Kingdom Competent Authority pursuant to this Chapter.

2. The United Kingdom shall not require an air carrier to provide elements of PNR data which are not already collected or held by the air carrier for reservation purposes.

3. The United Kingdom shall delete upon receipt any data transferred to it by an air carrier, pursuant to this Chapter, if that data element is not listed in ANNEX LAW-2.

Article LAW.PNR.22: Police and judicial cooperation

1. The United Kingdom shall share with Europol, Eurojust, within the scope of their respective mandates, or the police or a judicial authority of a Member State, as soon as possible, all relevant and appropriate analytical information containing PNR data obtained under this Chapter.

2. The United Kingdom shall share, at the request of Europol, Eurojust, within the scope of their respective mandates, or the police or a judicial authority of a Member State, PNR data, the results of processing those data, or analytical information containing PNR data obtained under this Chapter, in specific cases to prevent, detect, investigate, or prosecute within the Union a terrorist offence or serious crime.

3. The United Kingdom shall ensure that this information is shared in accordance with agreements and arrangements on law enforcement or information sharing between the United Kingdom and Europol, Eurojust, or that Member State. In particular, exchange of information with Europol under this Article shall take place through the secure communication line for the purpose of exchange of information through Europol.

Article LAW.PNR.23: Non-Discrimination

The United Kingdom shall ensure that the safeguards applicable to the processing of PNR data apply to all passengers on an equal basis without distinctions that are not objectively justified.

Article LAW.PNR.24: Use of special categories of personal data

Any processing of special categories of personal data shall be prohibited under this Chapter. To the extent that the PNR data which is transferred to the United Kingdom Competent Authority includes

special categories of personal data, the United Kingdom Competent Authority shall delete such data immediately.

Article LAW.PNR.25: Data security and integrity

1. The United Kingdom shall implement regulatory, procedural or technical measures to protect PNR data against accidental, unlawful or unauthorized access, processing or loss.

2. The United Kingdom shall ensure compliance verification and the protection, security, confidentiality, and integrity of the data. The United Kingdom shall:

(a) apply encryption, authorization, and documentation procedures to the PNR data;

(b) limit access to PNR data to authorized officials;

(c) hold PNR data in a secure physical environment that is protected with access controls; and

(d) establish a mechanism that ensures that PNR data queries are conducted in a manner consistent with Article LAW.PNR.20 [Purposes of the use of PNR data].

3. If an individual's PNR data is accessed or disclosed without authorisation, the United Kingdom shall take measures to notify that individual, to mitigate the risk of harm, and to take remedial action.

4. The United Kingdom shall ensure that the United Kingdom Competent Authority promptly informs the Specialised Committee on Law Enforcement and Judicial Cooperation of any significant incidents of accidental, unlawful or unauthorised access, processing or loss of PNR data.

5. The United Kingdom shall ensure that any breach of data security, in particular leading to accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing will be subject to effective and dissuasive corrective measures which might include sanctions.

Article LAW.PNR.26: Transparency and notification to passengers

1. The United Kingdom shall ensure that the United Kingdom Competent Authority makes the following available on its website:

(a) a list of the legislation authorizing the collection of PNR data;

(b) the purpose(s) for the collection of PNR data;

(c) the manner of protecting the PNR data;

(d) the manner and extent to which the PNR data may be disclosed;

(e) information regarding the rights to access, correction, notation and redress; and

(f) contact information for inquiries.

2. The Parties shall work with interested parties, such as the aviation and air travel industry, to promote transparency, at the time of booking, on the purpose of the collection, processing and use of PNR data, and on how to request access, correction and redress. Air carriers shall provide passengers with clear and meaningful information in relation to the transfer of PNR data under this Chapter, including the recipient authority, the purpose of the transfer and the right to request from the recipient authority access to and rectification of the personal data of the passenger that has been transferred.

3. Where PNR data retained in accordance with Article LAW.PNR.28 [Retention of PNR data] has been used subject to the conditions set out in Article LAW.PNR.29 [Conditions for the use of PNR] or has been disclosed in accordance with Article LAW.PNR.31 [Disclosure within the United Kingdom] or Article LAW.PNR.32 [Disclosure outside the United Kingdom], the United Kingdom shall notify the passengers concerned in writing, individually and within a reasonable time once such notification is no longer liable to jeopardise the investigations by the government authorities concerned to the extent the relevant contact information of the passengers is available or can be retrieved taking into account reasonable efforts. The notification shall include information on how the individual concerned can seek administrative or judicial redress.

Article LAW.PNR.27: Automated processing of PNR data

1. The United Kingdom shall ensure that any automated processing of PNR data is based on non-discriminatory, specific and reliable pre-established models and criteria to enable the United Kingdom Competent Authority to:

(a) arrive at results targeting individuals who might be under a reasonable suspicion of involvement or participation in terrorist offences or serious crime as defined in paragraphs 2 and 3 of Article LAW.PNR.20 [Purposes of the use of PNR data]; or

(b) in exceptional circumstances, protect the vital interests of any individual as set out in paragraph 4 of Article LAW.PNR.20 [Purposes of the use of PNR data].

2. The United Kingdom shall ensure that the databases against which PNR data is compared are reliable, up to date and limited to those used by the United Kingdom in relation to the purposes of this Chapter set out in Article LAW.PNR.20 [Purposes of the use of PNR data].

3. The United Kingdom shall not take any decisions significantly adversely affecting a passenger solely on the basis of automated processing of PNR data.

Article LAW.PNR.28: Retention of PNR data

1. The United Kingdom shall not retain PNR data for more than five years from the date that it receives the PNR data.

2. Upon expiry of a period of six months after the transfer of the PNR data referred to in paragraph 1, all PNR data shall be depersonalised through masking out the following data elements which could serve to identify directly the passenger to whom the PNR data relate:

(a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;

(b) address, telephone number and electronic contact information of the passenger, the persons who made the flight reservation for the passenger, persons through whom an air passenger may be contacted and persons who are to be informed in the event of an emergency;

(c) all available payment/billing information to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate;

(d) frequent flyer information;

(e) other supplementary information (OSI), special service information (SSI) and special service request (SSR) information, to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

(f) any advance passenger information (API) data that have been collected.

3. Notwithstanding paragraph 1, the United Kingdom shall delete the PNR data of passengers after their departure from the country unless a risk assessment indicates the need to keep such PNR data. In order to establish this need, the United Kingdom shall identify objective evidence from which it may be inferred that certain passengers present the existence of a risk in terms of the fight against terrorism and serious crime.

4. For the purpose of paragraph 3, unless information is available on the exact date of departure, the date of departure should be considered as the last day of the period of maximum lawful stay in the United Kingdom of the passenger concerned.

5. The use of the data retained under this article is subject to the conditions laid down in Article LAW.PNR.29 [Conditions for the use of PNR].

6. An independent administrative body in the United Kingdom shall assess on a yearly basis the need to retain PNR data pursuant to paragraph 3.

7. Notwithstanding paragraphs 1, 2 and 3, the United Kingdom may retain PNR data, required for any specific action, review, investigation, enforcement action, judicial proceeding, prosecution, or enforcement of penalties, until concluded.

8. The United Kingdom shall destroy the PNR data at the end of the PNR data retention period.

Article LAW.PNR.29: Conditions for the use of PNR

The United Kingdom Competent Authority may use PNR data retained in accordance with Article LAW.PNR.28 [Retention of PNR data] for purposes other than security and border control checks, including any disclosure under Article LAW.PNR.31 [Disclosure within the United Kingdom] and Article LAW.PNR.32 [Disclosure outside the United Kingdom], only where new circumstances based on objective grounds indicate that the PNR data of one or more passengers might make an effective contribution to the attainment of the purposes of this Chapter as described in Article LAW.PNR.20 [Purposes of the use of PNR data]. Such use shall be subject to prior review by a court or by an independent administrative body in the United Kingdom based on a reasoned request by the United Kingdom Competent Authority within the domestic legal framework of procedures for the prevention, detection or prosecution of crime, except:

(a) in cases of validly established urgency; or,

(b) for the purpose of verifying the reliability and currency of the pre-established models and criteria on which the automated processing of PNR data is based, or of defining new models and criteria for such processing.

Article LAW.PNR.30: Logging and documenting of PNR data processing

The United Kingdom Competent Authority shall log and document all processing of PNR data. The United Kingdom shall only use a log or document to:

(a) self-monitor and to verify the lawfulness of data processing;

(b) ensure proper data integrity;

(c) ensure the security of data processing; and

(d) ensure oversight.

Article LAW.PNR.31: Disclosure within the United Kingdom

1. The United Kingdom Competent Authority shall not disclose PNR data to other government authorities in the United Kingdom unless the following conditions are met:

(a) the PNR data is disclosed to government authorities whose functions are directly related to the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data];

(b) the PNR data is disclosed only on a case-by-case basis;

(c) under the particular circumstances the disclosure is necessary for the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data];

(d) only the minimum amount of PNR data necessary is disclosed;

(e) the receiving government authority affords protection equivalent to the safeguards described in this Chapter; and

(f) the receiving government authority does not disclose the PNR data to another entity unless the disclosure is authorised by the United Kingdom Competent Authority respecting the conditions laid down in this paragraph.

2. When transferring analytical information containing PNR data obtained under this Chapter, the safeguards applying to PNR data in this Article shall be respected.

Article LAW.PNR.32: Disclosure outside the United Kingdom

1. The United Kingdom shall ensure that the United Kingdom Competent Authority does not disclose PNR data to government authorities in third States unless all the following conditions are met:

(a) the PNR data is disclosed to government authorities whose functions are directly related to the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data];

(b) the PNR data is disclosed only on a case-by-case basis;

(c) the PNR data is disclosed only if necessary for the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data];

(d) only the minimum PNR data necessary is disclosed;

(e) the third State to which the data is disclosed has either concluded an agreement with the Union that provides for the protection of personal data comparable to this Agreement or is subject to a decision of the European Commission pursuant to Union law, finding that the third State ensures an adequate level of data protection within the meaning of Union law.

2. If, in accordance with paragraph 1, the United Kingdom Competent Authority discloses PNR data collected under this Chapter originating in a Member State, the United Kingdom Competent Authority shall notify the authorities of that Member State of the disclosure at the earliest appropriate opportunity. The United Kingdom shall issue this notification in accordance with agreements and arrangements on law enforcement or information sharing between the United Kingdom and that Member State.

3. When transferring analytical information containing PNR data obtained under this Chapter, the safeguards applying to PNR data in this Article shall be respected.

Article LAW.PNR.33: Method of transfer

Air carriers shall transfer PNR data to the United Kingdom Competent Authority exclusively on the basis of the 'push method', a method whereby air carriers transfer PNR data into the database of the United Kingdom Competent Authority, and in accordance with the following procedures to be observed by air carriers, by which they:

(a) transfer PNR data by electronic means in compliance with the technical requirements of the United Kingdom Competent Authority or, in case of technical failure, by any other appropriate means ensuring an appropriate level of data security;

(b) transfer PNR data using a mutually accepted messaging format;

(c) transfer PNR data in a secure manner using common protocols required by the United Kingdom Competent Authority.

Article LAW.PNR.34: Frequency of transfer

1. The United Kingdom Competent Authority shall require air carriers to transfer the PNR data:

(a) on a scheduled basis, 24 to 48 hours before the scheduled flight departure time; and

(b) immediately after flight closure, that is, once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.

2. The United Kingdom Competent Authority shall permit air carriers to limit the transfer referred to in point (b) of paragraph 1 to updates of the transfers referred to in point (a) of that paragraph.

3. The United Kingdom Competent Authority shall inform air carriers of the specified times for the transfers.

4. In specific cases where there is an indication that additional access is necessary to respond to a specific threat related to the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data], the United Kingdom Competent Authority may require an air carrier to provide PNR data prior to, between or after the scheduled transfers. In exercising this discretion, the United Kingdom Competent Authority shall act judiciously and proportionately and use the method of transfer described in Article LAW.PNR.33 [Method of transfer].

Article LAW.PNR.35: Cooperation

The United Kingdom Competent Authority and the respective authorities of the Member States shall cooperate to pursue the coherence of their PNR data processing regimes in a manner that further enhances the security of citizens of the United Kingdom, the Union and elsewhere.

Article LAW.PNR.36: Non-derogation

This Chapter shall not be construed to derogate from any obligation between the United Kingdom and Member States or third States to make or respond to a request under a mutual assistance instrument.

Article LAW.PNR.37: Consultation and review

1. The Parties shall advise each other of any measure that is to be enacted and that may affect this Chapter.

2. When carrying out joint reviews of this Chapter as referred in Article LAW.OTHER.135 [Review and evaluation] (1)(b), the Parties shall pay particular attention to the necessity and proportionality of processing and retaining PNR data for each of the purposes set out in Article LAW.PNR.20 [Purposes of the use of PNR data]. The joint reviews shall also include the examination of how the United Kingdom Competent Authority has ensured that the pre-established models, criteria and databases referred to in Article LAW.PNR.27 [Automated processing of PNR data] are reliable, relevant and current, taking into account statistical data.

Chapter four: Cooperation on operational information

Article LAW.OPIN.38: Objective

1. The objective of this Chapter is to ensure that the competent law enforcement authorities of the United Kingdom on the one hand and of the Member States on the other hand may, pursuant to the provisions of this Chapter, exchange existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations in the context of the detection, prevention or investigation of criminal offences as listed in ANNEX LAW-4 to this Agreement according to the following provisions, to the extent that the transfer of this information and intelligence is not covered by other Chapters of this Agreement.

2. No data processed in databases established on the basis of Union law shall be provided to the United Kingdom in response to a request under this Chapter.

Article LAW.OPIN.39: Definitions

For the purpose of this Chapter, the following definitions apply:

(a) "competent law enforcement authority" means a domestic police, customs or other authority that is authorised by domestic law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies, bodies or other units dealing especially with national security issues are not considered competent law enforcement authority for the purpose of this Chapter.

In respect of the Member States, law enforcement authorities declared in accordance with Article 2(a) of Framework Decision 2006/960/JHA are considered as competent law enforcement authorities for the purpose of this Chapter. The Specialised Committee on Law Enforcement and Judicial Cooperation shall be notified of eventual modifications to the aforementioned declarations.

The United Kingdom shall by [XXXXX] notify the Specialised Committee on Law Enforcement and Judicial Cooperation of the authorities considered as competent law enforcement authority for the purpose of this Chapter.

(b) "criminal investigation": a procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts;

(c) "criminal intelligence operation": a procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by domestic law to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future;

(d) "information and/or intelligence":

(i) any type of information or data which is held by law enforcement authorities;

(ii) any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with Article LAW.OPIN.40(5) [Provision of information and intelligence].

Article LAW.OPIN.40: Provision of information and intelligence

1. States shall ensure that information and intelligence will be provided at the request of a competent law enforcement authority of another State pursuant to the provisions of this Chapter, acting in accordance with the powers conferred upon it by domestic law, conducting a criminal investigation or a criminal intelligence operation.

2. No conditions stricter than those applicable at domestic level for providing and requesting information and intelligence shall be applied by States for providing information and intelligence to competent law enforcement authorities pursuant to this Chapter. In particular, States shall not subject the exchange of information or intelligence which in an internal procedure may be accessed by the requested competent law enforcement authority without a judicial agreement or authorisation, to such an agreement or authorisation.

3. Where the information or intelligence sought may, under the domestic law applicable to the requested competent law enforcement authority, be accessed by the requested competent law enforcement authority only pursuant to an agreement or authorisation of a judicial authority, the requested competent law enforcement authority shall be obliged to ask the competent domestic judicial authority for an agreement or authorisation to access and exchange the information sought.

4. Where the information or intelligence sought has been obtained from another State or from a third State and is subject to the rule of speciality, its transmission to the competent law enforcement authority pursuant to this Chapter may only take place with the consent of the State or third State that provided the information or intelligence.

5. This Chapter does not impose any obligation on States to gather and store information and intelligence for the purpose of providing it to competent law enforcement authorities of another State, or to obtain any information or intelligence by means of coercive measures, defined in accordance with domestic law, in the State receiving the request for information or intelligence.

6. This Chapter does not impose any obligation on States to provide information and intelligence to be used as evidence before a judicial authority nor does it give any right to use such information or intelligence for that purpose. Where a State has obtained information or intelligence in accordance with this Chapter, and wishes to use it as evidence before a judicial authority, it shall obtain prior consent of the State that provided the information or intelligence through the use of Mutual Assistance as provided in Chapter eight.

7. States shall, where permitted by and in accordance with their domestic law, provide information or intelligence previously obtained by means of coercive measures.

Article LAW.OPIN.41: Requests for information and intelligence

1. Information and intelligence may be requested, and may subsequently only be processed, for the purposes set out in Article LAW.OPIN.38 [Objective].

A request for information and intelligence can be sent where there are factual reasons to believe that relevant information and intelligence is available to a competent law enforcement authority of the Member States or the United Kingdom. The request shall set out those factual reasons and explain the purpose for which the information and intelligence is sought and the connection between the purpose and the person who is the subject of the information and intelligence.

2. The requesting competent law enforcement authority shall not request more information or intelligence or setting narrower time frames than necessary for the purpose of the request.

3. Requests for information or intelligence shall contain at least the information set out in ANNEX LAW-4.

Article LAW.OPIN.42: Time limits for provision of information and intelligence

1. States shall have procedures in place so that they can respond within at most eight hours to urgent requests for information and intelligence regarding offences referred to in ANNEX LAW-4, when the requested information or intelligence is held in a domestic database directly accessible by a competent law enforcement authority.

2. If the requested competent law enforcement authority is unable to respond within eight hours, it shall provide reasons for that on the form set out in ANNEX LAW-4. Where the provision of the information or intelligence requested within the period of eight hours would put a disproportionate burden on the requested law enforcement authority, it may postpone the provision of the information or intelligence. In that case the requested law enforcement authority shall immediately inform the requesting law enforcement authority of this postponement and shall provide the requested information or intelligence as soon as possible, but not later than within three days.

3. Parties shall ensure that for non-urgent cases, requests for information and intelligence regarding offences referred to in ANNEX LAW-4 should be responded to within one week if the requested information or intelligence is held in a database directly accessible by a law enforcement authority. If the requested competent law enforcement authority is unable to respond within one week, it shall provide reasons for that on the form set out in ANNEX LAW-4.

4. In all other cases, Parties shall ensure that the information sought is communicated to the requesting competent law enforcement authority within 14 days. If the requested competent law enforcement authority is unable to respond within 14 days, it shall provide reasons for that on the form set out in ANNEX LAW-4.

Article LAW.OPIN.43: Spontaneous exchange of information and intelligence

1. Without prejudice to Article LAW.OPIN.44 [Reasons to withhold information or intelligence], the competent law enforcement authorities may, without any prior request being necessary, provide each other information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to ANNEX LAW-4. The modalities of such spontaneous exchange shall be regulated by the domestic law of State providing the information or intelligence.

2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question by the providing competent law enforcement authority.

Article LAW.OPIN.44: Reasons to withhold information or intelligence

1. [Without prejudice to Article LAW.OPIN.40 (2) [Provision of information and intelligence], a competent law enforcement authority may refuse to provide information or intelligence only if there are factual reasons to assume that the provision of the information or intelligence would:

(a) harm essential national security interests of the requested State;

(b) jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals;

(c) clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested; or

(d) result in the prosecution in a State of a person who has been finally judged by another State in respect of the same acts provided that, if a penalty has been imposed, has been enforced, is in the process of being enforced or can no longer be enforced under the law of the sentencing State.

2. Where the request pertains to an offence punishable by a term of imprisonment of a maximum of one year or less under the law of the requested competent law enforcement authority, that authority may refuse to provide the requested information or intelligence.

3. The competent law enforcement authority shall refuse to provide information or intelligence if the competent judicial authority has not authorised the access and exchange of the information or intelligence requested pursuant to Article LAW.OPIN.40 (3) [Provision of information and intelligence].

Article LAW.OPIN.45: Communication channels and language

1. Exchange of information and intelligence according to this Chapter may take place via the secure communication line for the purpose of exchange of information through Europol or any other any existing channels for international law enforcement cooperation. The language used for the request and the exchange of information of intelligence shall be the one applicable for the channel used.

2. When making the declarations or notifications in accordance with Article LAW.OPIN.39 [Definitions], Member States or the United Kingdom shall also provide details of the contacts to which requests may be sent in cases of urgency. These details may be modified at any time. The Specialised Committee on Law Enforcement and Judicial Cooperation shall communicate to the Member States, the United Kingdom and the European Commission the declarations received.

Chapter five: Cooperation with Europol

Article LAW.EUROPOL.46: Objective

The objective of this Chapter is to establish cooperative relations between Europol and the competent authorities of the United Kingdom in order to support and strengthen the action by the Member States and the United Kingdom as well as their mutual cooperation in preventing and combating serious crime, terrorism and forms of crime which affect a common interest covered by a Union policy.

Article LAW.EUROPOL.47: Definitions

For the purpose of this Chapter, the following definitions apply:

(a) “Europol” means the European Union Agency for Law Enforcement Cooperation, set up under Regulation (EU) 2016/794 (the “Europol Regulation”);

(b) "Competent authority" means, for the Union, Europol, and, for the United Kingdom a domestic law enforcement authority responsible under domestic law for preventing and combatting criminal offences;

The United Kingdom shall by [XXXXX] notify the Specialised Committee on Law Enforcement and Judicial Cooperation of the authorities considered as competent law enforcement authority for the purpose of this Chapter and provide a short description of their competences.

Article LAW.EUROPOL.48: Forms of crime

1. The cooperation as established under this Chapter shall relate to the forms of crime within Europol's competence, as listed in ANNEX LAW-5, including related criminal offences.

2. Related criminal offences shall be the criminal offences committed in order to procure the means of committing the forms of crime referred to in paragraph 1 of this Article, criminal offences committed in order to facilitate or carry out such acts, and criminal offences committed to ensure the impunity of such acts.

3. Where the list of forms of crime for which Europol is competent under Union law is changed, the Specialised Committee on Law enforcement and judicial cooperation may, from the date when the change to Europol's competence enters into force, upon a proposal from the Union, amend ANNEX LAW-5 accordingly.

Article LAW.EUROPOL.49: Scope of cooperation

The cooperation may, in addition to the exchange of personal data under the conditions laid down in this Chapter and in accordance with the tasks of Europol as outlined in the Europol Regulation, in particular include the exchange of information such as specialist knowledge, general situation reports, results of strategic analysis, information on criminal investigation procedures, information on crime prevention methods, the participation in training activities, the provision of advice and support in individual criminal investigations as well as operational cooperation.

Article LAW.EUROPOL.50: Domestic contact point and liaison officers

1. The United Kingdom shall designate a domestic contact point to act as the central point of contact between Europol and competent authorities of the United Kingdom and notify the Specialised Committee on Law Enforcement and Judicial Cooperation about this.

2. For the purpose of facilitating the cooperation as laid down in this Chapter, the United Kingdom shall second a liaison officer to Europol. Europol may second a liaison officer to the United Kingdom.

3. The United Kingdom shall ensure that its liaison officer has speedy and, where technically possible, direct access to the relevant domestic databases of the United Kingdom that necessary for them to fulfil their tasks.

4. The details of liaison officers' tasks referred to in paragraph 2, their rights and obligations and the costs involved, shall be governed by administrative arrangements concluded between

Europol and the competent authorities of the United Kingdom as referred to in Article LAW.EUROJUST.74 [Channels of transmission].

Article LAW.EUROPOL.51: Exchanges of information

1. Exchanges of information between the competent authorities shall comply with the objective and provisions of this Chapter. Personal data shall be processed only for the specific purposes referred to in paragraph 2.

2. The competent authorities shall clearly indicate, at the latest at the moment of transferring personal data, the specific purpose or purposes for which the personal data are being transferred. For transfers to Europol, the purpose or purposes of such transfer of personal data shall be specified in line with the specific purposes of processing set out in the Europol Regulation. If the competent authority of the United Kingdom has not done so, Europol, in agreement with that authority, shall process the information in order to determine the relevance of such information as well as the purpose or purposes for which it is to be further processed. Europol may process information for a purpose different from that for which information has been provided only if authorised so to do by the competent authority of the United Kingdom.

3. The competent authorities receiving the personal data shall give an undertaking stating that such data will be processed only for the purpose for which they were transferred. The personal data shall be deleted as soon as they are no longer necessary for the purpose for which they were transferred.

Article LAW.EUROPOL.52: Restrictions on access to and further use of transferred personal data

1. The transferring competent authority may indicate, at the moment of transferring personal data, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further processing of it. Where the need for such restrictions becomes apparent after the personal data have been transferred, the transferring competent authority shall inform the receiving competent authority accordingly.

2. The receiving competent authority shall comply with any restriction on access or further use of the personal data indicated by the transferring competent authority as described in paragraph 1.

3. Each Party shall ensure that personal data transferred under this Chapter have not been obtained in violation of internationally recognised human rights and are not used to request, hand down or execute a death penalty or any form of cruel or inhuman treatment.

Article LAW.EUROPOL.53: Different categories of data subjects

1. The transfer of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be prohibited unless such transfer is strictly necessary and proportionate in individual cases for preventing or combating a criminal offence.

2. The Parties shall ensure that the processing of personal data under paragraph 1 is subject to additional safeguards, including restrictions on access, additional security measures and limitations on onward transfers.

Article LAW.EUROPOL.54: Assessment of reliability of the source and accuracy of information

1. The competent authorities shall indicate as far as possible, at latest at the moment of transferring the information, the reliability of the source of the information on the basis of the following criteria:

(a) where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source which, in the past, has proved to be reliable in all instances;

(b) where the information is provided by a source from which information received has in most instances proved to be reliable;

(c) where the information is provided by a source from which information received has in most instances proved to be unreliable;

(d) where the reliability of the source cannot be assessed.

2. The competent authorities shall indicate as far as possible, at latest at the moment of transferring the information, the accuracy of the information on the basis of the following criteria:

(a) information the accuracy of which is not in doubt;

(b) information known personally to the source but not known personally to the official passing it on;

(c) information not known personally to the source but corroborated by other information already recorded;

(d) information which is not known personally to the source and cannot be corroborated.

3. Where the receiving competent authority, on the basis of information already in its possession, comes to the conclusion that the assessment of information or of its source supplied by the transferring competent authority in accordance with paragraphs 1 and 2 needs correction, it shall inform that competent authority and shall attempt to agree on an amendment to the assessment. The receiving competent authority shall not change the assessment of information received or of its source without such agreement.

4. If a competent authority receives information without an assessment, it shall attempt as far as possible and where possible in agreement with the transferring competent authority to assess the reliability of the source or the accuracy of the information on the basis of information already in its possession.

5. If no reliable assessment can be made the information shall be evaluated as at paragraph 1 (d) and paragraph 2(d) above.

Article LAW.EUROPOL.55: Secure Communication Line

1. The Parties agree to the establishment, implementation and operation of a secure communication line for the purpose of exchange of information between Europol and the competent authority of the United Kingdom.

2. Administrative arrangements between Europol and the competent authority of the United Kingdom as referred to in Article LAW.EUROPOL.57 [Exchange of sensitive non-classified and classified information] shall regulate the secure communication line's terms and conditions of use.

Article LAW.EUROPOL.56: Liability for unauthorised or incorrect personal data processing

1. The competent authorities shall be liable, in accordance with their respective legal frameworks, for any damage caused to an individual as a result of legal or factual errors in information exchanged. In order to avoid liability under their respective legal frameworks vis-à-vis an injured party, neither Europol nor the competent authorities of the United Kingdom may plead that the respective other competent authority had transferred inaccurate information.

2. If these legal or factual errors occurred as a result of information erroneously communicated or of failure on the part of either Europol or the competent authorities of the United Kingdom to comply with their obligations, they shall be bound to repay, on request, any amounts paid as compensation under paragraph 1 above, unless the information was used by Europol or the competent authorities of the United Kingdom in breach of this Chapter.

3. Europol and the competent authorities of the United Kingdom shall not require each other to pay for punitive or non-compensatory damages under paragraphs 1 and 2 above.

Article LAW.EUROPOL.57: Exchange of sensitive non-classified and classified information

The exchange of sensitive non-classified and classified information, if necessary under this Chapter, shall be regulated by an Administrative Arrangement on Confidentiality concluded between Europol and the competent authorities of the United Kingdom implementing the Protocol on the Security of Classified Information.

Article LAW.EUROPOL.58: Administrative arrangement

The details of cooperation between the Parties as appropriate to implement provisions of this Chapter shall be the subject of an administrative arrangement concluded between Europol and the competent authorities of the United Kingdom in accordance with Article 25(1) of Regulation (EU) 2016/794.

Article LAW.EUROPOL.59: Notification of implementation

1. The competent authorities shall make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data transferred under this Chapter including the means available for the exercise of the rights of data subjects. Each Party shall ensure that a copy of that document be provided to the other Party.

2. Where not already in place, the competent authorities shall adopt rules specifying how compliance with the provisions regarding the processing of personal data will be enforced in

practice. A copy of these rules shall be sent to the other Party and the respective supervisory authorities.

Article LAW.EUROPOL.60: Powers of Europol

Nothing in this Chapter shall be construed as creating an obligation on Europol to cooperate with the United Kingdom competent authorities beyond Europol's competence as set out in the relevant Union legislation.

Chapter six: Cooperation with Eurojust

Article LAW.EUROJUST.61: Objective

The objective of this Chapter is to establish cooperation between Eurojust and the competent authorities of the United Kingdom in combatting forms of serious crimes as defined in Article LAW.EUROJUST.63 [Forms of crime].

Article LAW.EUROJUST.62: Definitions

For the purpose of this Chapter, the following definitions apply:

(a) "Eurojust" means European Union Agency for Criminal Justice Cooperation (Eurojust), set up under Regulation (EU) 2018/1727 (the "Eurojust Regulation");

(b) "competent authority" means, for the Union, Eurojust, represented by the College or a National Member and, for the United Kingdom a domestic authority responsible under domestic law for investigating and prosecuting criminal offences.

The United Kingdom shall by [XXXXX] notify the Specialised Committee on Law enforcement and judicial cooperation of the authorities considered as competent authority for the purpose of this Chapter and provide a short description of their competences.

(c) "College" means the College of Eurojust, as referred to in the Eurojust Regulation;

(d) "National Member" means the National Member seconded to Eurojust by each Member State of the Union, as referred to in the Eurojust Regulation;

(e) "Deputy" means a person who shall be able to act on behalf of or substitute the National Member, as referred to in the Eurojust Regulation;

(f) "Assistant" means a person who may assist a National Member or the Liaison Prosecutor, as referred to in the Eurojust Regulation and in Article [xy] of this Agreement;

(g) "Liaison Prosecutor" means a public prosecutor seconded by the United Kingdom to Eurojust and subject to the domestic legislation of the United Kingdom as regards his or her status;

(h) "Liaison Magistrate" means a magistrate posted by Eurojust to the United Kingdom in accordance with the Eurojust Regulation;

(i) "Domestic Correspondent for Terrorism Matters" means one of the contact points designated by the United Kingdom authorities in accordance with Article LAW.EUROJUST.65 [Contact

point to Eurojust] of this Agreement, responsible for handling correspondence related to terrorism matters;

(j) "Judicial authorities" for the United Kingdom means [PLACEHOLDER];

(k) "Administrative Director" means the Administrative Director as referred to in the Eurojust Regulation;

(l) "Eurojust staff" means the staff referred to in the Eurojust Regulation.

Article LAW.EUROJUST.63: Forms of crime

1. The cooperation as established under this Chapter shall relate to all forms of serious crime within the competence of Eurojust, as listed in ANNEX LAW-6, including related criminal offences.

2. Related criminal offences shall be the criminal offences committed in order to procure the means of committing forms of crime referred to in paragraph 1 of this Article, criminal offences committed in order to facilitate or commit such acts, and criminal offences committed to ensure the impunity of such acts.

3. Where the list of forms of crime for which Eurojust is competent under Union law is changed, the Specialised Committee on Law enforcement and judicial cooperation may, from the date when the change to Eurojust's competence enters into force, upon a proposal from the Union, amend ANNEX LAW-6 accordingly.

Article LAW.EUROJUST.64: Scope of cooperation

The Parties shall ensure that Eurojust and the competent authorities of the United Kingdom cooperate in the fields of activity set forth in Articles 2 and 54 of the Eurojust Regulation and in this Chapter.

Article LAW.EUROJUST.65: Contact point to Eurojust

1. The United Kingdom shall put in place or appoint at least one contact point to Eurojust within the competent authorities of the United Kingdom.

2. The United Kingdom shall designate one of its contact points as the United Kingdom Domestic Correspondent for Terrorism Matters.

3. The United Kingdom shall communicate to the Specialised Committee on Law enforcement and judicial cooperation contact points referred to in paragraphs 1 and 2.

Article LAW.EUROJUST.66: Liaison Prosecutor

1. To facilitate cooperation as laid down in this Chapter, the United Kingdom competent authority shall second a Liaison Prosecutor to Eurojust.

2. The mandate and the duration of secondment shall be determined by the United Kingdom competent authority.

3. The Liaison Prosecutor may be assisted by two persons. When necessary, these persons may replace him or her.

4. The United Kingdom competent authority shall inform Eurojust of the nature and extent of the judicial powers of the Liaison Prosecutor within the United Kingdom own territory to accomplish his or her tasks in accordance with the purpose of this Chapter. The United Kingdom competent authority shall establish the competence of its Liaison Prosecutor to act in relation to foreign judicial authorities.

5. The Liaison Prosecutor shall have access to the information contained in the domestic criminal records or in any other register of the United Kingdom in the same way as stipulated by the United Kingdom legislation in the case of a prosecutor or person of equivalent competence.

6. The Liaison Prosecutor shall have the power to contact the competent authorities of the United Kingdom directly.

7. The details of the Liaison Prosecutor's tasks referred to in paragraph 2, their rights and obligations and the costs involved, shall be governed by working arrangements concluded between Eurojust and the competent authorities of the United Kingdom as referred to in Article LAW.EUROJUST.74 [channels of transmission].

8. The working documents of the Liaison Prosecutor shall be held inviolable by Eurojust.

Article LAW.EUROJUST.67: Liaison Magistrate

1. For the purpose of facilitating judicial cooperation with the United Kingdom in cases in which Eurojust provides assistance, Eurojust may post a Liaison Magistrate to the United Kingdom, in accordance with Article 53 of the Eurojust Regulation.

2. The details of liaison Magistrate' tasks referred to in paragraph 1, their rights and obligations and the costs involved, shall be governed by working arrangements concluded between Eurojust and the competent authorities of the United Kingdom as referred to in Article LAW.EUROJUST.62 [Definitions].

Article LAW.EUROJUST.68: Operational and strategic meetings

1. The Liaison Prosecutor, his or her assistant or assistants, and representatives of other competent authorities of the United Kingdom, including the contact point to Eurojust, may participate in operational and strategic meetings, at the invitation of the President of the College and with the approval of the National Members concerned.

2. National Members, their deputies and assistants, the Administrative Director and Eurojust staff may also attend meetings organised by the Liaison Prosecutor or other competent authorities of the United Kingdom, including the contact point to Eurojust.

Article LAW.EUROJUST.69: Exchange of information

Eurojust and the United Kingdom competent authorities may exchange any non- personal data in so far as relevant for the cooperation set out in Article LAW.EUROJUST.63, LAW.EUROJUST.65 and Article LAW.EUROJUST.66 and subject to any restrictions pursuant to Article LAW.EUROJUST.73.

Article LAW.EUROJUST.70: Exchange of personal data

1. Personal data requested and received by competent authorities under this Chapter shall be processed by them only for the objectives set out in Article LAW.EUROJUST.63 [Forms of crime], LAW.EUROJUST.65 [Contact point to Eurojust] and Article LAW.EUROJUST.66 [Liaison Prosecutor], the specific purposes referred to in paragraph 2 and subject to the restrictions on access or further use referred to in paragraph 3.

2. The transferring competent authority shall clearly indicate, at the latest at the moment of transferring personal data, the specific purpose or purposes for which the data are being transferred.

3. The transferring competent authority may indicate, at the moment of transferring personal data, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further processing of it. Where the need for such restrictions become apparent after the information has been provided, the transferring authority shall inform the receiving authority accordingly.

4. The receiving competent authority shall comply with any restriction on access or further use of the personal data indicated by the transferring competent authority as described in paragraph 3.

Article LAW.EUROJUST.71: Channels of transmission

Information shall be exchanged:

(a) either between the Liaison Prosecutor or, if no Liaison Prosecutor is appointed or otherwise available, the United Kingdom's contact point to Eurojust and the National Members concerned or the College; or

(b) if Eurojust has posted a Liaison Magistrate to the United Kingdom, between the Liaison Magistrate and any competent authority of the United Kingdom; or

(c) directly between a competent authority in the United Kingdom and the National Members concerned or the College. In this event, the Liaison Prosecutor or [if applicable] the Liaison Magistrate, shall be informed about any such information exchanges.

(d) The competent authorities may agree to use other channels for the exchange of information in particular cases.

(e) The competent authorities shall ensure that their respective representatives are authorised to exchange information at the appropriate level and in accordance with respectively United Kingdom legislation and the Eurojust Regulation, and are adequately screened.

Article LAW.EUROJUST.72: Liability for unauthorized or incorrect personal data processing

1. The competent authorities shall be liable, in accordance with their respective legal frameworks, for any damage caused to an individual as a result of legal or factual errors in information exchanged. In order to avoid liability under their respective legal frameworks vis-à-vis an injured party, neither Eurojust nor the competent authorities of the United Kingdom may plead that the respective other competent authority had transferred inaccurate information.

2. If these legal or factual errors occurred as a result of information erroneously communicated or of failure on the part of either Eurojust or the competent authorities of the United Kingdom to comply with their obligations, they shall be bound to repay, on request, any amounts paid as compensation under paragraph 1 above, unless the information was used by Eurojust or the competent authorities of the United Kingdom in breach of this Chapter.

3. Eurojust and the competent authorities of the United Kingdom shall not require each other to pay for punitive or non-compensatory damages under paragraphs 1 and 2 above.

Article LAW.EUROJUST.73: Exchange of sensitive non-classified and classified information

The exchange of sensitive non-classified and classified information, if necessary under this Chapter, shall be regulated by a Working Arrangement on Confidentiality concluded between Eurojust and the competent authorities of the United Kingdom implementing the Protocol No XX on the Security of Classified Information.

Article LAW.EUROJUST.74: Working arrangement

The modalities of cooperation between the Parties as appropriate to implement this Chapter shall be the subject of a working arrangement concluded between Eurojust and the competent authorities of the United Kingdom in accordance with Article 47(3) and 56(3) of Regulation (EU) 2018/1727.

Article LAW.EUROJUST.75: Powers of Eurojust

Nothing in this Chapter shall be construed as creating an obligation on Eurojust to cooperate with the competent authorities of the United Kingdom beyond Eurojust's competence as set out in the relevant Union legislation.

Chapter seven: Surrender

Article LAW.SURR.76: Objective

The objective of this Chapter is to ensure that the extradition system between, on the one hand, the Member States and, on the other hand, the United Kingdom shall be based on a mechanism of surrender pursuant to an arrest warrant in accordance with the terms of this Chapter.

Article LAW.SURR.77: Definitions

For the purpose of this Chapter, the following definitions apply:

(a) "arrest warrant" means a judicial decision issued either by a Member State with a view to the arrest and surrender by the United Kingdom of a requested person, or by the United Kingdom with a view to the arrest and surrender by a Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order.

(b) "judicial authority" means a judge, a court or a public prosecutor.

Article LAW.SURR.78: Scope

1. An arrest warrant may be issued for acts punishable by the law of the issuing State by a custodial sentence or a detention order for a maximum period of at least 12 months or, where a sentence has been passed or a detention order has been made, for sentences of at least four months.

2. Without prejudice to paragraphs 3 and 4, surrender shall be subject to the condition that the acts for which the arrest warrant has been issued constitute an offence under the law of the executing State, whatever the constituent elements or however it is described.

3. Subject to Article LAW.SURR.79 [Grounds for mandatory non-execution of the arrest warrant], Article LAW.SURR.80 [Other grounds for non-execution of the arrest warrant] (1)(b) to (h), Article LAW.SURR.81 [Political offence exception], Article LAW.SURR.82 [Nationality exception] and Article LAW.SURR.83 [Guarantees to be given by the issuing State in particular cases], in no case shall a State refuse to execute an arrest warrant issued in relation to the behaviour of any person who contributes to the commission by a group of persons acting with a common purpose of one or more offences in the field of terrorism referred to in Articles 1 and 2 of the European Convention on the Suppression of Terrorism or in Articles 3 to 14 of the EU Directive of 15 March 2017 on combating terrorism, or in relation to illicit trafficking in narcotic drugs and psychotropic substances, or murder, grievous bodily injury, kidnapping, illegal restraint, hostage-taking and rape, punishable by deprivation of liberty or a detention order of a maximum of at least 12 months, even where that person does not take part in the actual execution of the offence or offences concerned; such contribution shall be intentional and made with the further knowledge that his or her participation will contribute to the achievement of the organisation's criminal activities.

4. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand may make a declaration to the effect that, on the basis of reciprocity, the condition of double criminality referred to in paragraph 2 shall not be applied under the conditions set out hereafter. The following offences, if they are punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing State, shall, under the terms of this Agreement and without verification of the double criminality of the act, give rise to surrender pursuant to an arrest warrant:

- participation in a criminal organisation,
- terrorism,
- trafficking in human beings,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- fraud, including that affecting the financial interests of the Union,

- laundering proceeds of crime,
- counterfeiting currency, including of the euro,
- computer-related crime,
- environmental crime, including illicit trafficking in endangered animal species and varieties,
- facilitation of unauthorized entry and residence,
- murder,
- grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage-taking,
- racism and xenophobia,
- organised or armed robbery,
- illicit trafficking in cultural goods, including antiques and works of art,
- swindling,
- racketeering and extortion,
- counterfeiting and piracy of products,
- forgery of administrative documents and trafficking therein,
- forgery of means of payment,
- illicit trafficking in hormonal substances and other growth promoters,
- illicit trafficking in nuclear or radioactive materials,
- trafficking in stolen vehicles,
- rape,
- arson,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft/ships,
- sabotage.

Article LAW.SURR.79: Grounds for mandatory non-execution of the arrest warrant

Execution of the arrest warrant shall be refused in the following cases:

(a) if the offence on which the arrest warrant is based is covered by amnesty in the executing State, where that State had jurisdiction to prosecute the offence under its own criminal law;

(b) if the competent executing judicial authority is informed that the requested person has been finally judged by a State in respect of the same acts provided that, if a penalty has been imposed, has been enforced, is in the process of being enforced or can no longer be enforced under the law of the sentencing State ;

(c) if the person who is the subject of the arrest warrant may not, owing to his age, be held criminally responsible for the acts on which the arrest warrant is based under the law of the executing State.

Article LAW.SURR.80: Other grounds for non-execution of the arrest warrant

1. Execution of the arrest warrant may be refused in the following cases:

(a) if, in one of the cases referred to in Article LAW.SURR.78 [Scope] (2), the act on which the arrest warrant is based does not constitute an offence under the law of the executing State; however, in relation to taxes or duties, customs and exchange, execution of the arrest warrant shall not be refused on the ground that the law of the executing State does not impose the same kind of tax or duty or does not contain the same type of rules as regards taxes, duties and customs and exchange regulations as the law of the issuing State;

(b) where the person who is the subject of the arrest warrant is being prosecuted in the executing State for the same act as that on which the arrest warrant is based;

(c) where the judicial authorities of the executing State have decided either not to prosecute for the offence on which the arrest warrant is based or to halt proceedings, or where a final judgement has been passed upon the requested person in a State, in respect of the same acts, which prevents further proceedings;

(d) where the criminal prosecution or punishment of the requested person is statute-barred according to the law of the executing State and the acts fall within the jurisdiction of that State under its own criminal law;

(e) if the executing judicial authority is informed that the requested person has been finally judged by a third State in respect of the same acts provided that, if a penalty has been imposed, has been enforced, is in the process of being enforced or can no longer be enforced under the law of the sentencing State;

(f) if the arrest warrant has been issued for the purposes of execution of a custodial sentence or detention order, where the requested person is staying in, or is a national or a resident of the executing State and that State undertakes to execute the sentence or detention order in accordance with its domestic law;

(g) where the arrest warrant relates to offences which:

(i) are regarded by the law of the executing State as having been committed in whole or in part in the territory of the executing State or in a place treated as such; or

(ii) have been committed outside the territory of the issuing State and the law of the executing State does not allow prosecution for the same offences when committed outside its territory;

(h) if the arrest warrant has been issued for the purpose of executing a custodial sentence or a detention order, where the requested person did not appear in person at the trial resulting in the decision, unless the arrest warrant states that the person, in accordance with further procedural requirements defined in the domestic law of the issuing State:

(i) in due time:

A. either was summoned in person and thereby informed of the scheduled date and place of the trial which resulted in the decision, or by other means actually received official information of the scheduled date and place of that trial in such a manner that it was unequivocally established that he or she was aware of the scheduled trial;

and

B. was informed that a decision may be handed down if he or she does not appear for the trial;

or

(ii) being aware of the scheduled trial, had given a mandate to a lawyer, who was either appointed by the person concerned or by the State, to defend him or her at the trial, and was indeed defended by that lawyer at the trial;

or

(iii) after being served with the decision and being expressly informed about the right to a retrial, or an appeal, in which the person has the right to participate and which allows the merits of the case, including fresh evidence, to be re-examined, and which may lead to the original decision being reversed:

A. expressly stated that he or she does not contest the decision;

or

B. did not request a retrial or appeal within the applicable time frame;

or

(iv) was not personally served with the decision but:

A. will be personally served with it without delay after the surrender and will be expressly informed of his or her right to a retrial, or an appeal, in which the

person has the right to participate and which allows the merits of the case, including fresh evidence, to be re-examined, and which may lead to the original decision being reversed;

and

B. will be informed of the time frame within which he or she has to request such a retrial or appeal, as mentioned in the relevant arrest warrant;

(i) when there are reasons to believe, on the basis of objective elements, that the said arrest warrant has been issued for the purpose of prosecuting or punishing a person on the grounds of his or her sex, race, religion, ethnic origin, nationality, language, political opinions or sexual orientation, or that that person's position may be prejudiced for any of these reasons.

2. In case the arrest warrant is issued for the purpose of executing a custodial sentence or detention order under the conditions of paragraph 1 (h) (iv) and the person concerned has not previously received any official information about the existence of the criminal proceedings against him or her, he or she may, when being informed about the content of the arrest warrant, request to receive a copy of the judgment before being surrendered. Immediately after having been informed about the request, the issuing authority shall provide the copy of the judgment via the executing authority to the person sought. The request of the person sought shall neither delay the surrender procedure nor delay the decision to execute the arrest warrant. The provision of the judgment to the person concerned is for information purposes only; it shall neither be regarded as a formal service of the judgment nor actuate any time limits applicable for requesting a retrial or appeal.

3. In case a person is surrendered under the conditions of paragraph (1) (h) (iv) and he or she has requested a retrial or appeal, the detention of that person awaiting such retrial or appeal shall, until these proceedings are finalised, be reviewed in accordance with the domestic law of the issuing State, either on a regular basis or upon request of the person concerned. Such a review shall in particular include the possibility of suspension or interruption of the detention. The retrial or appeal shall begin within due time after the surrender.

Article LAW.SURR.81: Political offence exception

1. Execution may not be refused on the ground that the offence may be regarded by the executing State as a political offence, as an offence connected with a political offence or an offence inspired by political motives.

2. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand, may make, however, a declaration to the effect that paragraph 1 will be applied only in relation to:

(a) the offences referred to in Articles 1 and 2 of the European Convention on the Suppression of Terrorism;

(b) offences of conspiracy or association — which correspond to the description of behaviour referred to in Article LAW.SURR.78 [Scope] (3) — to commit one or more of the offences referred to in Articles 1 and 2 of the European Convention on the Suppression of Terrorism; and

(c) Articles 3 to 14 of the Directive of 15 March 2017 on combating terrorism.

3. Where an arrest warrant has been issued by a State having made a declaration as referred to in paragraph 2, or by a State on behalf of which such a declaration has been made, the State executing the arrest warrant, may apply reciprocity.

Article LAW.SURR.82: Nationality exception

1. Execution may not be refused on the ground that the person claimed is a national of the executing State.

2. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand, may make a declaration to the effect that their own nationals will not be surrendered or that surrender of their own nationals will be authorised only under certain specified conditions.

3. Where an arrest warrant has been issued by a State having made a declaration as referred to in paragraph 2, or by a State for which such a declaration has been made, any other State may, in the execution of the arrest warrant, apply reciprocity.

Article LAW.SURR.83: Guarantees to be given by the issuing State in particular cases

The execution of the arrest warrant by the executing judicial authority may be subject to the following conditions:

(a) if the offence on the basis of which the arrest warrant has been issued is punishable by custodial life sentence or lifetime detention order the execution of the said arrest warrant may be subject to the condition that the issuing State gives an assurance deemed sufficient by the executing State that it will review the penalty or measure imposed, on request or at the latest after 20 years, or will encourage the application of measures of clemency to which the person is entitled to apply for under the law or practice of the issuing State, aiming at a non-execution of such penalty or measure;

(b) where a person who is the subject of an arrest warrant for the purposes of prosecution is a national or resident of the executing State, surrender may be subject to the condition that the person, after being heard, is returned to the executing State in order to serve there the custodial sentence or detention order passed against him in the issuing State.

Article LAW.SURR.84: Determination of the competent judicial authorities

1. The issuing judicial authority shall be the judicial authority of the issuing State which is competent to issue an arrest warrant by virtue of the domestic law of that State.

2. The executing judicial authority shall be the judicial authority of the executing State which is competent to execute the arrest warrant by virtue of the domestic law of that State.

3. The Parties shall inform each other of their competent authorities.

Article LAW.SURR.85: Recourse to the central authority

1. The Parties may notify each other of the central authority for each State, having designated such an authority, or, when the legal system of the relevant State so provides, of more than one central authority to assist the competent judicial authorities.

2. In doing so the Parties may indicate that, as a result of the organisation of the internal judicial system of the relevant States, the central authority(ies) is/are responsible for the administrative transmission and reception of arrest warrants as well as for all other official correspondence relating thereto. These indications shall be binding upon all the authorities of the issuing State.

Article LAW.SURR.86: Content and form of the arrest warrant

1. The arrest warrant shall contain the following information set out in accordance with the form contained in the ANNEX LAW-7:

(a) the identity and nationality of the requested person;

(b) the name, address, telephone and fax numbers and e-mail address of the issuing judicial authority;

(c) evidence of an enforceable judgement, an arrest warrant or any other enforceable judicial decision having the same effect, coming within the scope of Article LAW.SURR.77 [Definitions] and Article LAW.SURR.78 [Scope];

(d) the nature and legal classification of the offence, particularly in respect of Article LAW.SURR.78 [Scope];

(e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the requested person;

(f) the penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing State;

(g) if possible, other consequences of the offence.

2. The arrest warrant must be translated into the official language or one of the official languages of the executing State. Any Party may, before the date of entry into force of this Agreement or at a later date, make a declaration to the effect that a translation in one or more other official languages of a State will be accepted.

Article LAW.SURR.87: Transmission of an arrest warrant

When the location of the requested person is known, the issuing judicial authority may transmit the arrest warrant directly to the executing judicial authority.

Article LAW.SURR.88: Detailed procedures for transmitting an arrest warrant

1. If the issuing judicial authority does not know the competent executing judicial authority, it shall make the requisite enquiries, in order to obtain that information from the executing State.

2. The issuing judicial authority may call on the International Criminal Police Organisation ("Interpol") to transmit an arrest warrant.

3. The issuing judicial authority may forward the arrest warrant by any secure means capable of producing written records under conditions allowing the executing State to establish its authenticity.

4. All difficulties concerning the transmission or the authenticity of any document needed for the execution of the arrest warrant shall be dealt with by direct contacts between the judicial authorities involved, or, where appropriate, with the involvement of the central authorities of the States.

5. If the authority which receives an arrest warrant is not competent to act upon it, it shall automatically forward the arrest warrant to the competent authority in its State and shall inform the issuing judicial authority accordingly.

Article LAW.SURR.89: Rights of a requested person

1. When a requested person is arrested for the purpose of the execution of an arrest warrant, the executing judicial authority shall, in accordance with its domestic law, inform that person of the arrest warrant and of its contents, and also of the possibility of consenting to surrender to the issuing judicial authority. The requested person shall be provided promptly with an appropriate Letter of Rights containing information on the rights referred to in this Article and on the right to be heard by a judicial authority, if the requested person does not consent to the surrender. The Letter of Rights shall be drafted in a simple and accessible language.

2. A requested person who is arrested for the purpose of the execution of an arrest warrant and who does not speak or understand the language of the proceedings shall have the right to a translation of the arrest warrant and to interpretation during the relevant proceedings.

3. A requested person shall have the right to be assisted by a lawyer in accordance with the domestic law of the executing State upon arrest.

4. The competent authority in the executing State shall, without undue delay after arrest, inform the requested persons that they have the right to appoint a lawyer in the issuing State, for the purpose of assisting the lawyer in the executing State in the arrest warrant proceedings.

5. Where the requested person wishes to exercise the right to appoint a lawyer in the issuing State and does not have such a lawyer, the competent authority in the executing State shall promptly inform the competent authority in the issuing State. The competent authority of that State shall, without undue delay, provide the requested person with information to facilitate them in appointing a lawyer there.

6. The right of a requested person to appoint a lawyer in the issuing State is without prejudice to the time-limits set out in Article LAW.SURR.102 [Time limits for surrender of the person].

7. A requested person shall have a right to legal aid in the executing State upon arrest until surrender of the person or until the decision not to surrender the person becomes final.

8. A requested person who is subject of the arrest warrant proceeding for the purpose of conducting a criminal prosecution shall have the right to legal aid in the issuing State for the purpose of such proceedings in the executing State, in so far as legal aid is necessary to ensure effective access to justice.

9. A requested person who is arrested shall have the right to have at least one person, such as a relative or an employer, nominated by the person, informed of the arrest without undue delay if the person so wishes, unless temporary derogations are justified in the light of the particular circumstances of the case on the basis of the following compelling reasons:

(a) where there is an urgent need to avert serious adverse consequences for the life, liberty or physical integrity of a person;

(b) where there is an urgent need to prevent a situation where criminal proceedings could be substantially jeopardised.

10. A requested person who is arrested shall have the right to communicate without delay with at least one third person, such as a relative nominated by the person. The exercise of this right may be limited or deferred in view of imperative requirements or proportionate operational requirements.

11. A requested person who is a non-national of the executing State and who is arrested shall have the right to have the consular authorities of his State of nationality informed of the arrest without undue delay and to communicate with those authorities, if the person so wishes.

Article LAW.SURR.90 Rights of a requested person who is a child

In addition to the rights provided for in Article LAW.SURR.89 [Rights of a requested person], where the requested person is a child, that is a person below the age of 18 years, that person shall have the right:

(a) to have the holder of parental responsibility informed as soon as possible of the arrest and of the reasons pertaining thereto, unless this would be contrary to the best interests of the child, or if it is not possible because, after reasonable efforts have been made, no holder of parental responsibility can be reached or his or her identity is unknown, or he or she could, on the basis of objective and factual circumstances substantially jeopardise the proceedings, in which case another appropriate adult who is nominated by the child and accepted as such by the competent authority shall be informed;

(b) to be assisted by a lawyer in accordance with the domestic law of the executing State upon arrest;

(c) to a medical examination without undue delay with a view, in particular, to assessing the general mental and physical condition;

(d) to be held separately from adults unless it is considered to be in the child's bests interests not to do so;

(e) to have privacy respected;

(f) to be accompanied by the holder of parental responsibility or another appropriate adult during court hearings in which they are involved.

Article LAW.SURR.91: Keeping the person in detention

When a person is arrested on the basis of an arrest warrant, the executing judicial authority shall take a decision on whether the requested person should remain in detention, in accordance with the law of the executing State. The person may be released provisionally at any time in conformity with the domestic law of the executing State, provided that the competent authority of the said State takes all the measures it deems necessary to prevent the person absconding.

Article LAW.SURR.92: Consent to surrender

1. If the arrested person indicates that he or she consents to surrender, that consent and, if appropriate, express renunciation of entitlement to the 'speciality rule', referred to in Article LAW.SURR.106 [Possible prosecution for other offences] (2), shall be given before the executing judicial authority, in accordance with the domestic law of the executing State.

2. Each State shall adopt the measures necessary to ensure that consent and, where appropriate, renunciation, as referred to in paragraph 1, are established in such a way as to that the person concerned has expressed them voluntarily and in full awareness of the consequences. To that end, the requested person shall have the right to a lawyer.

3. The consent and, where appropriate, renunciation, as referred to in paragraph 1, shall be formally recorded in accordance with the procedure laid down by the domestic law of the executing State.

4. In principle, consent may not be revoked. Each State may provide that consent and, if appropriate, renunciation may be revoked, in accordance with the rules applicable under its domestic law. In this case, the period between the date of consent and that of its revocation shall not be taken into consideration in establishing the time limits laid down in Article LAW.SURR.102 [Time limits for surrender of the person]. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand, may make, at the time of notification provided for in Article LAW.OTHER.134 [Notifications] (1), a declaration indicating that they wish to have recourse to this possibility, specifying the procedures whereby revocation of consent shall be possible and any amendment to them.

Article LAW.SURR.93: Hearing of the requested person

Where the arrested person does not consent to his or her surrender as referred to in Article LAW.SURR.92 [Consent to surrender], he or she shall be entitled to be heard by the executing judicial authority, in accordance with the law of the executing State.

Article LAW.SURR.94: Surrender decision

1. The executing judicial authority shall decide, within the time limits and under the conditions defined in this Chapter, whether the person is to be surrendered.

2. If the executing judicial authority finds the information communicated by the issuing State to be insufficient to allow it to decide on surrender, it shall request that the necessary supplementary information, in particular with respect to Article LAW.SURR.79 [Grounds for mandatory non-execution of the arrest warrant] to Article LAW.SURR.81 [Political offence exception], Article LAW.SURR.83 [Guarantees to be given by the issuing State in particular cases] and Article LAW.SURR.86 [Content and form of the arrest warrant], be furnished as a matter of urgency and may fix a time limit for the receipt thereof, taking into account the need to observe the time limits set in Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant].

3. The issuing judicial authority may at any time forward any additional useful information to the executing judicial authority.

Article LAW.SURR.95: Decision in the event of multiple requests

1. If two or more States have issued a European arrest warrant or an arrest warrant for the same person, the decision as to which of those warrants shall be executed shall be taken by the executing judicial authority with due consideration of all the circumstances and especially the relative seriousness and place of the offences, the respective dates of the arrest warrant or European arrest warrant and whether they have been issued for the purposes of prosecution or for execution of a custodial sentence or detention order, and of legal obligations of Member States deriving from Union law regarding in particular the principles of freedom of movement and non-discrimination on grounds of nationality.

2. The executing judicial authority of a Member State may seek the advice of Eurojust when making the choice referred to in paragraph 1.

3. In the event of a conflict between an arrest warrant and a request for extradition presented by a third State, the decision as to whether the arrest warrant or the extradition request takes precedence shall be taken by the competent authority of the executing State with due consideration of all the circumstances, in particular those referred to in paragraph 1 and those mentioned in the applicable convention.

4. This Article shall be without prejudice to States' obligations under the Statute of the International Criminal Court.

Article LAW.SURR.96: Time limits and procedures for the decision to execute the arrest warrant

1. An arrest warrant shall be dealt with and executed as a matter of urgency.

2. In cases where the requested person consents to his surrender, the final decision on the execution of the arrest warrant should be taken within a period of 10 days after consent has been given.

3. In other cases, the final decision on the execution of the arrest warrant should be taken within a period of 60 days after the arrest of the requested person.

4. Where in specific cases the arrest warrant cannot be executed within the time limits laid down in paragraphs 2 or 3, the executing judicial authority shall immediately inform the issuing judicial authority thereof, giving the reasons for the delay. In such case, the time limits may be extended by a further 30 days.

5. The Union, on behalf of any of its Member States, may make, at the time of notification provided for in Article LAW.OTHER.LAW.OTHER.134 [Notifications] (1), a declaration indicating in which cases paragraphs 3 and 4 will not apply. The United Kingdom may apply reciprocity in relation to the Member States concerned.

6. As long as the executing judicial authority has not taken a final decision on the arrest warrant, it shall ensure that the material conditions necessary for effective surrender of the person remain fulfilled.

7. Reasons must be given for any refusal to execute an arrest warrant.

Article LAW.SURR.97: Situation pending the decision

1. Where the arrest warrant has been issued for the purpose of conducting a criminal prosecution, the executing judicial authority must:

(a) either agree that the requested person should be heard according to Article LAW.SURR.98 [Hearing the person pending the decision];

or

(b) agree to the temporary transfer of the requested person.

2. The conditions and the duration of the temporary transfer shall be determined by mutual agreement between the issuing and executing judicial authorities.

3. In the case of temporary transfer, the person must be able to return to the executing State to attend hearings concerning him or her as part of the surrender procedure.

Article LAW.SURR.98: Hearing the person pending the decision

1. The requested person shall be heard by a judicial authority, assisted by a lawyer designated in accordance with the law of the State of the requesting judicial authority.

2. The requested person shall be heard in accordance with the law of the executing State and with the conditions determined by mutual agreement between the issuing and executing judicial authorities.

3. The competent executing judicial authority may assign another judicial authority of its State to take part in the hearing of the requested person in order to ensure the proper application of this Article and of the conditions laid down.

Article LAW.SURR.99: Privileges and immunities

1. Where the requested person enjoys a privilege or immunity regarding jurisdiction or execution in the executing State, the time limits referred to in Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant] shall not start running unless, and counting from the day when, the executing judicial authority is informed of the fact that the privilege or immunity has been waived.

2. The executing State shall ensure that the material conditions necessary for effective surrender are fulfilled when the person no longer enjoys such privilege or immunity.

3. Where power to waive the privilege or immunity lies with an authority of the executing State, the executing judicial authority shall request it to exercise that power forthwith. Where power to waive the privilege or immunity lies with an authority of another State, third State or international organisation, it shall be for the issuing judicial authority to request it to exercise that power.

Article LAW.SURR.100: Competing international obligations

This Agreement shall not prejudice the obligations of the executing State where the requested person has been extradited to that State from a third State and where that person is protected by provisions of the arrangement under which he or she was extradited concerning speciality. The executing State shall take all necessary measures for requesting forthwith the consent of the State from which the requested person was extradited so that he or she can be surrendered to the State which issued the arrest warrant. The time limits referred to in Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant] shall not start running until the day on which these speciality rules cease to apply.

Pending the decision of the third State from which the requested person was extradited, the executing State will ensure that the material conditions necessary for effective surrender remain fulfilled.

Article LAW.SURR.101: Notification of the decision

The executing judicial authority shall notify the issuing judicial authority immediately of the decision on the action to be taken on the arrest warrant.

Article LAW.SURR.102: Time limits for surrender of the person

1. The person requested shall be surrendered as soon as possible on a date agreed between the authorities concerned.

2. He or she shall be surrendered no later than 10 days after the final decision on the execution of the arrest warrant.

3. If the surrender of the requested person within the period laid down in paragraph 2 is prevented by circumstances beyond the control of the issuing or executing State, the executing and issuing judicial authorities shall immediately contact each other and agree on a new surrender date. In that event, the surrender shall take place within 10 days of the new date thus agreed.

4. The surrender may exceptionally be temporarily postponed for serious humanitarian reasons, for example if there are substantial grounds for believing that it would manifestly endanger the requested person's life or health. The execution of the arrest warrant shall take place as soon as these grounds have ceased to exist. The executing judicial authority shall immediately inform the issuing judicial authority and agree on a new surrender date. In that event, the surrender shall take place within 10 days of the new date thus agreed.

5. Upon expiry of the time limits referred to in paragraphs 2 to 4, if the person is still being held in custody he shall be released.

Article LAW.SURR.103: Postponed or conditional surrender

1. The executing judicial authority may, after deciding to execute the arrest warrant, postpone the surrender of the requested person so that he or she may be prosecuted in the executing State or, if he or she has already been sentenced, so that he or she may serve, in its territory, a sentence passed for an act other than that referred to in the arrest warrant.

2. Instead of postponing the surrender, the executing judicial authority may temporarily surrender the requested person to the issuing State under conditions to be determined by mutual agreement between the executing and the issuing judicial authorities. The agreement shall be made in writing and the conditions shall be binding on all the authorities in the issuing State.

Article LAW.SURR.104: Transit

1. Each State shall permit the transit through its territory of a requested person who is being surrendered provided that it has been given information on:

(a) the identity and nationality of the person subject to the arrest warrant;

(b) the existence of an arrest warrant;

(c) the nature and legal classification of the offence;

(d) the description of the circumstances of the offence, including the date and place.

2. The State, on behalf of which a declaration has been made in accordance with Article LAW.SURR.82 [Nationality exception] (2), to the effect that nationals will not be surrendered or that surrender will be authorised only under certain specified conditions, may, under the same terms, refuse the transit of its nationals through its territory or submit it to the same conditions.

3. The Parties shall notify each other of the authority designated for each State responsible for receiving transit requests and the necessary documents, as well as any other official correspondence relating to transit requests.

4. The transit request and the information set out in paragraph 1 may be addressed to the authority designated pursuant to paragraph 3 by any means capable of producing a written record. The State of transit shall notify its decision by the same procedure.

5. This Chapter does not apply in the case of transport by air without a scheduled stopover. However, if an unscheduled landing occurs, the issuing State shall provide the authority designated pursuant to paragraph 3 with the information provided for in paragraph 1.

6. Where a transit concerns a person who is to be extradited from a third State to a State, this Article shall apply *mutatis mutandis*. In particular the expression 'arrest warrant' as defined in Article LAW.SURR.77 [Definitions] (a) shall be deemed to be replaced by 'extradition request'.

Article LAW.SURR.105: Deduction of the period of detention served in the executing State

1. The issuing State shall deduct all periods of detention arising from the execution of an arrest warrant from the total period of detention to be served in the issuing State as a result of a custodial sentence or detention order being passed.

2. To that end, all information concerning the duration of the detention of the requested person on the basis of the arrest warrant shall be transmitted by the executing judicial authority or the central authority designated under Article LAW.SURR.85 [Recourse to the central authority] to the issuing judicial authority at the time of the surrender.

Article LAW.SURR.106: Possible prosecution for other offences

1. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand, may notify each other that, in relations with other States to which the same notification applies, consent is presumed to have been given for the prosecution, sentencing or detention with a view to the carrying out of a custodial sentence or detention order for an offence committed prior to his or her surrender, other than that for which he or she was surrendered, unless in a particular case the executing judicial authority states otherwise in its decision on surrender.

2. Except in the cases referred to in paragraphs 1 and 3, a person surrendered may not be prosecuted, sentenced or otherwise deprived of his or her liberty for an offence committed prior to his or her surrender other than that for which he or she was surrendered.

3. Paragraph 2 does not apply in the following cases:

(a) when the person having had an opportunity to leave the territory of the State to which he or she has been surrendered has not done so within 45 days of his or her final discharge, or has returned to that territory after leaving it;

(b) the offence is not punishable by a custodial sentence or detention order;

(c) the criminal proceedings do not give rise to the application of a measure restricting personal liberty;

(d) when the person could be liable to a penalty or a measure not involving the deprivation of liberty, in particular a financial penalty or a measure in lieu thereof, even if the penalty or measure may give rise to a restriction of his or her personal liberty;

(e) when the person consented to be surrendered, where appropriate at the same time as he or she renounced the speciality rule, in accordance with Article LAW.SURR.92 [Consent to surrender];

(f) when the person, after his/her surrender, has expressly renounced entitlement to the speciality rule with regard to specific offences preceding his/her surrender. Renunciation shall be given before the competent judicial authorities of the issuing State and shall be recorded in accordance with that State's domestic law. The renunciation shall be drawn up in such a way as to make clear that the person has given it voluntarily and in full awareness of the consequences. To that end, the person shall have the right to a lawyer;

(g) where the executing judicial authority which surrendered the person gives its consent in accordance with paragraph 4.

4. A request for consent shall be submitted to the executing judicial authority, accompanied by the information mentioned in Article LAW.SURR.86 [Content and form of the arrest warrant](1) and a translation as referred to in Article LAW.SURR.86 [Content and form of the arrest warrant](2). Consent shall be given when the offence for which it is requested is itself subject to surrender in accordance with the provisions of this Chapter. Consent shall be refused on the grounds referred to in Article LAW.SURR.79 [Grounds for mandatory non-execution of the arrest warrant] and otherwise may be refused only on the grounds referred to in Article LAW.SURR.80 [Other grounds for non-execution of the arrest warrant], or Article LAW.SURR.81 [Political offence exception] (2) and Article LAW.SURR.82 [Nationality exception](2). The decision shall be taken no later than 30 days after receipt of the request. For the situations mentioned in Article LAW.SURR.83 [Guarantees to be given by the issuing State in particular cases] the issuing State must give the guarantees provided for therein.

Article LAW.SURR.107: Surrender or subsequent extradition

1. The United Kingdom, on the one hand, and the Union, on behalf of any of its Member States, on the other hand, may notify each other that, in relations with other States to which the same notification applies, the consent for the surrender of a person to a State other than the executing State pursuant to an arrest warrant or European arrest warrant issued for an offence committed prior to his or her surrender is presumed to have been given, unless in a particular case the executing judicial authority states otherwise in its decision on surrender.

2. In any case, a person who has been surrendered to the issuing State pursuant to an arrest warrant may, without the consent of the executing State, be surrendered to a State other than the executing State pursuant to an arrest warrant or European arrest warrant issued for any offence committed prior to his or her surrender in the following cases:

(a) where the requested person, having had an opportunity to leave the territory of the State to which he or she has been surrendered, has not done so within 45 days of his final discharge, or has returned to that territory after leaving it;

(b) where the requested person consents to be surrendered to a State other than the executing State pursuant to an arrest warrant or European arrest warrant. Consent shall be given before the competent judicial authorities of the issuing State and shall be recorded in accordance with that State's domestic law. It shall be drawn up in such a way as to make clear that the person concerned has given it voluntarily and in full awareness of the consequences. To that end, the requested person shall have the right to a lawyer;

(c) where the requested person is not subject to the speciality rule, in accordance with Article LAW.SURR.106 [Possible prosecution for other offences] (3)(a), (e), (f) and (g).

3. The executing judicial authority shall consent to the surrender to another State according to the following rules:

(a) the request for consent shall be submitted in accordance with Article LAW.SURR.87 [Transmission of an arrest warrant], accompanied by the information mentioned in Article LAW.SURR.86 [Content and form of the arrest warrant](1) and a translation as stated in Article LAW.SURR.86 [Content and form of the arrest warrant](2);

(b) consent shall be given when the offence for which it is requested is itself subject to surrender in accordance with the provisions of this Agreement;

(c) the decision shall be taken no later than 30 days after receipt of the request;

(d) consent shall be refused on the grounds referred to in Article LAW.SURR.79 [Grounds for mandatory non-execution of the arrest warrant] and otherwise may be refused only on the grounds referred to in Article LAW.SURR.80 [Other grounds for non-execution of the arrest warrant] or Article LAW.SURR.81 [Political offence exception] (2) and Article LAW.SURR.82 [Nationality exception](2).

4. For the situations referred to in Article LAW.SURR.83 [Guarantees to be given by the issuing State in particular cases], the issuing State must give the guarantees provided for therein.

5. Notwithstanding paragraph 1, a person who has been surrendered pursuant to an arrest warrant shall not be extradited to a third State without the consent of the competent authority of the State which surrendered the person. Such consent shall be given in accordance with the Conventions by which that State is bound, as well as with its domestic law.

Article LAW.SURR.108: Handing over of property

1. At the request of the issuing judicial authority or on its own initiative, the executing judicial authority shall, in accordance with its domestic law, seize and hand over property which:

(a) may be required as evidence; or

(b) has been acquired by the requested person as a result of the offence.

2. The property referred to in paragraph 1 shall be handed over even if the arrest warrant cannot be carried out owing to the death or escape of the requested person.

3. If the property referred to in paragraph 1 is liable to seizure or confiscation in the territory of the executing State, the latter may, if the property is needed in connection with pending criminal proceedings, temporarily retain it or hand it over to the issuing State, on condition that it is returned.

4. Any rights which the executing State or third parties may have acquired in the property referred to in paragraph 1 shall be preserved. Where such rights exist, the issuing State shall return the property without charge to the executing State as soon as the criminal proceedings have been terminated.

Article LAW.SURR.109: Expenses

1. Expenses incurred in the territory of the executing State for the execution of an arrest warrant shall be borne by that State.

2. All other expenses shall be borne by the issuing State.

Article LAW.SURR.110: Relation to other legal instruments

1. Without prejudice to their application in relations between States and third States, this Chapter shall, from its date of entry into force, replace the corresponding provisions of the following conventions applicable in the field of extradition in relations between the United Kingdom, on the one hand, and Member States, on the other hand:

(a) the European Convention on Extradition of 13 December 1957 and its additional protocols; and

(b) the European Convention on the suppression of terrorism of 27 January 1977 as far as extradition is concerned as amended by the 2003 Protocol once it will enter into force.

2. Where the conventions or agreements referred to in paragraph 1 apply to the territories of States or to territories for whose external relations a State is responsible to which this Chapter does not apply, these instruments shall continue to govern the relations existing between those territories and the other States.

Article LAW.SURR.111: Review of declarations

When carrying out the joint review of this Chapter as referred to in Article LAW.OTHER.135 [Review and evaluation](1)(b), the Parties shall also consider the need to maintain the declarations made under Article LAW.SURR.78 [Scope](4), Article LAW.SURR.81 [Political offence exception] (2), Article LAW.SURR.82 [Nationality exception] (2) and Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant](5) of this Agreement. Where the declarations referred to in Article LAW.SURR.82 [Nationality exception](2) are not renewed, they shall expire five years after the date of entry into force of this Agreement.

Article LAW.SURR.112: Ongoing arrest warrants in case of disapplication

Notwithstanding Article.LAW.OTHER.136 [Suspension and disapplication] (1) and (2) and Article FINPROV.8 [Termination], the provisions of this Chapter shall apply in respect of arrest warrants where the requested person was arrested before the disapplication of this Chapter for the purposes of the execution of an arrest warrant, irrespective of the decision of the executing judicial authority as to whether the requested person is to remain in detention or be provisionally released.

Chapter eight: Mutual assistance

Article LAW.MUTAS.113: Objective

The objective of this Chapter is to supplement the provisions and facilitate the application between Member States to which the following Convention and Protocols are applicable, on the one hand, and the United Kingdom, on the other hand, of:

(a) the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, the "European Mutual Assistance Convention";

(b) the Additional Protocol of 17 March 1978 to the European Mutual Assistance Convention;

(c) the Second Additional Protocol of 8 November 2001 to the European Mutual Assistance Convention.

Article LAW.MUTAS.114: Definitions

For the purposes of this Chapter, "competent authority" means any authority which is competent to send and/or receive requests for mutual assistance in accordance with the provisions of the Convention and the Protocols referred to in Article LAW.MUTAS.113 [Objective] and as defined by States in their respective declarations addressed to the Secretary General of the Council of Europe. “Competent authority” shall in any case include the European Public Prosecutor’s Office, established in accordance with Council Regulation (EU) 2017/1939, for the purpose of mutual assistance in respect of offences for which the European Public Prosecutor’s Office has exercised its competences in accordance with Articles 22, 23 and 25 of Council Regulation (EU) 2017/1939.

Article LAW.MUTAS.115: Recourse to a different type of investigative measure

1. The competent authority of the requested State shall have, wherever possible, recourse to an investigative measure other than that provided for in the request for mutual assistance where:

(a) the investigative measure indicated in the request does not exist under the law of the requested State; or

(b) the investigative measure indicated in the request would not be available in a similar domestic case.

2. Without prejudice to the grounds for refusal available under the Convention and Protocols referred to in Article LAW.MUTAS.113 [Objective], as well as under Article LAW.MUTAS.117 [Ne bis in idem], paragraph (1) does not apply to the following investigative measures, which always have to be available under the law of the requested State:

(a) the obtaining of information contained in databases held by police or judicial authorities and directly accessible by the competent authority of the requested State in the framework of criminal proceedings;

(b) the hearing of a witness, expert, victim, suspected or accused person or third party in the territory of the requested State;

(c) any non-coercive investigative measure as defined under the law of the requested State;

(d) the identification of persons holding a subscription of a specified phone number or IP address.

3. The competent authority of the requested State may also have recourse to an investigative measure other than that indicated in the request for mutual assistance where the investigative measure selected by the competent authority of the requested State would achieve the same result by less intrusive means than the investigative measure indicated in the request.

4. When the competent authority of the requested State decides to avail itself of the possibility referred to in paragraphs 1 and 3, it shall first inform the competent authority of the requesting State, which may decide to withdraw or supplement the request.

5. Where, in accordance with paragraph 1, the investigative measure indicated in the request does not exist under the law of the requested State or it would not be available in a similar domestic case and where there is no other investigative measure which would have the same result as the investigative measure requested, the competent authority of the requested State shall notify the competent authority of the requesting State that it has not been possible to provide the assistance requested.

Article LAW.MUTAS.116: Obligation to inform

1. The competent authority of the requested State which receives the request for mutual assistance shall, without delay, and in any case within a week of the reception of the request, acknowledge the receipt thereof. The same obligation shall apply to the authority to which the request was transmitted in accordance with Article 18 of the European Mutual Assistance Convention.

2. The competent authority of the requested State shall inform the competent authority of the requesting State immediately by any means:

(a) if it is impossible to execute the request for mutual assistance due to the fact that the request is incomplete or manifestly incorrect; or

(b) if the competent authority of the requested State, in the course of the execution of the request for mutual assistance, considers without further enquiries that it may be appropriate to carry out investigative measures not initially foreseen, or which could not be specified when the request for mutual assistance was made, in order to enable the competent authority of the requesting State to take further action in the specific case.

Article LAW.MUTAS.117: Ne bis in idem

Mutual assistance may be refused, in addition to the grounds listed in the Convention and the Protocols referred to in Article LAW.MUTAS.113 [Objective], if the person for whom the assistance is requested and who is subject to criminal investigations, prosecutions or other proceedings, including judicial proceedings, in the requesting State, has been finally judged by a State in respect of the same acts provided that, if a penalty has been imposed, has been enforced, is in the process of being enforced or can no longer be enforced under the law of the sentencing State.

Article LAW.MUTAS.118: Time limits

1. A request for mutual assistance shall be executed as soon as possible but no later than 120 days after its receipt.

2. Where it is indicated in the request for mutual assistance that, due to procedural deadlines, the seriousness of the offence or other particularly urgent circumstances, a shorter deadline than that provided in paragraph 1 is necessary, or where it is indicated in the request that a measure for mutual assistance must be carried out on a specific date, the requested State shall take as full account as possible of this requirement.

3. Where a request for mutual assistance is made for taking of provisional measures pursuant to Article 24 of the Second Additional Protocol of 8 November 2001 to the European Mutual Assistance Convention, the competent authority of the requested State shall decide and communicate the decision on the provisional measure as soon as possible and, wherever practicable, within 24 hours of receipt of the request. Before lifting any provisional measure taken pursuant to this article, the competent authority of the requested State shall, wherever possible, give the competent authority of the requesting State an opportunity to present its reasons in favour of continuing the measure.

4. Where in a specific case, the time limit set out in paragraph 1 or the specific date set out in paragraph 2 cannot be met, the competent authority of the requested State shall, without delay, inform the competent authority of the requesting State by any means, giving the reasons for the delay and shall consult with the competent authority of the requesting State on the appropriate timing to execute the request for mutual assistance.

Article LAW.MUTAS.119: Joint Investigation Teams

The competent authorities shall consider to use combined legal bases for the mutual agreement of a Joint Investigation Teams to address the specific needs of the different authorities especially setting out on one hand the relations between the United Kingdom and the Member States and on the other hand, ensuring the application of Union law for the relationship between Member States within the Joint Investigation Team.

Chapter nine: Exchange of information extracted from criminal records

Article LAW.EXINF.120: Objective

1. The objective of this Chapter is to enable exchanges of information extracted from criminal records between, on the one hand, the Member States and, on the other hand, the United Kingdom.

2. In the relations between the United Kingdom and the Member States and without prejudice to their application in the relations between States and third States, the provisions of this Chapter:

(a) supplement Article 13 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and its Additional Protocols of 17 March 1978 and 8 November 2001; and

(b) replace Article 22 (1) of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, as supplemented by Article 4 of its Additional Protocol of 17 March 1978.

3. In their relations among each other, the Member States, on the one hand, and the United Kingdom, on the other hand, shall waive the right to rely on their reservations to Article 13 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and to Article 4 of the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 17 March 1978.

Article LAW.EXINF.121: Definitions

For the purpose of this Chapter, the following definitions shall apply:

(a) "conviction" means any final decision of a criminal court against a natural person in respect of a criminal offence, to the extent that the decision is entered in the criminal records of the convicting State;

(b) "criminal proceedings" means the pre-trial stage, the trial stage and the execution of the conviction;

(c) "criminal record" means the domestic register or registers recording convictions in accordance with domestic law;

Article LAW.EXINF.122: Central authorities

1. Each State shall designate one or more central authorities competent for exchanges of information extracted from criminal records pursuant to this Chapter.

2. Each State shall inform the Specialised Committee on Law enforcement and judicial cooperation of the central authority or authorities designated in accordance with paragraph 1.

Article LAW.EXINF.123: Notifications

1. Each State shall take the necessary measures to ensure that all convictions handed down within its territory are accompanied, when provided to its criminal record, by information on the nationality or nationalities of the convicted person if he is a national of another State.

2. The central authority of each State shall inform the central authorities of any other State of all criminal convictions handed down within its territory in respect of nationals of the latter State, as well as of any subsequent alterations or deletions of information contained in the criminal records, as entered in the criminal records. The central authorities of the States shall communicate such information to each other at least once per month.

3. If the central authority of a State becomes aware of the fact that a convicted person is a national of two or more other States, the relevant information shall be transmitted to each of those States, even if the convicted person is a national of the State within whose territory he was convicted.

Article LAW.EXINF.124: Requests for information

1. When information from the criminal record of a State is requested at domestic level for the purposes of criminal proceedings against a person or for any purposes other than that of criminal proceedings, the central authority of that State may, in accordance with its domestic law, submit a

request to the central authority of another State for information and related data to be extracted from the criminal record.

2. When a person asks the central authority of a State other than the one of the person's nationality for information on its own criminal record, that central authority shall submit a request to the central authority of the State of the person's nationality for information and related data to be extracted from the criminal record in order to be able to include such information and related data in the extract to be provided to the person concerned.

Article LAW.EXINF.125: Replies to requests

1. Replies to the requests referred to in Article 13 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 shall be transmitted by the central authority of the requested State to the central authority of the requesting State, as soon as possible and in any event within a period not exceeding twenty working days from the date the request was received.

2. When replying to requests made for the purpose of recruitment for professional or organised voluntary activities involving direct and regular contacts with children, the Member States and the United Kingdom shall lift any limitations stipulated in their domestic law preventing the exchange of information extracted from criminal records for such purposes.

Article LAW.EXINF.126: Channel of communication

The exchange of information extracted from criminal records between the Member States and the United Kingdom shall take place electronically. Technical and procedural specifications are laid down in ANNEX LAW-8.

Chapter ten: Anti-money laundering and counter-terrorism financing

Article LAW.AML.127: Objective

The objective of this Chapter is to support and strengthen the action by the Union and the United Kingdom for preventing and combating money laundering and terrorism financing, including particularly through compliance with Financial Action Task Force (FATF) standards as well as ensuring high standards on transparency and entities subject to anti-money laundering and counter-terrorism frameworks.

Article LAW.AML.128: Definitions

For the purpose of this Chapter, the following definitions apply:

(a) "beneficial owner" means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

(i) in the case of corporate entities:

A. The natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings,

or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with the domestic law of the Parties or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control.

B. If, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(ii) in the case of trusts, all following persons:

A. the settlor(s);

B. the trustee(s);

C. the protector(s), if any;

D. the beneficiaries or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

E. any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(iii) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (ii).

Article LAW.AML.129: Anti-money laundering and counter-terrorism financing

1. The Parties agree to support international efforts to prevent and fight against money laundering and terrorist financing, particularly through compliance with Financial Action Task Force (FATF) standards and associated cooperation. The Parties recognize the need to cooperate on preventing the use of their financial systems to launder the proceeds of all criminal activity, including drug trafficking and corruption, and to combat the financing of terrorism. This cooperation extends to the seizure and confiscation of assets or funds derived from criminal activity, within their respective legal frameworks and laws.

2. The Parties shall exchange relevant information, as appropriate within their respective legal frameworks and laws, and implement the appropriate measures to combat money laundering and the financing of terrorism, guided by the recommendations of the Financial Action Task Force and standards applied by other relevant international bodies active in the area.

Article LAW.AML.130: Beneficial Ownership Transparency for corporate and other legal entities

1. The Parties shall ensure that corporate and other legal entities incorporated within their territories are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. The Parties shall ensure that breaches of this Article are subject to effective, proportionate and dissuasive measures or sanctions.

The Parties shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures in accordance with their domestic anti-money laundering and Counter-Terrorism Financing framework.

The Parties shall require that the beneficial owners of corporate or other legal entities, including through shares, voting rights, ownership interest, bearer shareholdings or control via other means, provide those entities with all the information necessary for the corporate or other legal entity to comply with the requirements in the first subparagraph.

2. The Parties shall require that the information referred to in paragraph 1 can be accessed in a timely manner by their competent authorities and Financial Intelligence Units (FIU).

3. The Parties shall ensure that the information referred to in paragraph 1 is held in a central register, for the EU in each Member State, for example a commercial register, companies register, or a public register.

4. The Parties shall ensure that the information held in the central register referred to in paragraph 3 is adequate, accurate and current, and shall put in place mechanisms to this effect. Such mechanisms shall include requiring obliged entities and, if appropriate and to the extent that this requirement does not interfere unnecessarily with their functions, competent authorities to report any discrepancies they find between the beneficial ownership information available in the central registers and the beneficial ownership information available to them. In the case of reported discrepancies, the Parties shall ensure that appropriate actions be taken to resolve the discrepancies in a timely manner and, if appropriate, a specific mention be included in the central register in the meantime.

5. The Parties shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with their domestic anti-money laundering and counter-terrorism financing framework;

(c) any member of the general public.

The persons referred to in point (c) shall be permitted to access at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held.

The Parties may, under conditions to be determined in domestic law, provide for access to additional information enabling the identification of the beneficial owner. That additional information shall include at least the date of birth or contact details in accordance with data protection rules.

6. The Parties may choose to make the information held in their central registers referred to in paragraph 3 available on the condition of online registration and the payment of a fee, which shall not exceed the administrative costs of making the information available, including costs of maintenance and developments of the register.

7. The Parties shall ensure that competent authorities and FIUs have timely and unrestricted access to all information held in the central register referred to in paragraph 3 without alerting the entity concerned. The Parties shall also allow timely access by obliged entities when taking customer due diligence measures in accordance with their domestic anti-money laundering and counter terrorist financing framework.

Competent authorities granted access to the central register referred to in paragraph 3 shall be those public authorities with designated responsibilities for combating money laundering or terrorist financing, as well as tax authorities, supervisors of obliged entities and authorities that have the function of investigating or prosecuting money laundering, associated predicate offences and terrorist financing, tracing and seizing or freezing and confiscating criminal assets.

8. The Parties shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 3 to the competent authorities and to the FIUs of the other party in a timely manner and free of charge.

9. The Parties shall require that obliged entities do not rely exclusively on the central register referred to in paragraph 3 to fulfil their customer due diligence requirements with their domestic anti-money laundering and counter-terrorism financing rules. Those requirements shall be fulfilled by using a risk-based approach.

10. In exceptional circumstances to be laid down in domestic law of the Parties, where the access referred to in points (b) and (c) of the first subparagraph of paragraph 5 would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable, the Parties may provide for an exemption from such access to all or part of the information on the beneficial ownership on a case-by-case basis. The Parties shall ensure that these exemptions are granted upon a detailed evaluation of the exceptional nature of the circumstances. Rights to an administrative review of the exemption decision and to an effective judicial remedy shall be guaranteed. The Party that has granted exemptions shall publish annual statistical data on the number of exemptions granted and reasons stated.

Exemptions granted pursuant to the first subparagraph shall not apply to the credit institutions and financial institutions, and to notaries and other independent legal professionals that are public officials, where they participate, whether by acting on behalf of and for their client in any financial or

real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

(a) buying and selling of real property or business entities;

(b) managing of client money, securities or other assets;

(c) opening or management of bank, savings or securities accounts;

(d) organisation of contributions necessary for the creation, operation or management of companies;

(e) creation, operation or management of trusts, companies, foundations, or similar structures.

Article LAW.AML.131: Beneficial Ownership Transparency for trusts and other types of legal arrangements

1. The Parties shall ensure that this Article applies to trusts and other types of legal arrangements, such as, inter alia, fiducie, certain types of Treuhand or fideicomiso, where such arrangements have a structure or functions similar to trusts. The Parties shall identify the characteristics to determine where legal arrangements have a structure or functions similar to trusts with regard to such legal arrangements governed under their law.

Each party shall require that trustees of any express trust administered in their territories obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. That information shall include the identity of:

(a) the settlor(s);

(b) the trustee(s);

(c) the protector(s) (if any);

(d) the beneficiaries or class of beneficiaries;

(e) any other natural person exercising effective control of the trust.

The Parties shall ensure that breaches of this Article are subject to effective, proportionate and dissuasive measures or sanctions.

2. The Parties shall ensure that trustees or persons holding equivalent positions in similar legal arrangements as referred to in paragraph 1 of this Article, disclose their status and provide the information referred to in paragraph 1 of this Article to obliged entities in a timely manner, where, as a trustee or as person holding an equivalent position in a similar legal arrangement, they form a business relationship or carry out an occasional transaction above the thresholds set out " in their domestic anti-money laundering and counter-terrorism financing framework for the application of customer due diligence by obliged entities.

3. The Parties shall require that the information referred to in paragraph 1 can be accessed in a timely manner by competent authorities and FIUs.

4. The Parties shall require that the beneficial ownership information of express trusts and similar legal arrangements as referred to in paragraph 1 shall be held in a central beneficial ownership register set up by the Parties where the trustee of the trust or person holding an equivalent position in a similar legal arrangement is established or resides. For the Union the central registers shall be set up at Member State level.

Where the place of establishment or residence of the trustee of the trust or person holding an equivalent position in similar legal arrangement is outside the territory of the Parties, the information referred to in paragraph 1 shall be held in a central register set up by the party where the trustee of the trust or person holding an equivalent position in a similar legal arrangement enters into a business relationship or acquires real estate in the name of the trust or similar legal arrangement.

Where the trustees of a trust or persons holding equivalent positions in a similar legal arrangement are established or reside in the territories of different Parties, or where the trustee of the trust or person holding an equivalent position in a similar legal arrangement enters into multiple business relationships in the name of the trust or similar legal arrangement in the territory of the two Parties, a certificate of proof of registration or an excerpt of the beneficial ownership information held in a register of on party may be considered as sufficient to consider the registration obligation fulfilled.

5. The Parties shall ensure that the information on the beneficial ownership of a trust or a similar legal arrangement is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities, within the framework of customer due diligence in accordance with their domestic anti-money laundering and counter-terrorism financing framework;

(c) any natural or legal person that can demonstrate a legitimate interest;

(d) any natural or legal person that files a written request in relation to a trust or similar legal arrangement which holds or owns a controlling interest in any corporate or other legal entity other than those referred to in Article LAW.AML.130 [Beneficial Ownership Transparency for corporate and other legal entities], through direct or indirect ownership, including through bearer shareholdings, or through control via other means.

The information accessible to natural or legal persons referred to in points (c) and (d) of the first subparagraph shall consist of the name, the month and year of birth and the country of residence and nationality of the beneficial owner, as well as nature and extent of beneficial interest held.

The Parties may, under conditions to be determined in their domestic law, provide for access of additional information enabling the identification of the beneficial owner. That additional information shall include at least the date of birth or contact details, in accordance with data protection rules. The Parties may allow for wider access to the information held in the register in accordance with their domestic law.

Competent authorities granted access to the central register referred to in paragraph 3a shall be public authorities with designated responsibilities for combating money laundering or terrorist financing, as well as tax authorities, supervisors of obliged entities and authorities that have the

function of investigating or prosecuting money laundering, associated predicate offences and terrorist financing, tracing, and seizing or freezing and confiscating criminal assets.

6. The Parties may choose to make the information held in their domestic registers referred to in paragraph 3a available on the condition of online registration and the payment of a fee, which shall not exceed the administrative costs of making the information available, including costs of maintenance and developments of the register.

7. The Parties shall require that the information held in the central register referred to in paragraph 4 is adequate, accurate and current, and shall put in place mechanisms to this effect. Such mechanisms shall include requiring obliged entities and, if appropriate and to the extent that this requirement does not interfere unnecessarily with their functions, competent authorities to report any discrepancies they find between the beneficial ownership information available in the central registers and the beneficial ownership information available to them. In the case of reported discrepancies the Parties shall ensure that appropriate actions be taken to resolve the discrepancies in a timely manner and, if appropriate, a specific mention be included in the central register in the meantime.

8. The Parties shall ensure that obliged entities do not rely exclusively on the central register referred to in paragraph 4 to fulfil their customer due diligence requirements as laid down in their domestic anti-money laundering and counter-terrorism financing framework. Those requirements shall be fulfilled by using a risk-based approach.

9. The Parties shall ensure that competent authorities and FIUs are able to provide the information referred to in paragraphs 1 and 3 to the competent authorities and to the FIUs of the other party in a timely manner and free of charge.

10. In exceptional circumstances to be laid down in domestic law, where the access referred to in points (b), (c) and (d) of the first subparagraph of paragraph 5 would expose the beneficial owner to disproportionate risk, risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, or where the beneficial owner is a minor or otherwise legally incapable, the Parties may provide for an exemption from such access to all or part of the information on the beneficial ownership on a case-by-case basis. The Parties shall ensure that these exemptions are granted upon a detailed evaluation of the exceptional nature of the circumstances. Rights to an administrative review of the exemption decision and to an effective judicial remedy shall be guaranteed. A party that has granted exemptions shall publish annual statistical data on the number of exemptions granted and reasons stated.

Exemptions granted pursuant to the first subparagraph shall not apply to the credit institutions and financial institutions, and to notaries and other independent legal professionals that are public officials, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts; (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures.

Where a Member State decides to establish an exemption in accordance with the first subparagraph, it shall not restrict access to information by competent authorities and FIUs.

Article LAW.AML.132: Business relationships and customer due diligence

1. The Parties shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction. Whenever entering into a new business relationship with a corporate or other legal entity, or a trust or a legal arrangement having a structure or functions similar to trusts ('similar legal arrangement') which are subject to the registration of beneficial ownership information pursuant to Article LAW.AML.130 [Beneficial Ownership Transparency for corporate and other legal entities] or Article LAW.AML.131 [Beneficial Ownership Transparency for trusts and other types of legal arrangements], the obliged entities shall collect proof of registration or an excerpt of the register.

2. By way of derogation from paragraph 1, the Parties may allow verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact.

3. By way of derogation from paragraph 1, the Parties may allow the opening of an account with a credit institution or financial institution, including accounts that permit transactions in transferable securities, provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the customer due diligence requirements laid down in their domestic Anti-Money Laundering and Counter Terrorism framework is obtained.

4. The Parties shall require that obliged entities apply the customer due diligence measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, or when the relevant circumstances of a customer change, or when the obliged entity has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s), or if the obliged entity has had this duty under Article 2.26bis (1)(a)[Taxation standards]

5. For life or other investment-related insurance business, the Parties shall ensure that, in addition to the customer due diligence measures required for the customer and the beneficial owner, credit institutions and financial institutions conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

(a) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, taking the name of the person;

(b) in the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the credit institutions or financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

With regard to points (a) and (b) of the first subparagraph, the verification of the identity of the beneficiaries shall take place at the time of the payout. In the case of assignment, in whole or in part, of the life or other investment-related insurance to a third party, credit institutions and financial institutions aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

6. In the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, an obliged entity shall obtain sufficient information concerning the beneficiary to satisfy the obliged entity that it will be able to establish the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

Article LAW.AML.133: Obliged entities

In addition to the obliged entities that are covered under the Parties' respective laws implementing the FATF standards, the Parties shall ensure that persons storing, trading or acting as intermediaries in the trade of works of art [high-value goods] when this is carried out by free ports or free trade zones as well as persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to €10,000 or more are considered obliged entities under their Anti-Money Laundering and Counter-Terrorism frameworks.

Chapter eleven: Other provisions

Article LAW.OTHER.134: Notifications

1. When notifying each other that they have completed their respective internal requirements and procedures for establishing their consent to be bound in accordance with Article FINPROV.10 [Entry into force], the Union and the United Kingdom shall make any of the notifications or declarations provided for in Article LAW.SURR.84 [Determination of the competent judicial authorities](3), Article LAW.SURR.84 [Determination of the competent judicial authorities](2) of this Agreement and may make any of the notifications or declarations provided for in Article LAW.SURR.78 [Scope] (4), Article LAW.SURR.81 [Political offence exception](2), Article LAW.SURR.82 [Nationality exception](2), Article LAW.SURR.85 [Recourse to the central authority](1), Article LAW.SURR.86 [Content and form of the arrest warrant](2), Article LAW.SURR.92 [Consent to surrender](4), Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant] (5), Article LAW.SURR.106 [Possible prosecution for other offences](1), Article LAW.SURR.107 [Surrender or subsequent extradition](1) of this Agreement. The declarations or notifications referred to in Article LAW.SURR.78 [Scope] (4), Article LAW.SURR.85 [Recourse to the central authority](1) and Article LAW.SURR.86 [Content and form of the arrest warrant](2) may be made at any time. The declarations or notifications referred to in Article LAW.SURR.84 [Determination of the competent judicial authorities](3) and Article LAW.SURR.54 [Transit] (2) may be modified, and those referred to in Article LAW.SURR.81 [Political offence exception] (2), Article LAW.SURR.82 [Nationality exception](2), Article LAW.SURR.85 [Recourse to the central authority](1), Article LAW.SURR.92 [Consent to surrender] (4), Article LAW.SURR.96 [Time limits and procedures for the decision to execute the arrest warrant](5), withdrawn, at all times. Where the Union makes declarations or notifications referred to in the first subparagraph, it shall indicate for which of its Member States the declaration applies.

2. When depositing its instrument of ratification referred to in Article FINPROV.10 [Entry into force], the United Kingdom shall notify the Union of the identity of the following authorities:

(a) the United Kingdom Competent Authority referred to in [PLACEHOLDER]; and,

(b) the independent public authorities as referred to in [PLACEHOLDER].

(c) the independent administrative body as referred to in [PLACEHOLDER].

The United Kingdom shall notify without delay any changes thereto.

The Union shall publish information referred to in this paragraph in the Official Journal of the European Union.

Article LAW.OTHER.135: Review and evaluation

1. The Parties shall jointly review the implementation of:

(a) Chapters Two, Six and Seven, no later than five years after the date of entry into force of this Agreement; and additionally if requested by either Party and jointly decided.

(b) Chapters Three, Four and Five one year after the date of entry into force of this Agreement, at regular intervals thereafter, and additionally if requested by either Party and jointly decided.

2. The Parties shall decide in advance on the modalities of the review and shall communicate to each other the composition of their respective teams. The teams shall include persons with appropriate expertise with respect to the issues under review. Subject to applicable laws, any participants in a review shall be required to respect the confidentiality of the discussions and to have appropriate security clearances. For the purposes of any review, the United Kingdom and the Union shall ensure access to relevant documentation, systems and personnel.

3. Without prejudice to paragraph 2, the review shall in particular address the practical implementation, interpretation and development of those Chapters and may also include issues such as the consequences of further development of the Union relating to the subject matter of those Chapters.

Article LAW.OTHER.136: Suspension and disapplication

1. The cooperation under this Title shall be conditional upon the United Kingdom's continued adherence to the European Convention on Human Rights and Protocols 1, 6 and 13 thereto, as well as upon the United Kingdom giving continued effect to these instruments under its domestic law.

2. Therefore, in the event that the United Kingdom abrogates the domestic law giving effect to the instruments referred to in paragraph 1 or makes amendments thereto to the effect of reducing the extent to which individuals can rely on them before domestic courts of the United Kingdom, this Title shall be suspended from the date such abrogation or amendment becomes effective. Suspension shall be terminated on the date the United Kingdom domestic law giving effect to the the said instruments again becomes effective.

3. Notwithstanding [Article on termination of the agreement], in the event that the United Kingdom denounces any of the instruments referred to in paragraph 1, this Title shall be disapplied from the date that such denunciation becomes effective.

4. Notwithstanding any suspension or disapplication of this Title, the Parties shall continue to apply the provisions of this Title to all [personal] data obtained before such suspension or disapplication and falling within the scope of this Title.

5. In case the Decision taken in accordance with Article 45 of the General Data Protection Regulation (EU) 2016/679 is either repealed or suspended by the Commission or declared invalid by the Court of Justice of the EU, the provisions of Chapter s three and ten shall be suspended.

6. In case the Decision taken in accordance with Article 36 of Directive (EU) 2016/680 is either repealed or suspended by the Commission or declared invalid by the Court of Justice of the EU, all provisions of this Title shall be suspended.

7. In case of disapplication, the Parties shall reach agreement on the continued use and storage of the information that has already been communicated between them pursuant to Chapters Four and Five. If no agreement is reached, either of the two Parties is entitled to require that the information which it has communicated be destroyed or returned to the transferring Party.

8. In case the Union considers it necessary to amend Chapter 2, because Union legislation relating to the subject matter governed by that Chapter is amended, or is in the process of being amended substantially, it may notify the United Kingdom accordingly with a view to agreeing on a formal amendment of this Agreement in relation to that Chapter. Where within [X months] of that notification the Parties have not concluded an agreement amending Chapter 2, the Union may decide to suspend the application of Chapter 2 for a period of up to [X months]. Before the end of that period, the Parties may agree on an extension of the suspension for an additional period of up to [X months]. If by the end of the suspension period the Parties have not concluded the agreement amending Chapter 2, its provisions shall cease to apply [specify the relevant point in time] unless the Union informs the United Kingdom that it no longer seeks any amendment to Chapter 2. In that case the provisions of Chapter 2 shall be reinstated.

Article LAW.OTHER.137: Expenses

The Parties shall bear their own expenses, which arise in the course of implementation of this Title, unless otherwise stipulated in this Title.

ANNEX LAW-1

TABLE OF CONTENTS

2.1. Overview
2.2. Security features related to message exchange
2.3. Security features not related to message exchange
3. Technical conditions of the data exchange
3.1. General description of the Eucaris application
3.2. Functional and non-functional requirements
CHAPTER 4: Evaluation procedure according to Article LAW.PRUM.17
1. Questionnaire
2. Pilot run
3. Evaluation visit
4. Report to the Council

CHAPTER 0: GENERAL PROVISIONS

Article 1: Aim

The aim of this Annex is to lay down the necessary data protection, administrative and technical provisions for the implementation of Articles LAW.PRUM.5 to LAW.PRUM.17.

Article 2: Technical specifications

States shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopic data and vehicle registration data. These technical specifications are laid down in Chapters 1 to 3 of this Annex.

Article 3: Communications network

The electronic exchange of DNA data, dactyloscopic data and vehicle registration data between States shall take place using the Trans European Services for Telematics between Administrations (TESTA II) communications network and further developments thereof.

Article 4: Availability of automated data exchange

States shall take all necessary measures to ensure that automated searching or comparison of DNA data, dactyloscopic data and vehicle registration data is possible 24 hours a day and seven days a week. In the event of a technical fault, the States' national contact points shall immediately inform each other and shall agree on temporary alternative information exchange arrangements in accordance with the legal provisions applicable. Automated data exchange shall be re-established as quickly as possible.

Article 5: Reference numbers for DNA data and dactyloscopic data

The reference numbers referred to in Articles LAW.PRUM.7 and LAW.PRUM.11 shall consist of a combination of the following:

(a) a code allowing the States, in the case of a match, to retrieve personal data and other information in their databases in order to supply it to one, several or all of the States in accordance with Article LAW.PRUM.14

(b) a code to indicate the national origin of the DNA profile or dactyloscopic data; and

(c) with respect to DNA data, a code to indicate the type of DNA profile.

Article 6: Principles of DNA data exchange

1. States shall use existing standards for DNA data exchange, such as the European Standard Set (ESS) or the Interpol Standard Set of Loci (ISSOL).

2. The transmission procedure, in the case of automated searching and comparison of DNA profiles, shall take place within a decentralised structure.

3. Appropriate measures shall be taken to ensure confidentiality and integrity for data being sent to other States, including their encryption.

4. States shall take the necessary measures to guarantee the integrity of the DNA profiles made available or sent for comparison to the other States and to ensure that these measures comply with international standards such as ISO 17025.

5. States shall use State codes in accordance with the ISO 3166-1 alpha-2 standard.

Article 7: Rules for requests and answers in connection with DNA data

1. A request for an automated search or comparison, as referred to in Article LAW.PRUM.8 or LAW.PRUM.9, shall include only the following information:

(a) the State code of the requesting State;

(b) the date, time and indication number of the request;

(c) DNA profiles and their reference numbers;

(d) the types of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles); and

(e) information required for controlling the database systems and quality control for the automatic search processes.

2. The answer (matching report) to the request referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches (hits) or no matches (no hits);

(b) the date, time and indication number of the request;

(c) the date, time and indication number of the answer;

(d) the State codes of the requesting and requested States;

(e) the reference numbers of the requesting and requested States;

(f) the type of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles);

(g) the requested and matching DNA profiles; and

(h) information required for controlling the database systems and quality control for the automatic search processes.

3. Automated notification of a match shall only be provided if the automated search or comparison has resulted in a match of a minimum number of loci. This minimum is set out in Chapter 1 of this Annex.

4. The States shall ensure that requests comply with declarations issued pursuant to Article LAW.PRUM7(3).

Article 8: Transmission procedure for automated searching of unidentified DNA profiles in accordance with Article LAW.PRUM.8

1. If, in a search with an unidentified DNA profile, no match has been found in the national database or a match has been found with an unidentified DNA profile, the unidentified DNA profile may then be transmitted to all other States' databases and if, in a search with this unidentified DNA profile, matches are found with reference DNA profiles and/or unidentified DNA profiles in other States' databases, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting State; if no matches can be found in other States' databases, this shall be automatically communicated to the requesting State.

2. If, in a search with an unidentified DNA profile, a match is found in other States' databases, each State concerned may insert a note to this effect in its national database.

Article 9: Transmission procedure for automated search of reference DNA profiles in accordance with Article LAW.PRUM.8

If, in a search with a reference DNA profile, no match has been found in the national database with a reference DNA profile or a match has been found with an unidentified DNA profile, this reference DNA profile may then be transmitted to all other States' databases and if, in a search with this reference DNA profile, matches are found with reference DNA profiles and/or unidentified DNA profiles in other States' databases, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting State; if no matches can be found in other States' databases, it shall be automatically communicated to the requesting State.

Article 10: Transmission procedure for automated comparison of unidentified DNA profiles in accordance with Article LAW.PRUM.9

1. If, in a comparison with unidentified DNA profiles, matches are found in other States' databases with reference DNA profiles and/or unidentified DNA profiles, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting State.

2. If, in a comparison with unidentified DNA profiles, matches are found in other States' databases with unidentified DNA profiles or reference DNA profiles, each State concerned may insert a note to this effect in its national database.

Article 11: Principles for the exchange of dactyloscopic data

1. The digitalisation of dactyloscopic data and their transmission to the other States shall be carried out in accordance with the uniform data format specified in Chapter 2 of this Annex.

2. Each State shall ensure that the dactyloscopic data it transmits are of sufficient quality for a comparison by the automated fingerprint identification systems (AFIS).

3. The transmission procedure for the exchange of dactyloscopic data shall take place within a decentralised structure.

4. Appropriate measures shall be taken to ensure the confidentiality and integrity of dactyloscopic data being sent to other States, including their encryption.

5. The States shall use State codes in accordance with the ISO 3166-1 alpha-2 standard.

Article 12: Search capacities for dactyloscopic data

1. Each State shall ensure that its search requests do not exceed the search capacities specified by the requested State. The United Kingdom shall declare their maximum search capacities per day for dactyloscopic data of identified persons and for dactyloscopic data of persons not yet identified.

2. The maximum numbers of candidates accepted for verification per transmission are set out in Chapter 2 of this Annex.

Article 13: Rules for requests and answers in connection with dactyloscopic data

1. The requested State shall check the quality of the transmitted dactyloscopic data without delay by a fully automated procedure. Should the data be unsuitable for an automated comparison, the requested State shall inform the requesting State without delay.

2. The requested State shall conduct searches in the order in which requests are received. Requests shall be processed within 24 hours by a fully automated procedure. The requesting State may, if its national law so prescribes, ask for accelerated processing of its requests and the requested State shall conduct these searches without delay. If deadlines cannot be met for reasons of *force majeure*, the comparison shall be carried out without delay as soon as the impediments have been removed.

Article 14: Principles of automated searching of vehicle registration data

1. For automated searching of vehicle registration data States shall use a version of the European Vehicle and Driving Licence Information System (Eucaris) software application especially designed for the purposes of Article LAW.PRUM.15, and amended versions of this software.

2. Automated searching of vehicle registration data shall take place within a decentralised structure.

3. The information exchanged via the Eucaris system shall be transmitted in encrypted form.

4. The data elements of the vehicle registration data to be exchanged are specified in Chapter 3 of the Annex.

5. In the implementation of Article LAW.PRUM.15, States may give priority to searches related to combating serious crime.

Article 15: Costs

Each State shall bear the costs arising from the administration, use and maintenance of the Eucaris software application referred to in Article 14(1).

Article 16: Purpose

1. Processing of personal data by the receiving State shall be permitted solely for the purposes for which the data have been supplied in accordance with Articles LAW.PRUM 5-17. Processing for

other purposes shall be permitted solely with the prior authorisation of the State administering the file and subject only to the national law of the receiving State. Such authorisation may be granted provided that processing for such other purposes is permitted under the national law of the State administering the file.

2. Processing of data supplied pursuant to Articles LAW.PRUM 8, 9 and 12 by the searching or comparing State shall be permitted solely in order to:

(a) establish whether the compared DNA profiles or dactyloscopic data match;

(b) prepare and submit a police or judicial request for legal assistance in compliance with national law if those data match;

(c) record within the meaning of Article 19 of this Chapter.

3. The State administering the file may process the data supplied to it in accordance with Articles LAW.PRUM 8, 9 and 12 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 19 of this Chapter. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the paragraph 2.

4. Data supplied in accordance with Article.LAW.PRUM.15 may be used by the State administering the file solely where this is necessary for the purpose of providing automated replies to search procedures or recording as specified in Article 19 of this Chapter. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 19 of this Chapter. The Member State may use data received in a reply solely for the procedure for which the search was made.

Article 17: Accuracy, current relevance and storage time of data

1. The States shall ensure the accuracy and current relevance of personal data. Should it transpire ex officio or from a notification by the data subject, that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to the receiving State(s). The State(s) concerned shall be obliged to correct or delete the data. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the receiving body has reason to believe that the supplied data are incorrect or should be deleted the supplying body shall be informed forthwith.

2. Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established shall, in accordance with the national law of the States, be marked with a flag at the request of the data subject. If a flag exists, this may be removed subject to the national law of the States and only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

3. Personal data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) if they are not or no longer necessary for the purpose for which they were supplied; if personal data have been supplied without request, the receiving body shall immediately check if they are necessary for the purposes for which they were supplied;

(b) following the expiry of the maximum period for keeping data laid down in the national law of the supplying State where the supplying body informed the receiving body of that maximum period at the time of supplying the data.

4. Where there is reason to believe that deletion would prejudice the interests of the data subject, the data shall be blocked instead of being deleted in compliance with national law. Blocked data may be supplied or used solely for the purpose which prevented their deletion.

Article 18: Technical and organisational measures to ensure data protection and data security

1. The supplying and receiving bodies shall take steps to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure.

2. The features of the technical specification of the automated search procedure are regulated in the implementing measures as referred to in Article LAW.PRUM.16 which guarantee that:

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;

(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to generally accessible networks; and

(c) the admissibility of searches in accordance with Article 19, paragraph (2), (5) and (6) can be checked.

Article 19: Logging and recording: special rules governing automated and non-automated supply

1. Each State shall guarantee that every non-automated supply and every non-automated receipt of personal data by the body administering the file and by the searching body is logged in order to verify the admissibility of the supply. Logging shall contain the following information:

(a) the reason for the supply;

(b) the data supplied;

(c) the date of the supply; and

(d) the name or reference code of the searching body and of the body administering the file.

2. The following shall apply to automated searches for data based on Articles LAW.PRUM. 8, 12 and 15 and to automated comparison pursuant to Article LAW.PRUM.9:

(a) only specially authorised officers of the national contact points may carry out automated searches or comparisons. The list of officers authorised to carry out automated searches or

comparisons shall be made available upon request to the supervisory authorities referred to in paragraph 6 and to the other States;

(b) each State shall ensure that each supply and receipt of personal data by the body administering the file and the searching body is recorded, including notification of whether or not a hit exists. Recording shall include the following information:

(i) the data supplied;

(ii) the date and exact time of the supply; and

(iii) the name or reference code of the searching body and of the body administering the file.

3. The searching body shall also record the reason for the search or supply as well as an identifier for the official who carried out the search and the official who ordered the search or supply.

4. The recording body shall immediately communicate the recorded data upon request to the competent data protection authorities of the relevant State at the latest within four weeks following receipt of the request. Recorded data may be used solely for the following purposes:

(a) monitoring data protection;

(b) ensuring data security.

5. The recorded data shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall be deleted immediately.

6. Responsibility for legal checks on the supply or receipt of personal data lies with the independent data protection authorities or, as appropriate, the judicial authorities of the respective States. Anyone can request these authorities to check the lawfulness of the processing of data in respect of their person in compliance with national law. Independently of such requests, these authorities and the bodies responsible for recording shall carry out random checks on the lawfulness of supply, based on the files involved.

7. The results of such checks shall be kept for inspection for 18 months by the independent data protection authorities. After this period, they shall be immediately deleted. Each data protection authority may be requested by the independent data protection authority of another State to exercise its powers in accordance with national law. The independent data protection authorities of the States shall perform the inspection tasks necessary for mutual cooperation, in particular by exchanging relevant information.

Article 20: Data subjects' rights to damages

Where a body of one State has supplied personal data under this Decision, the receiving body of the other State cannot use the inaccuracy of the data supplied as grounds to evade its liability vis-à-vis the injured party under national law. If damages are awarded against the receiving body because of

its use of inaccurate transfer data, the body which supplied the data shall refund the amount paid in damages to the receiving body in full.

Article 21: Information requested by the States

The receiving State shall inform the supplying State on request of the processing of supplied data and the result obtained.

Article 22: Declarations

1. The United Kingdom shall communicate its declarations pursuant to Articles LAW.PRUM 7(3), LAW.PRUM 13(1), LAW.PRUM 15(2) and article 12(1) of this Annex to the Specialised Committee on Law Enforcement and Judicial Cooperation.

2. Factual information provided by the United Kingdom through these declarations, and by Member States in accordance with Article LAW.PRUM 16(3), are included in the Manual as established in Article 18 (2) of Decision 2008/616/JHA.

3. States may amend declarations submitted in accordance with paragraph 1 at any time by means of a declaration submitted to the Specialised Committee on Law Enforcement and Judicial Cooperation. The Specialised Committee on Law Enforcement and Judicial Cooperation shall forward any declarations received to the General Secretariat of the Council.

4. The General Secretariat of the Council shall communicate any changes in the Manual referred to in paragraph 2 to the Specialised Committee on Law Enforcement and Judicial Cooperation.

Article 23: Preparation of decisions as referred to in Article LAW.PRUM.17

1. The Council shall take a decision as referred to in Article LAW.PRUM.17 on the basis of an evaluation report which shall be based on a questionnaire.

2. With respect to the automated data exchange in accordance with Articles LAW.PRUM.5 to LAW.PRUM.17, the evaluation report shall also be based on an evaluation visit and a pilot run that shall be carried out when the United Kingdom has informed the Specialised Committee on Law Enforcement and Judicial Cooperation that they have implemented the obligations imposed on them under Articles LAW.PRUM 5 to LAW.PRUM.17 and submit the declarations foreseen in Article 22 Further details of the procedure are set out in Chapter 4 of this Annex.

Article 24: Statistics and reporting

1. An evaluation of the administrative, technical and financial application of the data exchange pursuant to Articles LAW.PRUM 5 to LAW.PRUM.17 shall be carried out on a regular basis. The evaluation shall be carried out with respect to the data categories for which data exchange has started among the States concerned. The evaluation shall be based on reports of the respective States.

2. Each State will compile statistics on the results of the automated data exchange. In order to ensure comparability, the model for statistics will be compiled by the relevant Council Working

Group. These statistics will be forwarded annually to the Specialised Committee on Law Enforcement and Judicial Cooperation.

3. In addition, States will be requested on a regular basis not to exceed once per year to provide further information on the administrative, technical and financial implementation of automated data exchange as needed to analyse and improve the process.

4. Statistics and reporting made by Member States in accordance with Council Decisions 2008/615/JHA and 2008/616/JHA shall apply in relation to this Article.

CHAPTER 1: EXCHANGE OF DNA-DATA

1. DNA related forensic issues, matching rules and algorithms

1.1. Properties of DNA-profiles

The DNA profile may contain 24 pairs of numbers representing the alleles of 24 loci which are also used in the DNA-procedures of Interpol. The names of these loci are shown in the following table:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

The seven grey loci in the top row are both the present European Standard Set (ESS) and the Interpol Standard Set of Loci (ISSOL).

Inclusion Rules:

The DNA-profiles made available by the States for searching and comparison as well as the DNA-profiles sent out for searching and comparison must contain at least six full designated[1] loci and may contain additional loci or blanks depending on their availability. The reference DNA profiles must contain at least six of the seven ESS of loci. In order to raise the accuracy of matches, all available alleles shall be stored in the indexed DNA profile database and be used for searching and comparison. Each State should implement as soon as practically possible any new ESS of loci adopted by the EU.

Mixed profiles are not allowed, so that the allele values of each locus will consist of only two numbers, which may be the same in the case of homozygosity at a given locus.

Wild-cards and Micro-variants are to be dealt with using the following rules:

– Any non-numerical value except amelogenin contained in the profile (e.g. ‘o’, ‘f’, ‘r’, ‘na’, ‘nr’ or ‘un’) has to be automatically converted for the export to a wild card (*) and searched against all,

[1] ‘Full designated’ means the handling of rare allelle values is included.

- Numerical values ‘0’, ‘1’ or ‘99’ contained in the profile have to be automatically converted for the export to a wild card (*) and searched against all,

- If three alleles are provided for one locus the first allele will be accepted and the remaining two alleles have to be automatically converted for the export to a wild card (*) and searched against all,

- When wild card values are provided for allele 1 or 2 then both permutations of the numerical value given for the locus will be searched (e.g. 12, * could match against 12,14 or 9,12),

- Pentanucleotide (Penta D, Penta E and CD4) micro-variants will be matched according to the following:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x.4

  x.4 = x.3, x.4, x + 1,

- Tetranucleotide (the rest of the loci are tetranucleotides) micro-variants will be matched according to the following:

  x.1 = x, x.1, x.2

  x.2 = x.1, x.2, x.3

  x.3 = x.2, x.3, x + 1.

1.2. Matching rules

The comparison of two DNA-profiles will be performed on the basis of the loci for which a pair of allele values is available in both DNA-profiles. At least six full designated loci (exclusive of amelogenin) must match between both DNA-profiles before a hit response is provided.

A full match (Quality 1) is defined as a match, when all allele values of the compared loci commonly contained in the requesting and requested DNA-profiles are the same. A near match is defined as a match, when the value of only one of all the compared alleles is different in the two DNA profiles (Quality 2, 3 and 4). A near match is only accepted if there are at least six full designated matched loci in the two compared DNA profiles.

The reason for a near match may be:

- a human typing error at the point of entry of one of the DNA-profiles in the search request or the DNA-database,

- an allele-determination or allele-calling error during the generation procedure of the DNA-profile.

1.3. Reporting rules

Both full matches, near matches and 'no hits' will be reported.

The matching report will be sent to the requesting national contact point and will also be made available to the requested national contact point (to enable it to estimate the nature and number of possible follow-up requests for further available personal data and other information associated with the DNA-profile corresponding to the hit in accordance with Articles LAW.PRUM.14).

2. State code number table

In accordance with Article LAW.PRUM.6 to LAW.PRUM.10, ISO 3166-1 alpha-2 code are used for setting up the domain names and other configuration parameters required in the Prüm DNA data exchange applications over a closed network.

ISO 3166-1 alpha-2 codes are the following two-letter State codes.

State names	Code	State names	Code
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxemburg	LU
Czech Republic	CZ	Hungary	HU
Denmark	DK	Malta	MT
Germany	DE	Netherlands	NL
Estonia	EE	Austria	AT
Ireland	IE	Poland	PL
Greece	EL	Portugal	PT
Spain	ES	Romania	RO
France	FR	Slovakia	SK
Croatia	HR	Slovenia	SI
Italy	IT	Finland	FI
Cyprus	CY	Sweden	SE
Latvia	LV	United Kingdom	UK

3. Functional analysis

3.1. Availability of the system

Requests pursuant to Article LAW.PRUM.8 should reach the targeted database in the chronological order that each request was sent, responses should be dispatched to reach the requesting State within 15 minutes of the arrival of requests.

3.2. Second step

When a State receives a report of match, its national contact point is responsible for comparing the values of the profile submitted as a question and the values of the profile(s) received as an answer to validate and check the evidential value of the profile. National contact points can contact each other directly for validation purposes.

Legal assistance procedures start after validation of an existing match between two profiles, on the basis of a 'full match' or a 'near match' obtained during the automated consultation phase.

4. DNA interface control document

4.1. Introduction

4.1.1. *Objectives*

This Chapter defines the requirements for the exchange of DNA profile information between the DNA database systems of all States. The header fields are defined specifically for the Prüm DNA exchange, the data part is based on the DNA profile data part in the XML schema defined for the Interpol DNA exchange gateway.

Data are exchanged by SMTP (Simple Mail Transfer Protocol) and other state-of-the-art technologies, using a central relay mail server provided by the network provider. The XML file is transported as mail body.

4.1.2. *Scope*

This ICD defines the content of the message (mail) only. All network-specific and mail-specific topics are defined uniformly in order to allow a common technical base for the DNA data exchange.

This includes:

- the format of the subject field in the message to enable/allow for an automated processing of the messages,
- whether content encryption is necessary and if yes which methods should be chosen,
- the maximum length of messages.

4.1.3. *XML structure and principles*

The XML message is structured into;

– header part, which contains information about the transmission, and

– data part, which contains profile specific information, as well as the profile itself.

The same XML schema shall be used for request and response.

For the purpose of complete checks of unidentified DNA profiles (LAW.PRUM.9) it shall be possible to send a batch of profiles in one message. A maximum number of profiles within one message must be defined. The number is depending from the maximum allowed mail size and shall be defined after selection of the mail server.

XML example:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> datas structure repeated, if multiple profiles sent by (….) a single SMTP message, only allowed for Article 4 cases

</datas>]

</PRUEMDNA>

4.2. XML structure definition

The following definitions are for documentation purposes and better readability, the real binding information is provided by an XML schema file (PRUEM DNA.xsd).

4.2.1. *Schema PRUEMDNAx*

It contains the following fields:

Fields	Type	Description
header	PRUEM_header	Occurs: 1

datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. *Content of header structure*

4.2.2.1. PRUEM header

This is a structure describing the XML file header. It contains the following fields:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting State info
requested	PRUEM_header_info	Requested State info

4.2.2.2. PRUEM_header dir

Type of data contained in message, value can be:

Value	Description
R	Request
A	Answer

4.2.2.3. PRUEM header info

Structure to describe State as well as message date/time. It contains the following fields:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting State
destination_isocode	String	ISO 3166-2 code of the requested State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message

time	Time	Time of creation of message

4.2.3. *Content of PRUEM Profile data*

4.2.3.1. PRUEM_datas

This is a structure describing the XML profile data part. It contains the following fields:

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality!=0 (the original requested profile), then empty.

4.2.3.2. PRUEM_request_type

Type of data contained in message, value can be:

Value	Description
3	Requests pursuant to Article LAW.PRUM.8
4	Requests pursuant to Article LAW.PRUM.9

4.2.3.3. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: Case 'No Hit': original requesting profile sent back only; Case 'Hit': original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)
4	Hit with mismatch

4.2.3.4. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Type of data contained in message, value can be:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6. IPSG_DNA_profile

Structure describing a DNA profile. It contains the following fields:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7. IPSG_DNA_ISSOL

Structure containing the loci of ISSOL (Standard Group of Interpol loci). It contains the following fields:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8. IPSG_DNA_additional_loci

Structure containing the other loci. It contains the following fields:

Fields	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317

d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Structure describing a locus. It contains the following fields:

Fields	Type	Description
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. Application, security and communication architecture

5.1. Overview

In implementing applications for the DNA data exchange within the framework of Articles LAW.PRUM.6 to LAW.PRUM.10, a common communication network shall be used, which will be logically closed among the States. In order to exploit this common communication infrastructure of sending requests and receiving replies in a more effective way, an asynchronous mechanism to convey DNA and dactyloscopic data requests in a wrapped SMTP e-mail message is adopted. In fulfilment of security concerns, the mechanism s/MIME as extension to the SMTP functionality will be used to establish a true end-to-end secure tunnel over the network.

The operational TESTA (Trans European Services for Telematics between Administrations) is used as the communication network for data exchange among the States. TESTA is under the responsibility of the European Commission. Taking into account that national DNA databases and the current national access points of TESTA may be located on different sites in the States, access to TESTA may be set up either by:

1. using the existing national access point or establishing a new national TESTA access point; or by

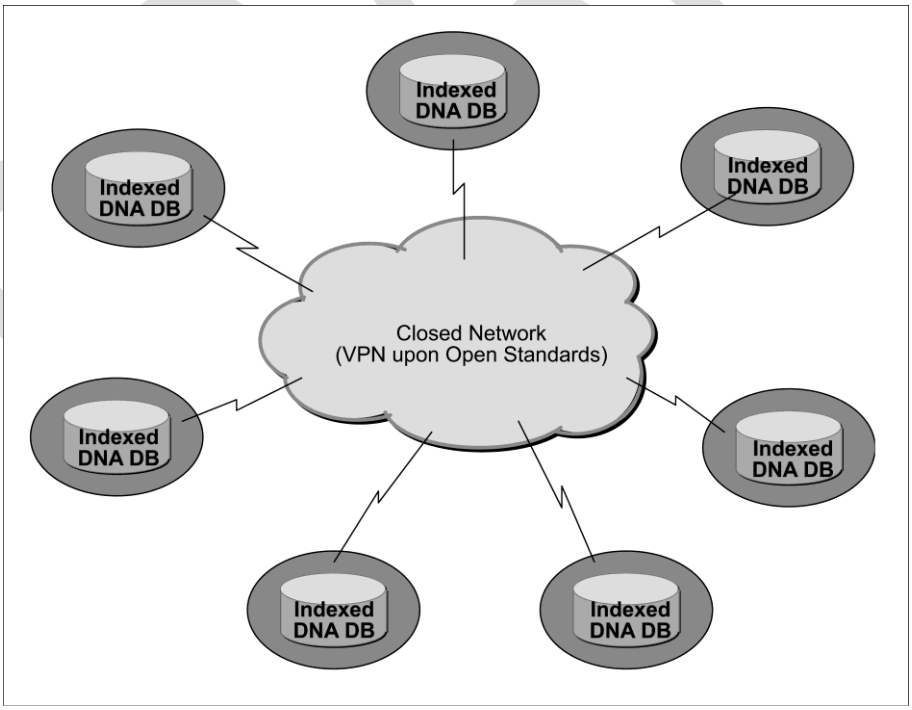
2. setting up a secure local link from the site where the DNA database is located and managed by the competent national agency to the existing national TESTA access point.

The protocols and standards deployed in the implementation of Article LAW.PRUM.6 to LAW.PRUM.10 applications comply with the open standards and meet the requirements imposed by national security policy makers of the States.

5.2. Upper Level Architecture

In the scope of Article LAW.PRUM.6 to LAW.PRUM.10, each State will make its DNA data available to be exchanged with and/or searched by other States in conformity with the standardised common data format. The architecture is based upon an any-to-any communication model. There exists neither a central computer server nor a centralised database to hold DNA profiles.

Figure 1: Topology of DNA Data Exchange



In addition to the fulfilment of national legal constraints at States' sites, each State may decide what kind of hardware and software should be deployed for the configuration at its site to comply with the requirements set out in Article LAW.PRUM.6 to LAW.PRUM.10.

5.3. Security Standards and Data Protection

Three levels of security concerns have been considered and implemented.

5.3.1. *Data Level*

DNA profile data provided by each State have to be prepared in compliance with a common data protection standard, so that requesting States will receive an answer mainly to indicate HIT or NO-HIT along with an identification number in case of a HIT, which does not contain any personal information. The further investigation after the notification of a HIT will be conducted at bilateral level pursuant to the existing national legal and organisational regulations of the respective States' sites.

5.3.2. *Communication Level*

Messages containing DNA profile information (requesting and replying) will be encrypted by means of a state-of-the-art mechanism in conformity with open standards, such as s/MIME, before they are forwarded to the sites of other States.

5.3.3. *Transmission Level*

All encrypted messages containing DNA profile information will be forwarded onto other States' sites through a virtual private tunnelling system administered by a trusted network provider at the international level and the secure links to this tunnelling system under the national responsibility. This virtual private tunnelling system does not have a connection point with the open Internet.

5.4. Protocols and Standards to be used for encryption mechanism: s/MIME and related packages

The open standard s/MIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol s/MIME (V3) allows signed receipts, security labels, and secure mailing lists and is layered on Cryptographic Message Syntax (CMS), an IETF specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data.

The underlying certificate used by s/MIME mechanism has to be in compliance with X.509 standard. In order to ensure common standards and procedures with other Prüm applications, the processing rules for s/MIME encryption operations or to be applied under various COTS (Commercial Product of the Shelves) environments, are as follows:

- the sequence of the operations is: first encryption and then signing,
- the encryption algorithm AES (Advanced Encryption Standard) with 256 bit key length and RSA with 1024 bit key length shall be applied for symmetric and asymmetric encryption respectively,
- the hash algorithm SHA-1 shall be applied.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Because of s/MIME's easy integration into national IT infrastructure at all States' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal 'Proof of Concept' in a more efficient way and reducing costs the open standard JavaMail API is however chosen for prototyping DNA data exchange. JavaMail API provides simple encryption and decryption of e-mails using s/MIME and/or OpenPGP. The intent is to provide a single, easy-to-use API for e-mail clients that want to send and received encrypted e-mail in either of the two most popular e-mail encryption formats. Therefore any state-of-the-art implementations to JavaMail API will suffice for the requirements set by Article LAW.PRUM.6 to LAW.PRUM.10, such as the product of Bouncy Castle JCE (Java Cryptographic Extension), which will be used to implement s/MIME for prototyping DNA data exchange among all States.

5.5. Application Architecture

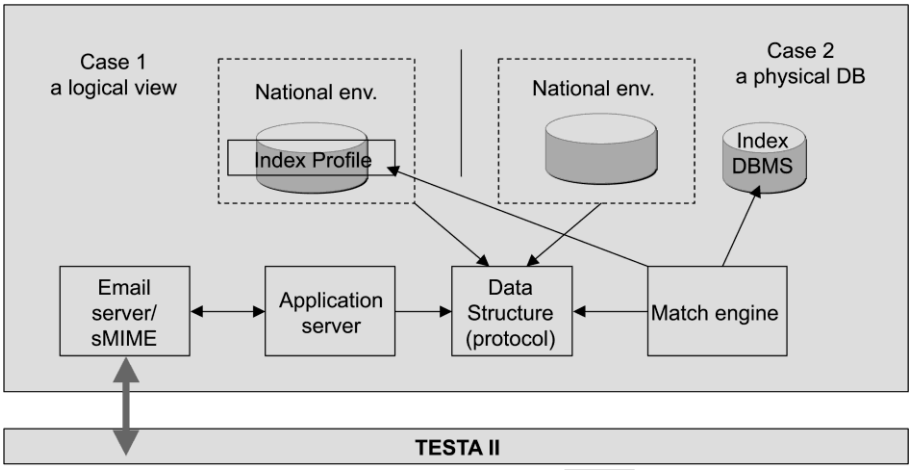
Each State will provide the other States with a set of standardised DNA profile data which are in conformity with the current common ICD. This can be done either by providing a logical view over individual national database or by establishing a physical exported database (indexed database).

The four main components: E-mail server/s/MIME, Application Server, Data Structure Area for fetching/feeding data and registering incoming/outgoing messages, and Match Engine implement the whole application logic in a product-independent way.

In order to provide all States with an easy integration of the components into their respective national sites, the specified common functionality has been implemented by means of open source components, which could be selected by each State depending on its national IT policy and regulations. Because of the independent features to be implemented to get access to indexed databases containing DNA profiles covered by Article LAW.PRUM.6 to LAW.PRUM.10, each State can freely select its hardware and software platform, including database and operating systems.

A prototype for the DNA Data Exchange has been developed and successfully tested over the existing common network. The version 1.0 has been deployed in the productive environment and is used for daily operations. States may use the jointly developed product but may also develop their own products. The common product components will be maintained, customised and further developed according to changing IT, forensic and/or functional police requirements.

Figure 2: Overview Application Topology



5.6. Protocols and Standards to be used for application architecture:

5.6.1. *XML*

The DNA data exchange will fully exploit XML-schema as attachment to SMTP e-mail messages. The eXtensible Markup Language (XML) is a W3C-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. The description of the DNA profile suitable for exchange among all States has been done by means of XML and XML schema in the ICD document.

5.6.2. *ODBC*

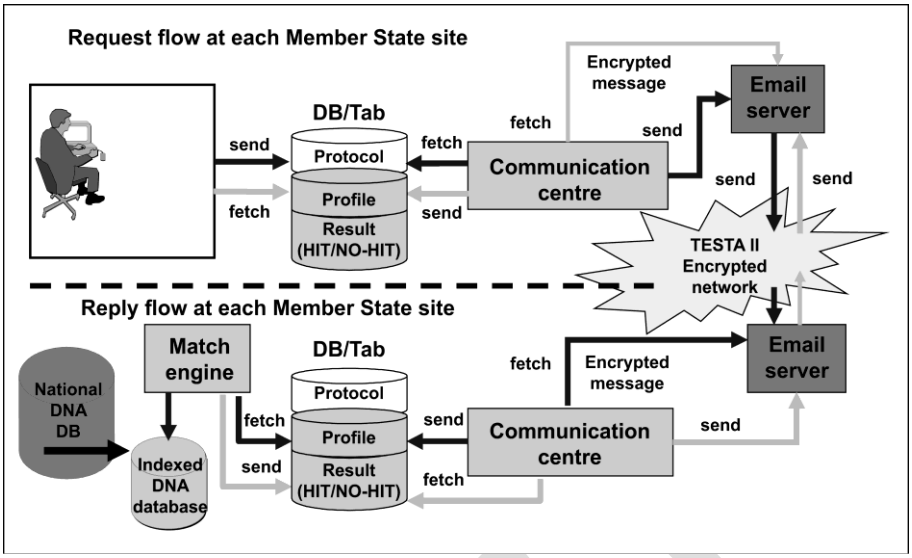
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has, however, certain drawbacks. Administering a large number of client machines can involve a diversity of drivers and DLLs. This complexity can increase system administration overhead.

5.6.3. *JDBC*

Java DataBase Connectivity (JDBC) is an API for the Java programming language that defines how a client may access a database. In contrast to ODBC, JDBC does not require to use a certain set of local DLLs at the Desktop.

The business logic to process DNA profile requests and replies at each States' site is described in the following diagram. Both requesting and replying flows interact with a neutral data area comprising different data pools with a common data structure.

Figure 3: Overview Application Workflow at each State's site



5.7. Communication Environment

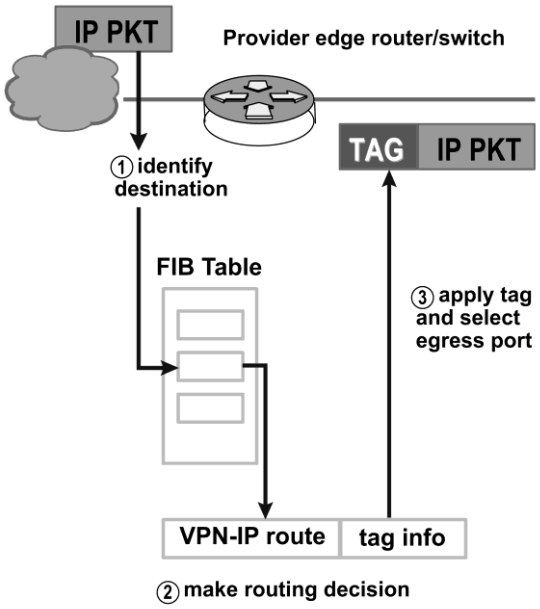
5.7.1. *Common Communication Network: TESTA and its follow-up infrastructure*

The application DNA data exchange will exploit the e-mail, an asynchronous mechanism, to send requests and to receive replies among the States. As all States have at least one national access point to the TESTA network, the DNA data exchange will be deployed over the TESTA network. TESTA provides a number of added-value services through its e-mail relay. In addition to hosting TESTA specific e-mail boxes, the infrastructure can implement mail distribution lists and routing policies. This allows TESTA to be used as a clearing house for messages addressed to administrations connected to the EU wide Domains. Virus check mechanisms may also be put in place.

The TESTA e-mail relay is built on a high availability hardware platform located at the central TESTA application facilities and protected by firewall. The TESTA Domain Name Services (DNS) will resolve resource locators to IP addresses and hide addressing issues from the user and from applications.

5.7.2. *Security Concern*

The concept of a VPN (Virtual Private Network) has been implemented within the framework of TESTA. Tag Switching Technology used to build this VPN will evolve to support Multi-Protocol Label Switching (MPLS) standard developed by the Internet Engineering Task Force (IETF).



MPLS is an IETF standard technology that speeds up network traffic flow by avoiding packet analysis by intermediate routers (hops). This is done on the basis of so-called labels that are attached to packet by the edge routers of the backbone, on the basis of information stored in the forwarding information base (FIB). Labels are also used to implement virtual private networks (VPNs).

MPLS combines the benefits of layer 3 routing with the advantages of layer 2 switching. Because IP addresses are not evaluated during transition through the backbone, MPLS does not impose any IP addressing limitations.

Furthermore e-mail messages over the TESTA will be protected by s/MIME driven encryption mechanism. Without knowing the key and possessing the right certificate, nobody can decrypt messages over the network.

5.7.3. *Protocols and Standards to be used over the communication network*

5.7.3.1. SMTP

Simple Mail Transfer Protocol is the de facto standard for e-mail transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and then the message text is transferred. SMTP uses TCP port 25 upon the specification by the IETF. To determine the SMTP server for a given domain name, the MX (Mail eXchange) DNS (Domain Name Systems) record is used.

Since this protocol started as purely ASCII text-based it did not deal well with binary files. Standards such as MIME were developed to encode binary files for transfer through SMTP. Today, most SMTP servers support the 8BITMIME and s/MIME extension, permitting binary files to be transmitted almost as easily as plain text. The processing rules for s/MIME operations are described in the section s/MIME (see Chapter 5.4).

SMTP is a ‘push’ protocol that does not allow one to ‘pull’ messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Within the framework of implementing DNA data exchange it is decided to use the protocol POP3.

5.7.3.2. POP

Local e-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. By using the SMTP Submit profile of the SMTP protocol, e-mail clients send messages across the Internet or over a corporate network. MIME serves as the standard for attachments and non-ASCII text in e-mail. Although neither POP3 nor SMTP requires MIME-formatted e-mail, essentially Internet e-mail comes MIME-formatted, so POP clients must also understand and use MIME. The whole communication environment of Article LAW.PRUM.6 to LAW.PRUM.10 will therefore include the components of POP.

5.7.4. *Network Address Assignment*

Operative environment

A dedicated block of C class subnet has currently been allocated by the European IP registration authority (RIPE) to TESTA. Further address blocks may be allocated to TESTA in the future if required. The assignment of IP addresses to States is based upon a geographical schema in Europe. The data exchange among States within the framework of Article LAW.PRUM.6 to LAW.PRUM.10 is operated over a European wide logically closed IP network.

Testing Environment

In order to provide a smooth running environment for the daily operation among all connected States, it is necessary to establish a testing environment over the closed network for new States which prepare to join the operations. A sheet of parameters including IP addresses, network settings, e-mail domains as well as application user accounts has been specified and should be set up at the corresponding State's site. Moreover, a set of pseudo DNA profiles has been constructed for the test purposes.

5.7.5. *Configuration Parameters*

A secure e-mail system is set up using the eu-admin.net domain. This domain with the associated addresses will not be accessible from a location not on the TESTA EU wide domain, because the names are only known on the TESTA central DNS server, which is shielded from the Internet.

The mapping of these TESTA site addresses (host names) to their IP addresses is done by the TESTA DNS service. For each Local Domain, a Mail entry will be added to this TESTA central DNS server, relaying all e-mail messages sent to TESTA Local Domains to the TESTA central Mail Relay. This TESTA central Mail Relay will then forward them to the specific Local Domain e-mail server using the Local Domain e-mail addresses. By relaying the e-mail in this way, critical information contained in e-mails will only pass the Europe - wide closed network infrastructure and not the insecure Internet.

It is necessary to establish sub-domains (*bold italics*) at the sites of all States upon the following syntax:

'*application-type.pruem.State-code.*eu-admin.net', where:

'*State-code*' takes the value of one of the two letter-code State codes (i.e. AT, BE, etc.).

'*application-type*' takes one of the values: DNA and FP.

By applying the above syntax, the sub domains for the States are shown in the following table:

State	Sub Domains	Comments
BE	*dna.pruem.be*.eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	fp.pruem.be.eu-admin.net	
BG	*dna.pruem.bg*.eu-admin.net	
	fp.pruem.bg.eu-admin.net	
CZ	*dna.pruem.cz*.eu-admin.net	
	fp.pruem.cz.eu-admin.net	
DK	*dna.pruem.dk*.eu-admin.net	
	fp.pruem.dk.eu-admin.net	
DE	*dna.pruem.de*.eu-admin.net	Using the existing TESTA II national access points
	fp.pruem.de.eu-admin.net	
EE	*dna.pruem.ee*.eu-admin.net	
	fp.pruem.ee.eu-admin.net	
IE	*dna.pruem.ie*.eu-admin.net	
	fp.pruem.ie.eu-admin.net	
EL	*dna.pruem.el*.eu-admin.net	
	fp.pruem.el.eu-admin.net	
ES	*dna.pruem.es*.eu-admin.net	Using the existing TESTA II national access point
	fp.pruem.es.eu-admin.net	
FR	*dna.pruem.fr*.eu-admin.net	Using the existing TESTA II national access point
	fp.pruem.fr.eu-admin.net	

HR	*dna.pruem.hr*.testa.eu	
	fp.pruem.hr.testa.eu	
IT	*dna.pruem.it*.eu-admin.net	
	fp.pruem.it.eu-admin.net	
CY	*dna.pruem.cy*.eu-admin.net	
	fp.pruem.cy.eu-admin.net	
LV	*dna.pruem.lv*.eu-admin.net	
	fp.pruem.lv.eu-admin.net	
LT	*dna.pruem.lt*.eu-admin.net	
	fp.pruem.lt.eu-admin.net	
LU	*dna.pruem.lu*.eu-admin.net	Using the existing TESTA II national access point
	fp.pruem.lu.eu-admin.net	
HU	*dna.pruem.hu*.eu-admin.net	
	fp.pruem.hu.eu-admin.net	
MT	*dna.pruem.mt*.eu-admin.net	
	fp.pruem.mt.eu-admin.net	
NL	*dna.pruem.nl*.eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	fp.pruem.nl.eu-admin.net	
AT	*dna.pruem.at*.eu-admin.net	Using the existing TESTA II national access point
	fp.pruem.at.eu-admin.net	
PL	*dna.pruem.pl*.eu-admin.net	
	fp.pruem.pl.eu-admin.net	
PT	*dna.pruem.pt*.eu-admin.net	……
	fp.pruem.pt.eu-admin.net	……
RO	*dna.pruem.ro*.eu-admin.net	
	fp.pruem.ro.eu-admin.net	

SI	*dna.pruem.si*.eu-admin.net	……
	fp.pruem.si.eu-admin.net	……
SK	*dna.pruem.sk*.eu-admin.net	
	fp.pruem.sk.eu-admin.net	
FI	*dna.pruem.fi*.eu-admin.net	*[To be inserted]*
	fp.pruem.fi.eu-admin.net	
SE	*dna.pruem.se*.eu-admin.net	
	fp.pruem.se.eu-admin.net	
UK	*dna.pruem.uk*.eu-admin.net	
	fp.pruem.uk.eu-admin.net	

CHAPTER 2: EXCHANGE OF DACTYLOSCOPIC DATA (INTERFACE CONTROL DOCUMENT)

The purpose of the following document interface Control Document is to define the requirements for the exchange of dactyloscopic information between the Automated Fingerprint Identification Systems (AFIS) of the States. It is based on the Interpol-Implementation of ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).

This version shall cover all basic definitions for Logical Records Type-1, Type-2, Type-4, Type-9, Type-13 and Type-15 required for image and minutiæ based dactyloscopic processing.

1. File Content Overview

A dactyloscopic file consists of several logical records. There are sixteen types of record specified in the original ANSI/NIST-ITL 1-2000 standard. Appropriate ASCII separation characters are used between each record and the fields and subfields within the records.

Only 6 record types are used to exchange information between the originating and the destination agency:

Type-1	→	Transaction information
Type-2	→	Alphanumeric persons/case data
Type-4	→	High resolution greyscale dactyloscopic images
Type-9	→	Minutiæ Record
Type-13	→	Variable resolution latent image record

Type-15	→	Variable resolution palmprint image record

1.1. Type-1 — File header

This record contains routing information and information describing the structure of the rest of the file. This record type also defines the types of transaction which fall under the following broad categories:

1.2. Type-2 — Descriptive text

This record contains textual information of interest to the sending and receiving agencies.

1.3. Type-4 — High resolution greyscale image

This record is used to exchange high resolution greyscale (eight bit) dactyloscopic images sampled at 500 pixels/inch. The dactyloscopic images shall be compressed using the WSQ algorithm with a ratio of not more than 15:1. Other compression algorithms or uncompressed images must not be used.

1.4. Type-9 — Minutiæ record

Type-9 records are used to exchange ridge characteristics or minutiæ data. Their purpose is partly to avoid unnecessary duplication of AFIS encoding processes and partly to allow the transmission of AFIS codes which contain less data than the corresponding images.

1.5. Type-13 — Variable-Resolution Latent Image Record

This record shall be used to exchange variable-resolution latent fingerprint and latent palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 grey-levels. If the quality of the latent image is sufficient it shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 grey-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

1.6. Variable-Resolution Palmprint Image Record

Type-15 tagged field image records shall be used to exchange variable-resolution palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 grey-levels. To minimise the amount of data all palmprint images shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 grey-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

2. Record format

A transaction file shall consist of one or more logical records. For each logical record contained in the file, several information fields appropriate to that record type shall be present. Each information field may contain one or more basic single-valued information items. Taken together these items are used to convey different aspects of the data contained in that field. An information field may also consist

of one or more information items grouped together and repeated multiple times within a field. Such a group of information items is known as a subfield. An information field may therefore consist of one or more subfields of information items.

2.1. Information separators

In the tagged-field logical records, mechanisms for delimiting information are implemented by use of four ASCII information separators. The delimited information may be items within a field or subfield, fields within a logical record, or multiple occurrences of subfields. These information separators are defined in the standard ANSI X3.4. These characters are used to separate and qualify information in a logical sense. Viewed in a hierarchical relationship, the File Separator 'FS' character is the most inclusive followed by the Group Separator 'GS', the Record Separator 'RS', and finally the Unit Separator 'US' characters. Table 1 lists these ASCII separators and a description of their use within this standard.

Information separators should be functionally viewed as an indication of the type data that follows. The 'US' character shall separate individual information items within a field or subfield. This is a signal that the next information item is a piece of data for that field or subfield. Multiple subfields within a field separated by the 'RS' character signals the start of the next group of repeated information item(s). The 'GS' separator character used between information fields signals the beginning of a new field preceding the field identifying number that shall appear. Similarly, the beginning of a new logical record shall be signalled by the appearance of the 'FS' character.

The four characters are only meaningful when used as separators of data items in the fields of the ASCII text records. There is no specific meaning attached to these characters occurring in binary image records and binary fields — they are just part of the exchanged data.

Normally, there should be no empty fields or information items and therefore only one separator character should appear between any two data items. The exception to this rule occurs for those instances where the data in fields or information items in a transaction are unavailable, missing, or optional, and the processing of the transaction is not dependent upon the presence of that particular data. In those instances, multiple and adjacent separator characters shall appear together rather than requiring the insertion of dummy data between separator characters.

For the definition of a field that consists of three information items, the following applies. If the information for the second information item is missing, then two adjacent 'US' information separator characters would occur between the first and third information items. If the second and third information items were both missing, then three separator characters should be used — two 'US' characters in addition to the terminating field or subfield separator character. In general, if one or more mandatory or optional information items are unavailable for a field or subfield, then the appropriate number of separator character should be inserted.

It is possible to have side-by-side combinations of two or more of the four available separator characters. When data are missing or unavailable for information items, subfields, or fields, there must be one separator character less than the number of data items, subfields, or fields required.

Table 1: Separators Used

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2. Record layout

For tagged-field logical records, each information field that is used shall be numbered in accordance with this standard. The format for each field shall consist of the logical record type number followed by a period '.', a field number followed by a colon ':', followed by the information appropriate to that field. The tagged-field number can be any one-to-nine digit number occurring between the period '.' and the colon ':'. It shall be interpreted as an unsigned integer field number. This implies that a field number of '2.123:' is equivalent to and shall be interpreted in the same manner as a field number of '2.000000123:'.

For purposes of illustration throughout this document, a three-digit number shall be used for enumerating the fields contained in each of the tagged-field logical records described herein. Field numbers will have the form of 'TT.xxx:' where the 'TT' represents the one- or two-character record type followed by a period. The next three characters comprise the appropriate field number followed by a colon. Descriptive ASCII information or the image data follows the colon.

Logical Type-1 and Type-2 records contain only ASCII textual data fields. The entire length of the record (including field numbers, colons, and separator characters) shall be recorded as the first ASCII field within each of these record types. The ASCII File Separator 'FS' control character (signifying the end of the logical record or transaction) shall follow the last byte of ASCII information and shall be included in the length of the record.

In contrast to the tagged-field concept, the Type-4 record contains only binary data recorded as ordered fixed-length binary fields. The entire length of the record shall be recorded in the first four-byte binary field of each record. For this binary record, neither the record number with its period, nor the field identifier number and its following colon, shall be recorded. Furthermore, as all the field lengths of this record is either fixed or specified, none of the four separator characters ('US', 'RS', 'GS', or 'FS') shall be interpreted as anything other than binary data. For the binary record, the 'FS' character shall not be used as a record separator or transaction terminating character.

3. Type-1 Logical Record: the File Header

This record describes the structure of the file, the type of the file, and other important information. The character set used for Type-1 fields shall contain only the 7-bit ANSI code for information interchange.

3.1. Fields for Type-1 Logical Record

3.1.1. *Field 1.001: Logical Record Length (LEN)*

This field contains the total count of the number of bytes in the whole Type-1 logical record. The field begins with '1.001:', followed by the total length of the record including every character of every field and the information separators.

3.1.2. *Field 1.002: Version Number (VER)*

To ensure that users know which version of the ANSI/NIST standard is being used, this four byte field specifies the version number of the standard being implemented by the software or system creating the file. The first two bytes specify the major version reference number, the second two the minor revision number. For example, the original 1986 Standard would be considered the first version and designated '0100' while the present ANSI/NIST-ITL 1-2000 standard is '0300'.

3.1.3. *Field 1.003: File Content (CNT)*

This field lists each of the records in the file by record type and the order in which the records appear in the logical file. It consists of one or more subfields, each of which in turn contains two information items describing a single logical record found in the current file. The subfields are entered in the same order in which the records are recorded and transmitted.

The first information item in the first subfield is '1', to refer to this Type-1 record. It is followed by a second information item which contains the number of other records contained in the file. This number is also equal to the count of the remaining subfields of field 1.003.

Each of the remaining subfields is associated with one record within the file, and the sequence of subfields corresponds to the sequence of records. Each subfield contains two items of information. The first is to identify the Type of the record. The second is the record's IDC. The 'US' character shall be used to separate the two information items.

3.1.4. *Field 1.004: Type of Transaction (TOT)*

This field contains a three letter mnemonic designating the type of the transaction. These codes may be different from those used by other implementations of the ANSI/NIST standard.

CPS: Criminal Print-to-Print Search. This transaction is a request for a search of a record relating to a criminal offence against a prints database. The person's prints must be included as WSQ-compressed images in the file.

In case of a No-HIT, the following logical records will be returned:

- 1 Type-1 Record,
- 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

- 1 Type-1 Record,

- 1 Type-2 Record,
- 1-14 Type-4 Record.

The CPS TOT is summarised in Table A.6.1 (Appendix 6).

PMS: Print-to-Latent Search. This transaction is used when a set of prints shall to be searched against an Unidentified Latent database. The response will contain the Hit/No-Hit decision of the destination AFIS search. If multiple unidentified latents exist, multiple SRE transactions will be returned, with one latent per transaction. The person's prints must be included as WSQ-compressed images in the file.

In case of a No-HIT, the following logical records will be returned:

- 1 Type-1 Record,
- 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1 Type-13 Record.

The PMS TOT is summarised in Table A.6.1 (Appendix 6).

MPS: Latent-to-Print Search. This transaction is used when a latent is to be searched against a Prints database. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a No-HIT, the following logical records will be returned:

- 1 Type-1 Record,
- 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

- 1 Type-1 Record,
- 1 Type-2 Record,
- 1 Type-4 or Type-15 Record.

The MPS TOT is summarised in Table A.6.4 (Appendix 6).

MMS: Latent-to-Latent Search. In this transaction the file contains a latent which is to be searched against an Unidentified Latent database in order to establish links between various scenes of crime. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a No-HIT, the following logical records will be returned:

– 1 Type-1 Record,

– 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

– 1 Type-1 Record,

– 1 Type-2 Record,

– 1 Type-13 Record.

The MMS TOT is summarised in Table A.6.4 (Appendix 6).

SRE: This transaction is returned by the destination agency in response to dactyloscopic submissions. The response will contain the Hit/No-Hit decision of the destination AFIS search. If multiple candidates exist, multiple SRE transactions will be returned, with one candidate per transaction.

The SRE TOT is summarised in Table A.6.2 (Appendix 6).

ERR: This transaction is returned by the destination AFIS to indicate a transaction error. It includes a message field (ERM) indicating the error detected. The following logical records will be returned:

– 1 Type-1 Record,

– 1 Type-2 Record.

The ERR TOT is summarised in Table A.6.3 (Appendix 6).

Table 2: Permissible Codes in Transactions

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Key:

M	=	Mandatory,
M*	=	Only one of both record-types may be included,
O	=	Optional,
C	=	Conditional on whether data is available,
—	=	Not allowed,
1*	=	Conditional depending on legacy systems.

3.1.5. *Field 1.005: Date of Transaction (DAT)*

This field indicates the date on which the transaction was initiated and must conform to the ISO standard notation of: YYYYMMDD

where YYYY is the year, MM is the month and DD is the day of the month. Leading zeros are used for single figure numbers. For example, '19931004' represents 4 October 1993.

3.1.6. *Field 1.006: Priority (PRY)*

This optional field defines the priority, on a level of 1 to 9, of the request. '1' is the highest priority and '9' the lowest. Priority '1' transactions shall be processed immediately.

3.1.7. *Field 1.007: Destination Agency Identifier (DAI)*

This field specifies the destination agency for the transaction.

It consists of two information items in the following format: CC/agency.

The first information item contains the Country Code, defined in ISO 3166, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

3.1.8. *Field 1.008: Originating Agency Identifier (ORI)*

This field specifies the file originator and has the same format as the DAI (Field 1.007).

3.1.9. *Field 1.009: Transaction Control Number (TCN)*

This is a control number for reference purposes. It should be generated by the computer and have the following format: YYSSSSSSSSA

where YY is the year of the transaction, SSSSSSSS is an eight-digit serial number, and A is a check character generated by following the procedure given in Appendix 2.

Where a TCN is not available, the field, YYSSSSSSSS, is filled with zeros and the check character generated as above.

3.1.10. *Field 1.010: Transaction Control Response (TCR)*

Where a request was sent out, to which this is the response, this optional field will contain the transaction control number of the request message. It therefore has the same format as TCN (Field 1.009).

3.1.11. *Field 1.011: Native Scanning Resolution (NSR)*

This field specifies the normal scanning resolution of the system supported by the originator of the transaction. The resolution is specified as two numeric digits followed by the decimal point and then two more digits.

For all transactions pursuant to Article LAW.PRUM.11 and LAW.PRUM.12 the sampling rate shall be 500 pixels/inch or 19,68 pixels/mm.

3.1.12. *Field 1.012: Nominal Transmitting Resolution (NTR)*

This five-byte field specifies the nominal transmitting resolution for the images being transmitted. The resolution is expressed in pixels/mm in the same format as NSR (Field 1.011).

3.1.13. *Field 1.013: Domain name (DOM)*

This mandatory field identifies the domain name for the user-defined Type-2 logical record implementation. It consists of two information items and shall be 'INT-I{}{US}}4.22{}{GS}}'.

3.1.14. *Field 1.014: Greenwich mean time (GMT)*

This mandatory field provides a mechanism for expressing the date and time in terms of universal Greenwich Mean Time (GMT) units. If used, the GMT field contains the universal date that will be in addition to the local date contained in Field 1.005 (DAT). Use of the GMT field eliminates local time inconsistencies encountered when a transaction and its response are transmitted between two places separated by several time zones. The GMT provides a universal date and 24-hour clock time independent of time zones. It is represented as 'CCYYMMDDHHMMSSZ', a 15-character string that is the concatenation of the date with the GMT and concludes with a 'Z'. The 'CCYY' characters shall represent the year of the transaction, the 'MM' characters shall be the tens and units values of the month, and the 'DD' characters shall be the tens and units values of the day of the month, the 'HH' characters represent the hour, the 'MM' the minute, and the 'SS' represents the second. The complete date shall not exceed the current date.

4. Type-2 Logical Record: Descriptive Text

The structure of most of this record is not defined by the original ANSI/NIST standard. The record contains information of specific interest to the agencies sending or receiving the file. To ensure that communicating dactyloscopic systems are compatible, it is required that only the fields listed below are contained within the record. This document specifies which fields are mandatory and which optional, and also defines the structure of the individual fields.

4.1. Fields for Type-2 Logical Record

4.1.1. *Field 2.001: Logical Record Length (LEN)*

This mandatory field contains the length of this Type-2 record, and specifies the total number of bytes including every character of every field contained in the record and the information separators.

4.1.2. *Field 2.002: Image Designation Character (IDC)*

The IDC contained in this mandatory field is an ASCII representation of the IDC as defined in the File Content field (CNT) of the Type-1 record (Field 1.003).

4.1.3. *Field 2.003: System Information (SYS)*

This field is mandatory and contains four bytes which indicate which version of the INT-I this particular Type-2 record complies with.

The first two bytes specify the major version number, the second two the minor revision number. For example, this implementation is based on INT-I version 4 revision 22 and would be represented as '0422'.

4.1.4. *Field 2.007: Case Number (CNO)*

This is a number assigned by the local dactyloscopic bureau to a collection of latents found at a scene-of-crime. The following format is adopted: CC/number

where CC is the Interpol Country Code, two alpha-numeric characters in length, and the number complies with the appropriate local guidelines and may be up to 32 alpha-numeric characters long.

This field allows the system to identify latents associated with a particular crime.

4.1.5. *Field 2.008: Sequence Number (SQN)*

This specifies each sequence of latents within a case. It can be up to four numeric characters long. A sequence is a latent or series of latents which are grouped together for the purposes of filing and/or searching. This definition implies that even single latents will still have to be assigned a sequence number.

This field together with MID (Field 2.009) may be included to identify a particular latent within a sequence.

4.1.6. *Field 2.009: Latent Identifier (MID)*

This specifies the individual latent within a sequence. The value is a single letter or two letters, with 'A' assigned to the first latent, 'B' to the second, and so on up to a limit of 'ZZ'. This field is used analogue to the latent sequence number discussed in the description for SQN (Field 2.008).

4.1.7. *Field 2.010: Criminal Reference Number (CRN)*

This is a unique reference number assigned by a national agency to an individual who is charged for the first time with committing an offence. Within one country no individual ever has more than one

CRN, or shares it with any other individual. However, the same individual may have Criminal Reference Numbers in several countries, which will be distinguishable by means of the country code.

The following format is adopted for CRN field: CC/number

where CC is the Country Code, defined in ISO 3166, two alpha-numeric characters in length, and the number complies with the appropriate national guidelines of the issuing agency, and may be up to 32 alpha-numeric characters long.

For transactions pursuant to Article LAW.PRUM.11 and LAW.PRUM.12 this field will be used for the national criminal reference number of the originating agency which is linked to the images in Type-4 or Type-15 Records.

4.1.8. *Field 2.012: Miscellaneous Identification Number (MN1)*

This fields contains the CRN (Field 2.010) transmitted by a CPS or PMS transaction without the leading country code.

4.1.9. *Field 2.013: Miscellaneous Identification Number (MN2)*

This fields contains the CNO (Field 2.007) transmitted by an MPS or MMS transaction without the leading country code.

4.1.10. *Field 2.014: Miscellaneous Identification Number (MN3)*

This fields contains the SQN (Field 2.008) transmitted by an MPS or MMS transaction.

4.1.11. *Field 2.015: Miscellaneous Identification Number (MN4)*

This fields contains the MID (Field 2.009) transmitted by an MPS or MMS transaction.

4.1.12. *Field 2.063: Additional Information (INF)*

In case of an SRE transaction to a PMS request this field gives information about the finger which caused the possible HIT. The format of the field is:

NN where *NN* is the finger position code defined in table 5, two digits in length.

In all other cases the field is optional. It consists of up to 32 alpha-numeric characters and may give additional information about the request.

4.1.13. *Field 2.064: Respondents List (RLS)*

This field contains at least two subfields. The first subfield describes the type of search that has been carried out, using the three-letter mnemonics which specify the transaction type in TOT (Field 1.004). The second subfield contains a single character. An ‘I’ shall be used to indicate that a HIT has been found and an ‘N’ shall be used to indicate that no matching cases have been found (NOHIT). The third subfield contains the sequence identifier for the candidate result and the total number of candidates separated by a slash. Multiple messages will be returned if multiple candidates exist.

In case of a possible HIT the fourth subfield shall contain the score up to six digits long. If the HIT has been verified the value of this subfield is defined as '999999'.

Example: 'CPS{}{RS}}I{}{RS}}001/001{}{RS}}999999{}{GS}}'

If the remote AFIS does not assign scores, then a score of zero should be used at the appropriate point.

4.1.14. *Field 2.074: Status/Error Message Field (ERM)*

This field contains error messages resulting from transactions, which will be sent back to the requester as part of an Error Transaction.

Table 3: Error messages

Numeric code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	Mandatory field missing
102	Invalid record type
103	Undefined field
104	Exceed the maximum occurrence
105	Invalid number of subfields
106	Field length too short
107	Field length too long
108	Field is not a number as expected
109	Field number value too small
110	Field number value too big
111	Invalid character
112	Invalid date
115	Invalid item value
116	Invalid type of transaction
117	Invalid record data
201	ERROR: INVALID TCN

501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY.

Error messages in the range between 100 and 199:

These error messages are related to the validation of the ANSI/NIST records and defined as:

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>…

where

- error_code is a code uniquely related to a specific reason (see table 3),
- field_id is the ANSI/NIST field number of the incorrect field (e.g. 1.001, 2.001, …) in the format <record_type>.<field_id>.<sub_field_id>,
- dynamic text is a more detailed dynamic description of the error,
- LF is a Line Feed separating errors if more then one error is encountered,
- for type-1 record the ICD is defined as '-1'.

Example:

201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {}{LF}} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION

This field is mandatory for error transactions.

4.1.15. *Field 2.320: Expected Number of Candidates (ENC)*

This field contains the maximum number of candidates for verification expected by the requesting agency. The value of ENC must not exceed the values defined in table 11.

5. Type-4 Logical Record: High Resolution GreyScale Image

It should be noted that Type-4 records are binary rather than ASCII in nature. Therefore each field is assigned a specific position within the record, which implies that all fields are mandatory.

The standard allows both image size and resolution to be specified within the record. It requires Type-4 Logical Records to contain dactyloscopic image data that are being transmitted at a nominal pixel density of 500 to 520 pixels per inch. The preferred rate for new designs is at a pixel density of

500 pixels per inch or 19,68 pixels per mm. 500 pixels per inch is the density specified by the INT-I, except that similar systems may communicate with each other at a non-preferred rate, within the limits of 500 to 520 pixels per inch.

5.1. Fields for Type-4 Logical Record

5.1.1. *Field 4.001: Logical Record Length (LEN)*

This four-byte field contains the length of this Type-4 record, and specifies the total number of bytes including every byte of every field contained in the record.

5.1.2. *Field 4.002: Image Designation Character (IDC)*

This is the one-byte binary representation of the IDC number given in the header file.

5.1.3. *Field 4.003: Impression Type (IMP)*

The impression type is a single-byte field occupying the sixth byte of the record.

Table 4: Finger Impression Type

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4. *Field 4.004: Finger Position (FGP)*

This fixed-length field of 6 bytes occupies the seventh through twelfth byte positions of a Type-4 record. It contains possible finger positions beginning in the left most byte (byte 7 of the record). The known or most probable finger position is taken from table 5. Up to five additional fingers may be referenced by entering the alternate finger positions in the remaining five bytes using the same

format. If fewer than five finger position references are to be used the unused bytes are filled with binary 255. To reference all finger positions code 0, for unknown, is used.

Table 5: Finger position code and maximum size			
Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40,0	40,0
Right thumb	1	45,0	40,0
Right index finger	2	40,0	40,0
Right middle finger	3	40,0	40,0
Right ring finger	4	40,0	40,0
Right little finger	5	33,0	40,0
Left thumb	6	45,0	40,0
Left index finger	7	40,0	40,0
Left middle finger	8	40,0	40,0
Left ring finger	9	40,0	40,0
Left little finger	10	33,0	40,0
Plain right thumb	11	30,0	55,0
Plain left thumb	12	30,0	55,0
Plain right four fingers	13	70,0	65,0
Plain left four fingers	14	70,0	65,0

For scene of crime latents only the codes 0 to 10 should be used.

5.1.5. *Field 4.005: Image Scanning Resolution (ISR)*

This one-byte field occupies the 13th byte of a Type-4 record. If it contains ‘0’ then the image has been sampled at the preferred scanning rate of 19,68 pixels/mm (500 pixels per inch). If it contains ‘1’ then the image has been sampled at an alternative scanning rate as specified in the Type-1 record.

5.1.6. *Field 4.006: Horizontal Line Length (HLL)*

This field is positioned at bytes 14 and 15 within the Type-4 record. It specifies the number of pixels contained in each scan line. The first byte will be the most significant.

5.1.7. *Field 4.007: Vertical Line Length (VLL)*

This field records in bytes 16 and 17 the number of scan lines present in the image. The first byte is the most significant.

5.1.8. *Field 4.008: Greyscale Compression Algorithm (GCA)*

This one-byte field specifies the greyscale compression algorithm used to encode the image data. For this implementation, a binary code 1 indicates that WSQ compression (Appendix 7) has been used.

5.1.9. *Field 4.009: The Image*

This field contains a byte stream representing the image. Its structure will obviously depend on the compression algorithm used.

6. Type-9 Logical Record: Minutiæ Record

Type-9 records shall contain ASCII text describing minutiæ and related information encoded from a latent. For latent search transaction, there is no limit for these Type-9 records in a file, each of which shall be for a different view or latent.

6.1. Minutiæ extraction

6.1.1. *Minutia type identification*

This standard defines three identifier numbers that are used to describe the minutia type. These are listed in table 6. A ridge ending shall be designated Type 1. A bifurcation shall be designated Type 2. If a minutia cannot be clearly categorised as one of the above two types, it shall be designated as 'other', Type 0.

Table 6: Minutia types

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. *Minutia placement and type*

For templates to be compliant with Section 5 of the ANSI INCITS 378-2004 standard, the following method, which enhances the current INCITS 378-2004 standard, shall be used for determining placement (location and angular direction) of individual minutiae.

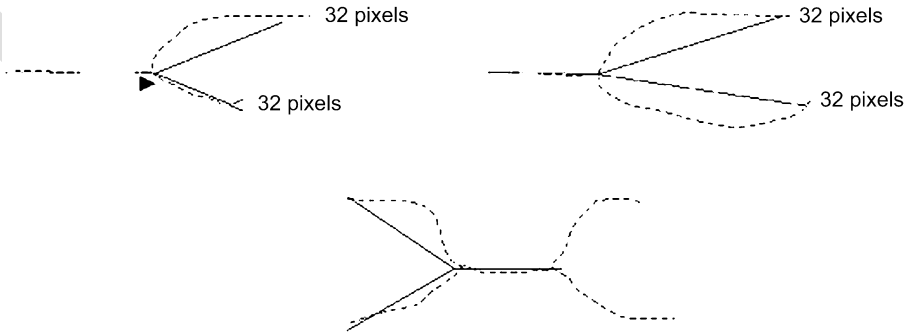
The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is the location of the minutia. Similarly, the location of the minutia for a bifurcation shall be the point of forking of the medial skeleton of the ridge. If the three legs of the ridge were each thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia.

After all ridge endings have been converted to bifurcations, all of the minutiae of the dactyloscopic image are represented as bifurcations. The X and Y pixel coordinates of the intersection of the three legs of each minutia can be directly formatted. Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figure 6.1.2 illustrates the three methods used for determining the end of a leg that is based on a scanning resolution of 500 ppi.

The ending is established according to the event that occurs first. The pixel count is based on a scan resolution of 500 ppi. Different scan resolutions would imply different pixel counts.

- a distance of 0,064" (the 32nd pixel),
- the end of skeleton leg that occurs between a distance of 0,02" and 0,064" (the 10th through the 32nd pixels); shorter legs are not used,
- a second bifurcation is encountered within a distance of 0,064" (before the 32nd pixel).

Figure 6.1.2



The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

6.1.3. *Coordinate system*

The coordinate system used to express the minutiae of a fingerprint shall be a Cartesian coordinate system. Minutiae locations shall be represented by their x and y coordinates. The origin of the

coordinate system shall be the upper left corner of the original image with x increasing to the right and y increasing downward. Both x and y coordinates of a minutiae shall be represented in pixel units from the origin. It should be noted that the location of the origin and units of measure is not in agreement with the convention used in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.1.4. *Minutiæ direction*

Angles are expressed in standard mathematical format, with zero degrees to the right and angles increasing in the counter clockwise direction. Recorded angles are in the direction pointing back along the ridge for a ridge ending and toward the centre of the valley for a bifurcation. This convention is 180 degrees opposite of the angle convention described in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.2. Fields for Type-9 Logical record INCITS-378 Format

All fields of the Type-9 records shall be recorded as ASCII text. No binary fields are permissible in this tagged-field record.

6.2.1. *Field 9.001: Logical record length (LEN)*

This mandatory ASCII field shall contain the length of the logical record specifying the total number of bytes, including every character of every field contained in the record.

6.2.2. *Field 9.002: Image designation character (IDC)*

This mandatory two-byte field shall be used for the identification and location of the minutiæ data. The IDC contained in this field shall match the IDC found in the file content field of the Type-1 record.

6.2.3. *Field 9.003: Impression type (IMP)*

This mandatory one-byte field shall describe the manner by which the dactyloscopic image information was obtained. The ASCII value of the proper code as selected from table 4 shall be entered in this field to signify the impression type.

6.2.4. *Field 9.004: Minutiæ format (FMT)*

This field shall contain a ‘U’ to indicate that the minutiae are formatted in M1-378 terms. Even though information may be encoded in accordance with the M1-378 standard, all data fields of the Type-9 record must remain as ASCII text fields.

6.2.5. *Field 9.126: CBEFF information*

This field shall contain three information items. The first information item shall contain the value ‘27’ (0x1B). This is the identification of the CBEFF Format Owner assigned by the International Biometric Industry Association (IBIA) to INCITS Technical Committee M1. The <US> character shall delimit this item from the CBEFF Format Type that is assigned a value of ‘513’ (0x0201) to indicate that this record contains only location and angular direction data without any Extended Data Block information. The <US> character shall delimit this item from the CBEFF Product Identifier (PID) that identifies the ‘owner’ of the encoding equipment. The vendor establishes this value. It can be obtained from the IBIA website (www.ibia.org) if it is posted.

6.2.6. *Field 9.127: Capture equipment identification*

This field shall contain two information items separated by the <US> character. The first shall contain 'APPF' if the equipment used originally to acquire the image was certified to comply with Appendix F (IAFIS Image Quality Specification, 29 January 1999) of CJIS-RS-0010, the Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification. If the equipment did not comply it will contain the value of 'NONE'. The second information item shall contain the Capture Equipment ID which is a vendor-assigned product number of the capture equipment. A value of '0' indicates that the capture equipment ID is unreported.

6.2.7. *Field 9.128: Horizontal line length (HLL)*

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image. The maximum horizontal size is limited to 65534 pixels.

6.2.8. *Field 9.129: Vertical line length (VLL)*

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image. The maximum vertical size is limited to 65534 pixels.

6.2.9. *Field 9.130: Scale units (SLC)*

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A '1' in this field indicates pixels per inch, or a '2' indicates pixels per centimetre. A '0' in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

6.2.10. *Field 9.131: Horizontal pixel scale (HPS)*

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the horizontal component of the pixel aspect ratio.

6.2.11. *Field 9.132: Vertical pixel scale (VPS)*

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the vertical component of the pixel aspect ratio.

6.2.12. *Field 9.133: Finger view*

This mandatory field contains the view number of the finger associated with this record's data. The view number begins with '0' and increments by one to '15'.

6.2.13. *Field 9.134: Finger position (FGP)*

This field shall contain the code designating the finger position that produced the information in this Type-9 record. A code between 1 and 10 taken from table 5 or the appropriate palm code from table 10 shall be used to indicate the finger or palm position.

6.2.14. *Field 9.135: Finger quality*

The field shall contain the quality of the overall finger minutiæ data and shall be between 0 and 100. This number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutiæ record.

6.2.15. *Field 9.136: number of minutiæ*

The mandatory field shall contain a count of the number of minutiæ recorded in this logical record.

6.2.16. *Field 9.137: Finger minutiæ data*

This mandatory field has six information items separated by the <US> character. It consists of several subfields, each containing the details of single minutiae. The total number of minutiae subfields must agree with the count found in field 136. The first information item is the minutiae index number, which shall be initialised to '1' and incremented by '1' for each additional minutia in the fingerprint. The second and third information items are the 'x' coordinate and 'y' coordinates of the minutiae in pixel units. The fourth information item is the minutiae angle recorded in units of two degrees. This value shall be nonnegative between 0 and 179. The fifth information item is the minutiae type. A value of '0' is used to represent minutiae of type 'OTHER', a value of '1' for a ridge ending and a value of '2' for a ridge bifurcation. The sixth information item represents the quality of each minutiae. This value shall range from 1 as a minimum to 100 as a maximum. A value of '0' indicates that no quality value is available. Each subfield shall be separated from the next with the use of the <RS> separator character.

6.2.17. *Field 9.138: Ridge count information*

This field consists of a series of subfields each containing three information items. The first information item of the first subfield shall indicate the ridge count extraction method. A '0' indicates that no assumption shall be made about the method used to extract ridge counts, nor their order in the record. A '1' indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in four quadrants, and ridge counts for each centre minutia are listed together. A '2' indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in eight octants, and ridge counts for each centre minutia are listed together. The remaining two information items of the first subfield shall both contain '0'. Information items shall be separated by the <US> separator character. Subsequent subfields will contain the centre minutiae index number as the first information item, the neighbouring minutiae index number as the second information item, and the number of ridges crossed as the third information item. Subfields shall be separated by the <RS> separator character.

6.2.18. *Field 9.139: Core information*

This field will consist of one subfield for each core present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the core recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

6.2.19. *Field 9.140: Delta information*

This field will consist of one subfield for each delta present in the original image. Each subfield consists of three information items. The first two items contain the ‘x’ and ‘y’ coordinate positions in pixel units. The third information item contains the angle of the delta recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

7. Type-13 variable-resolution latent image record

The Type-13 tagged-field logical record shall contain image data acquired from latent images. These images are intended to be transmitted to agencies that will automatically extract or provide human intervention and processing to extract the desired feature information from the images.

Information regarding the scanning resolution used, the image size, and other parameters required to process the image, are recorded as tagged-fields within the record.

Table 7: Type-13 variable-resolution latent record layout

Ident	Cond. code	Field Number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE	N	9	9	1	1	16

			DATE						
HLL	M	13.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13.013	FINGER POSITION	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
COM	O	13.020	COMMENT	A	2	128	0	1	135

RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13.200 13.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13.999	IMAGE DATA	B	2	—	1	1	—

Key for character type: N = Numeric; A = Alphabetic; AN = Alphanumeric; B = Binary

7.1. Fields for the Type-13 logical record

The following paragraphs describe the data contained in each of the fields for the Type-13 logical record.

Within a Type-13 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-13 record, table 7 lists the 'condition code' as being mandatory 'M' or optional 'O', the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the 'field size per occurrence' include all character separators used in the field. The 'maximum byte count' includes the field number, the information, and all the character separators including the 'GS' character.

7.1.1. *Field 13.001: Logical record length (LEN)*

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-13 logical record. Field 13.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

7.1.2. *Field 13.002: Image designation character (IDC)*

This mandatory ASCII field shall be used to identify the latent image data contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

7.1.3. *Field 13.003: Impression type (IMP)*

This mandatory one- or two-byte ASCII field shall indicate the manner by which the latent image information was obtained. The appropriate latent code choice selected from table 4 (finger) or table 9 (palm) shall be entered in this field.

7.1.4. *Field 13.004: Source agency/ORI (SRC)*

This mandatory ASCII field shall contain the identification of the administration or organisation that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/agency.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, agency, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

7.1.5. *Field 13.005: Latent capture date (LCD)*

This mandatory ASCII field shall contain the date that the latent image contained in the record was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and unit values of the day in the month. For example, 20000229 represents 29 February 2000. The complete date must be a legitimate date.

7.1.6. *Field 13.006: Horizontal line length (HLL)*

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

7.1.7. *Field 13.007: Vertical line length (VLL)*

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

7.1.8. *Field 13.008: Scale units (SLC)*

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A ‘1’ in this field indicates pixels per inch, or a ‘2’ indicates pixels per centimetre. A ‘0’ in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

7.1.9. *Field 13.009: Horizontal pixel scale (HPS)*

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a ‘1’ or a ‘2’. Otherwise, it indicates the horizontal component of the pixel aspect ratio.

7.1.10. *Field 13.010: Vertical pixel scale (VPS)*

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a ‘1’ or a ‘2’. Otherwise, it indicates the vertical component of the pixel aspect ratio.

7.1.11. *Field 13.011: Compression algorithm (CGA)*

This mandatory ASCII field shall specify the algorithm used to compress greyscale images. See Appendix 7 for the compression codes.

7.1.12. *Field 13.012: Bits per pixel (BPX)*

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of '8' for normal greyscale values of '0' to '255'. Any entry in this field greater than '8' shall represent a greyscale pixel with increased precision.

7.1.13. *Field 13.013: Finger/palm position (FGP)*

This mandatory tagged-field shall contain one or more the possible finger or palm positions that may match the latent image. The decimal code number corresponding to the known or most probable finger position shall be taken from table 5 or the most probable palm position from table 10 and entered as a one- or two-character ASCII subfield. Additional finger and/or palm positions may be referenced by entering the alternate position codes as subfields separated by the 'RS' separator character. The code '0', for 'Unknown Finger', shall be used to reference every finger position from one through ten. The code '20', for 'Unknown Palm', shall be used to reference every listed palmprint position.

7.1.14. *Field 13.014-019: Reserved for future definition (RSV)*

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.15. *Field 13.020: Comment (COM)*

This optional field may be used to insert comments or other ASCII text information with the latent image data.

7.1.16. *Field 13.021-199: Reserved for future definition (RSV)*

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.17. *Fields 13.200-998: User-defined fields (UDF)*

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

7.1.18. *Field 13.999: Image data (DAT)*

This field shall contain all data from a captured latent image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, '13.999:' is followed by image data in a binary representation.

Each pixel of uncompressed greyscale data shall normally be quantised to eight bits (256 grey levels) contained in a single byte. If the entry in BPX Field 13.012 is greater or less than '8', the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the GCA field.

7.2. End of Type-13 variable-resolution latent image record

For the sake of consistency, immediately following the last byte of data from Field 13.999 an 'FS' separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-13 record.

8. Type-15 variable-resolution palmprint image record

The Type-15 tagged-field logical record shall contain and be used to exchange palmprint image data together with fixed and user-defined textual information fields pertinent to the digitised image. Information regarding the scanning resolution used, the image size and other parameters or comments required to process the image are recorded as tagged-fields within the record. Palmprint images transmitted to other agencies will be processed by the recipient agencies to extract the desired feature information required for matching purposes.

The image data shall be acquired directly from a subject using a live-scan device, or from a palmprint card or other media that contains the subject's palmprints.

Any method used to acquire the palmprint images shall be capable of capturing a set of images for each hand. This set shall include the writer's palm as a single scanned image, and the entire area of the full palm extending from the wrist bracelet to the tips of the fingers as one or two scanned images. If two images are used to represent the full palm, the lower image shall extend from the wrist bracelet to the top of the interdigital area (third finger joint) and shall include the thenar, and hypothenar areas of the palm. The upper image shall extend from the bottom of the interdigital area to the upper tips of the fingers. This provides an adequate amount of overlap between the two images that are both located over the interdigital area of the palm. By matching the ridge structure and details contained in this common area, an examiner can confidently state that both images came from the same palm.

As a palmprint transaction may be used for different purposes, it may contain one or more unique image areas recorded from the palm or hand. A complete palmprint record set for one individual will normally include the writer's palm and the full palm image(s) from each hand. Since a tagged-field logical image record may contain only one binary field, a single Type-15 record will be required for each writer's palm and one or two Type-15 records for each full palm. Therefore, four to six Type-15 records will be required to represent the subject's palmprints in a normal palmprint transaction.

8.1. Fields for the Type-15 logical record

The following paragraphs describe the data contained in each of the fields for the Type-15 logical record.

Within a Type-15 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-15 record, table 8 lists the 'condition code' as

being mandatory ‘M’ or optional ‘O’, the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the ‘field size per occurrence’ include all character separators used in the field. The ‘maximum byte count’ includes the field number, the information, and all the character separators including the ‘GS’ character.

8.1.1. *Field 15.001: Logical record length (LEN)*

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-15 logical record. Field 15.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

8.1.2. *Field 15.002: Image designation character (IDC)*

This mandatory ASCII field shall be used to identify the palmprint image contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

8.1.3. *Field 15.003: Impression type (IMP)*

This mandatory one-byte ASCII field shall indicate the manner by which the palmprint image information was obtained. The appropriate code selected from table 9 shall be entered in this field.

8.1.4. *Field 15.004: Source agency/ORI (SRC)*

This mandatory ASCII field shall contain the identification of the administration or organisation that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/agency.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, agency, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

8.1.5. *Field 15.005: Palmprint capture date (PCD)*

This mandatory ASCII field shall contain the date that the palmprint image was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and units values of the day in the month. For example, the entry 20000229 represents 29 February 2000. The complete date must be a legitimate date.

8.1.6. *Field 15.006: Horizontal line length (HLL)*

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

8.1.7. *Field 15.007: Vertical line length (VLL)*

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

8.1.8. *Field 15.008: Scale units (SLC)*

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A ‘1’ in this field indicates pixels per inch, or a ‘2’ indicates pixels per centimetre. A ‘0’ in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

8.1.9. *Field 15.009: Horizontal pixel scale (HPS)*

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a ‘1’ or a ‘2’. Other-wise, it indicates the horizontal component of the pixel aspect ratio.

8.1.10. *Field 15.010: Vertical pixel scale (VPS)*

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a ‘1’ or a ‘2’. Otherwise, it indicates the vertical component of the pixel aspect ratio.

Table 8: Type-15 variable-resolution palmprint record layout

Ident	Cond. code	Field number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE	AN	6	35	1	1	42

			AGENCY/ORI						
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014	RESERVED FOR	—	—	—	—	—	—

		15.019	FUTURE INCLUSION						
COM	O	15.020	COMMENT	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15.200 15.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15.999	IMAGE DATA	B	2	—	1	1	—

Table 9: Palm Impression Type	
Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11. *Field 15.011: Compression algorithm (CGA)*

This mandatory ASCII field shall specify the algorithm used to compress greyscale images. An entry of 'NONE' in this field indicates that the data contained in this record are uncompressed. For those images that are to be compressed, this field shall contain the preferred method for the compression of tenprint fingerprint images. Valid compression codes are defined in Appendix 7.

8.1.12. *Field 15.012: Bits per pixel (BPX)*

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of '8' for normal greyscale values of '0' to '255'. Any entry in this field greater than or less than '8' shall represent a greyscale pixel with increased or decreased precision respectively.

Table 10: Palm Codes, Areas and Sizes

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28387	139,7	203,2
Right Full Palm	21	28387	139,7	203,2
Right Writer s Palm	22	5645	44,5	127,0
Left Full Palm	23	28387	139,7	203,2
Left Writer s Palm	24	5645	44,5	127,0
Right Lower Palm	25	19516	139,7	139,7
Right Upper Palm	26	19516	139,7	139,7
Left Lower Palm	27	19516	139,7	139,7
Left Upper Palm	28	19516	139,7	139,7
Right Other	29	28387	139,7	203,2
Left Other	30	28387	139,7	203,2

8.1.13. *Field 15.013: Palmprint position (PLP)*

This mandatory tagged-field shall contain the palmprint position that matches the palmprint image. The decimal code number corresponding to the known or most probable palmprint position shall be taken from table 10 and entered as a two-character ASCII subfield. Table 10 also lists the maximum image areas and dimensions for each of the possible palmprint positions.

8.1.14. *Field 15.014-019: Reserved for future definition (RSV)*

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.15. *Field 15.020: Comment (COM)*

This optional field may be used to insert comments or other ASCII text information with the palmprint image data.

8.1.16. *Field 15.021-199: Reserved for future definition (RSV*)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.17. *Fields 15.200-998: User-defined fields (UDF)*

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

8.1.18. *Field 15.999: Image data (DAT)*

This field shall contain all of the data from a captured palmprint image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, '15.999:' is followed by image data in a binary representation. Each pixel of uncompressed greyscale data shall normally be quantised to eight bits (256 grey levels) contained in a single byte. If the entry in BPX Field 15.012 is greater or less than 8, the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the CGA field.

8.2. End of Type-15 variable-resolution palmprint image record

For the sake of consistency, immediately following the last byte of data from Field 15.999 an 'FS' separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-15 record.

8.3. Additional Type-15 variable-resolution palmprint image records

Additional Type-15 records may be included in the file. For each additional palmprint image, a complete Type-15 logical record together with the 'FS' separator is required.

Table 11: Maximum numbers of candidates accepted for verification per transmission

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Search types:

TP/TP: ten-print against ten-print

LT/TP: fingerprint latent against ten-print

LP/PP: palmprint latent against palmprint

TP/UL: ten-print against unsolved fingerprint latent

LT/UL: fingerprint latent against unsolved fingerprint latent

PP/ULP: palmprint against unsolved palmprint latent

LP/ULP: palmprint latent against unsolved palmprint latent

9. Appendices to Chapter 2 (exchange of dactyloscopic data)

9.1. Appendix 1 ASCII Separator Codes

ASCII	Position[2]	Description
LF	1/10	Separates error codes in Field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

9.2. Appendix 2 Calculation of Alpha-Numeric Check Character

For TCN and TCR (Fields 1.09 and 1.10):

The number corresponding to the check character is generated using the following formula:

(YY * $10^{8 + S}$SSSSSSS) Modulo 23

Where YY and SSSSSSSS are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

For CRO (Field 2.010)

The number corresponding to the check character is generated using the following formula:

(YY * 10^6 + NNNNNN) Modulo 23

Where YY and NNNNNN are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

[2] This is the position as defined in the ASCII standard.

Check Character Look-up Table		
1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3. Appendix 3 Character Codes

7-bit ANSI code for information interchange										
ASCII Character Set										
+	0	1	2	3	4	5	6	7	8	9
30				!	’	#	$	%	&	‘
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{}{	|	}}	~			

9.4. Appendix 4 Transaction Summary

Type 1 Record (mandatory)					
Identifier	Field number	Field name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if transaction is a response to the origin agency

Type 2 Record (mandatory)						
Identifier	Field number	Field name	CPS/PMS	MPS/MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M

CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if data is available

*	=	if the transmission of the data is in accordance with national law (not covered by Article LAW.PRUM.11 and LAW.PRUM.12)

9.5. Appendix 5 Type-1 Record Definitions

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	1.001	Logical Record Length	N	1.001:230{}{GS}}
VER	M	1.002	Version	N	1.002:0300{}{GS

			Number		}}
CNT	M	1.003	File Content	N	1.003:1{}{US}}15{}{RS}}2{}{US}}00{}{RS}}4{}{US}}01{}{RS}}4{}{US}}02{}{RS}}4{}{US}}03{}{RS}}4{}{US}}04{}{RS}}4{}{US}}05{}{RS}}4{}{US}}06{}{RS}}4{}{US}}07{}{RS}}4{}{US}}08{}{RS}}4{}{US}}09{}{RS}}4{}{US}}10{}{RS}}4{}{US}}11{}{RS}}4{}{US}}12{}{RS}}4{}{US}}13{}{RS}}4{}{US}}14{}{GS}}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{}{GS}}
DAT	M	1.005	Date	N	1.005:20050101{}{GS}}
PRY	M	1.006	Priority	N	1.006:4{}{GS}}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{}{GS}}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{}{GS}}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{}{GS}}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{}{GS}}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{}{GS}}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19,68{}{GS}}

DOM	M	1.013	Domain Name	AN	1.013: INT-I{}{US}}4,22{}{GS}}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Under the Condition Column: O = Optional, M = Mandatory, C = Conditional

Under the Character Type Column: A = Alpha, N = Numeric, B = Binary

1* allowed characters for agency name are ['0..9', 'A..Z', 'a..z', '_', '.', '', '-']

9.6. Appendix 6 Type-2 Record Definitions

Table A.6.1: CPS- and PMS-Transaction					
Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{}{GS}}
IDC	M	2.002	Image Designation Character	N	2.002:00{}{GS}}
SYS	M	2.003	System Information	N	2.003:0422{}{GS}}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{}{GS}}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{}{GS}}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{}{GS}}

Table A.6.2: SRE-Transaction					
Identifier	Condition	Field number	Field name	Character type	Example data

LEN	M	2.001	Logical Record Length	N	2.001:909{}{GS}}
IDC	M	2.002	Image Designation Character	N	2.002:00{}{GS}}
SYS	M	2.003	System Information	N	2.003:0422{}{GS}}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{}{GS}}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{}{GS}}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{}{GS}}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{}{GS}}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{}{GS}}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{}{GS}}
RLS	M	2.064	Respondents List	AN	2.064:CPS{}{RS}}I{}{RS}}001/001{}{RS}}999999{}{GS}}

Table A.6.3: ERR-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{}{GS}}

IDC	M	2.002	Image Designation Character	N	2.002:00{}{GS}}
SYS	M	2.003	System Information	N	2.003:0422{}{GS}}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{}{GS}}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{}{GS}}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{}{GS}}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{}{GS}}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{}{GS}}
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {}{LF}} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {}{GS}}

Table A.6.4: MPS- and MMS-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{}{GS}}
IDC	M	2.002	Image Designation Character	N	2.002:00{}{GS}}
SYS	M	2.003	System Information	N	2.003:0422{}{GS}}

CNO	M	2.007	Case Number	AN	2.007:E999999999{}{GS}}
SQN	C	2.008	Sequence Number	N	2.008:0001{}{GS}}
MID	C	2.009	Latent Identifier	A	2.009:A{}{GS}}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{}{GS}}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{}{GS}}

Under the Condition Column: O = Optional, M = Mandatory, C = Conditional

Under the Character Type Column: A = Alpha, N = Numeric, B = Binary

1* allowed characters are ['0..9', 'A..Z', 'a..z', '_', '.', '', '-',',']

9.7. Appendix 7 Greyscale Compression Codes

Compression Codes

Compression	Value	Remarks
Wavelet Scalar Quantisation Greyscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated 19 December 1997	WSQ	Algorithm to be used for the compression of greyscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500dpi.
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of greyscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi

9.8. Appendix 8 Mailspecification

To improve the internal workflow the mailsubject of a PRUEM transaction has to be filled with the country code (CC) of the State that send the message and the Type of Transaction (TOT Field 1.004).

Format: CC/type of transaction

Example: 'DE/CPS'

The mailbody can be empty.

CHAPTER 3: EXCHANGE OF VEHICLE REGISTRATION DATA

1. Common data-set for automated search of vehicle registration data

1.1. Definitions

The definitions of mandatory data elements and optional data elements set out in Article 16(4) are as follows:

Mandatory (M):

The data element has to be communicated when the information is available in a State's national register. Therefore there is an obligation to exchange the information when available.

Optional (O):

The data element may be communicated when the information is available in a State's national register. Therefore there is no obligation to exchange the information even when the information is available.

An indication (Y) is given for each element in the data set where the element is specifically identified as important in relation with Article LAW.PRUM.15.

1.2. Vehicle/owner/holder search

1.2.1. *Triggers for the search*

There are two different ways to search for the information as defined in the next paragraph:

- by Chassis Number (VIN), Reference Date and Time (optional),
- by License Plate Number, Chassis Number (VIN) (optional), Reference Date and Time (optional).

By means of these search criteria, information related to one and sometimes more vehicles will be returned. If information for only one vehicle has to be returned, all the items are returned in one response. If more than one vehicle is found, the requested State itself can determine which items will be returned; all items or only the items to refine the search (e.g. because of privacy reasons or because of performance reasons).

The items necessary to refine the search are pictured in paragraph 1.2.2.1. In paragraph 1.2.2.2 the complete information set is described.

When the search is done by Chassis Number, Reference Date and Time, the search can be done in one or all of the participating States.

When the search is done by License Number, Reference Data and Time, the search has to be done in one specific State.

Normally the actual Date and Time is used to make a search, but it is possible to conduct a search with a Reference Date and Time in the past. When a search is made with a Reference Date and Time in the past and historical information is not available in the register of the specific State because no such information is registered at all, the actual information can be returned with an indication that the information is actual information.

1.2.2. *Data set*

1.2.2.1. Items to be returned necessary for the refinement of the search

Item	M/O[3]	Remarks	Prüm Y/N[4]
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1[5]) e.g. Ford, Opel, Renault, etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y
EU Category Code	M	(J) mopeds, motorbikes, cars, etc.	Y

1.2.2.2. Complete data set

Item	M/O[6]	Remarks	Prüm Y/N
Data relating to holders of the vehicle		(C.1[7]) The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for surname, infixes, titles, etc., and the name in printable format will be communicated	Y
First name	M	(C.1.2) separate fields for first name(s) and initials will be used,	Y

3 M = mandatory when available in national register, O = optional.
4 All the attributes specifically allocated by the States are indicated with Y.
5 Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999.
6 M = mandatory when available in national register, O = optional.
7 Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999.

		and the name in printable format will be communicated	
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence, etc., and the Address in printable format will be communicated	Y
Gender	M	Male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm, etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: – is the vehicle owner, – is not the vehicle owner, – is not identified by the registration certificate as being the vehicle owner.	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y
Address	M	(C.2.3)	Y

Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm, etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault, etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane.	Y
Nature of the vehicle/EU Category Code	M	(J) mopeds, motorbikes, cars, etc.	Y
Date of first registration	M	(B) Date of first registration of the vehicle somewhere in the world.	Y
Start date (actual) registration	M	(I) Date of the registration to which the specific certificate of the vehicle refers.	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	Y

Status	M	Scrapped, stolen, exported, etc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	Regular, transito, etc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document.	Y
Vehicle document id 2[8]	O	A second document ID as printed on the vehicle document.	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y
ID number	O	An identifier that uniquely identifies the company.	N
Type of ID number	O	The type of ID number (e.g. number of the Chamber of Commerce)	N

2. Data Security

2.1. Overview

The Eucaris software application handles secure communication to the other States and communicates to the back-end legacy systems of States using XML. States exchange messages by directly sending them to the recipient. The data centre of a State is connected to the TESTA network of EU.

[8] In Luxembourg two separate vehicle registration document ID's are used.

The XML-messages sent over the network are encrypted. The technique to encrypt these messages is SSL. The messages sent to the back-end are plain text XML-messages since the connection between the application and the back-end shall be in a protected environment.

A client application is provided which can be used within a State to query their own register or other States' registers. The clients will be identified by means of user-id/password or a client certificate. The connection to a user may be encrypted, but this is the responsibility of each individual State.

2.2. Security Features related to message exchange

The security design is based on a combination of HTTPS and XML signature. This alternative uses XML-signature to sign all messages sent so the server and can authenticate the sender of the message by checking the signature. 1-sided SSL (only a server certificate) is used to protect the confidentiality and integrity of the message in transit and provides protection against deletion/replay and insertion attacks. Instead of bespoke software development to implement 2-sided SSL, XML-signature is implemented. Using XML-signature is closer to the web services roadmap than 2-sided SSL and therefore more strategic.

The XML-signature can be implemented in several ways but the chosen approach is to use XML Signature as part of the Web Services Security (WSS). WSS specifies how to use XML-signature. Since WSS builds upon the SOAP standard, it is logical to adhere to the SOAP standard as much as possible.

2.3. Security features not related to message exchange

2.3.1. *Authentication of users*

The users of the Eucaris web application authenticate themselves using a username and password. Since standard Windows authentication is used, States can enhance the level of authentication of users if needed by using client certificates.

2.3.2. *User roles*

The Eucaris software application supports different user roles. Each cluster of services has its own authorisation. E.g. (exclusive) users of the '"Treaty of Eucaris" — functionality' may not use the '"Prüm" — functionality'. Administrator services are separated from the regular end-user roles.

2.3.3. *Logging and tracing of message exchange*

Logging of all message types is facilitated by the Eucaris software application. An administrator function allows the national administrator to determine which messages are logged: requests from end-users, incoming requests from other States, provided information from the national registers, etc.

The application can be configured to use an internal database for this logging, or an external (Oracle) database. The decision on what messages have to be logged clearly depends on logging facilities elsewhere in the legacy systems and connected client applications.

The header of each message contains information on the requesting State, the requesting organisation within that State and the user involved. Also the reason of the request is indicated.

By means of the combined logging in the requesting and responding State complete tracing of any message exchange is possible (e.g. on request of a citizen involved).

Logging is configured through the Eucaris web client (menu Administration, Logging configuration). The logging functionality is performed by the Core System. When logging is enabled, the complete message (header and body) is stored in one logging record. Per defined service, and per message type that passes along the Core System, the logging level can be set.

Logging Levels

The following logging levels are possible:

Private — Message is logged: The logging is NOT available to the extract logging service but is available on a national level only, for audits and problem solving.

None — Message is not logged at all.

Message Types

Information exchange between States consists of several messages, of which a schematic representation is given in the figure below.

The possible message types (in the figure shown for the Eucaris Core System of State X) are the following:

1. Request to Core System_Request message by Client
2. Request to Other State_Request message by Core System of this State
3. Request to Core System of this State_Request message by Core System of other State
4. Request to Legacy Register_Request message by Core System
5. Request to Core System_Request message by Legacy Register
6. Response from Core System_Request message by Client
7. Response from Other State_Request message by Core System of this State
8. Response from Core System of this State_Request message by other State
9. Response from Legacy Register_Request message by Core System
10. Response from Core System_Request message by Legacy Register

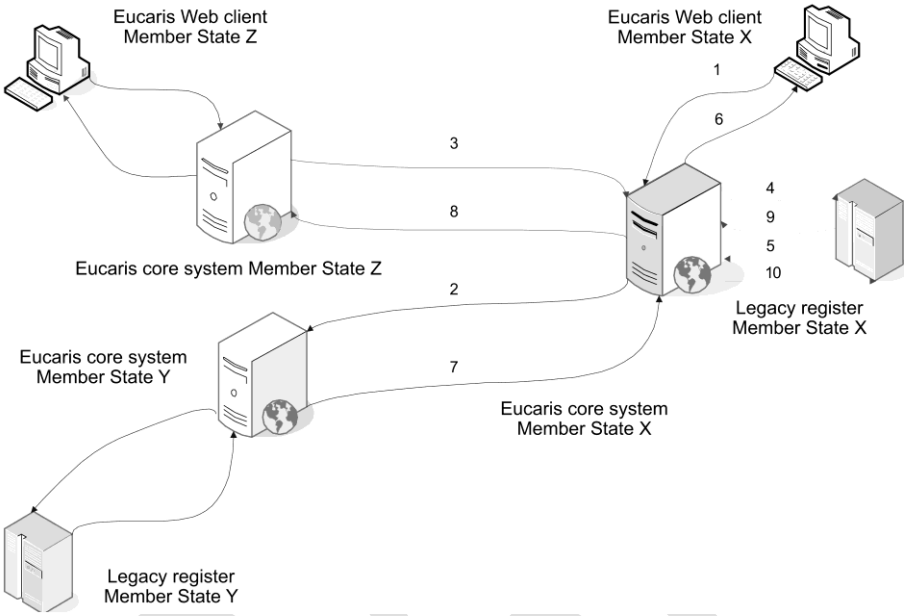
The following information exchanges are shown in the figure:

- Information request from State X to State Y — blue arrows. This request and response consists of message types 1, 2, 7 and 6, respectively,

- Information request from State Z to State X — red arrows. This request and response consists of message types 3, 4, 9 and 8, respectively,

- Information request from the legacy register to its core system (this route also includes a request from a custom client behind the legacy register) — green arrows. This kind of request consists of message types 5 and 10,

Figure: Message types for logging



2.3.4. *Hardware Security Module*

A Hardware Security Module is not used.

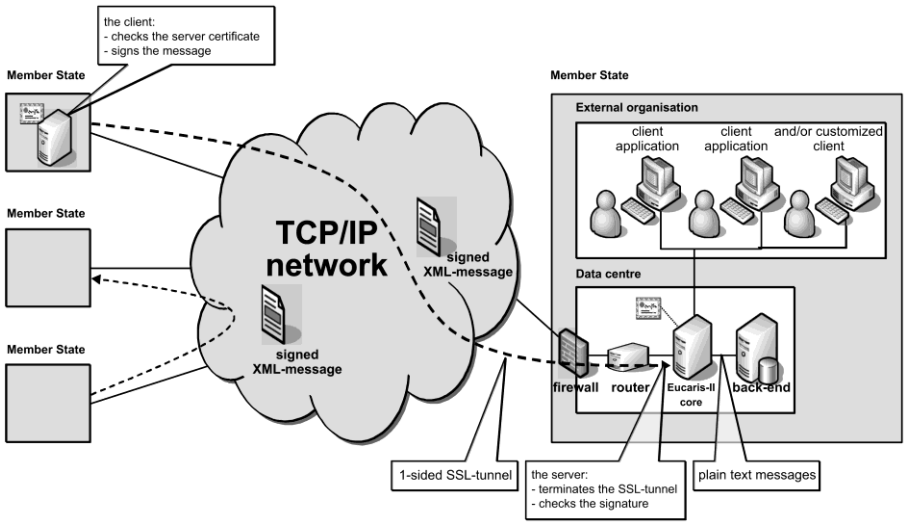
A Hardware Security Module (HSM) provides good protection for the key used to sign messages and to identify servers. This adds to the overall level of security but an HSM is expensive to buy/maintain and there are no requirements to decide for a FIPS 140-2 level 2 or level 3 HSM. Since a closed network is used that mitigates threats effectively, it is decided not to use an HSM initially. If an HSM is necessary e.g. to obtain accreditation, it can be added to the architecture.

3. Technical conditions of the data exchange

3.1. General description of the Eucaris application

3.1.1. *Overview*

The Eucaris application connects all participating States in a mesh network where each State communicates directly to another State. There is no central component needed for the communication to be established. The Eucaris application handles secure communication to the other States and communicates to the back-end legacy systems of States using XML. The following picture visualises this architecture.



State exchange messages by directly sending them to the recipient. The data centre of a State is connected to the network used for the message exchange (TESTA). To access the TESTA network, States connect to TESTA via their national gate. A firewall shall be used to connect to the network and a router connects the Eucaris application to the firewall. Depending on the alternative chosen to protect the messages, a certificate is used either by the router or by the Eucaris application.

A client application is provided which can be used within a State to query its own register or other States' registers. The client application connects to Eucaris. The clients will be identified by means of user-id/password or a client certificate. The connection to a user in an external organisation (e.g. police) may be encrypted but this is the responsibility of each individual State.

3.1.2. *Scope of the system*

The scope of the Eucaris system is limited to the processes involved in the exchange of information between the Registration Authorities in the States and a basic presentation of this information. Procedures and automated processes in which the information is to be used, are outside the scope of the system.

States can choose either to use the Eucaris client functionality or to set up their own customised client application. In the table below, it is described which aspects of the Eucaris system are mandatory to use and/or prescribed and which are optional to use and/or free to determine by the States.

Eucaris aspects	M/O[9]	Remark
Network concept	M	The concept is an ‘any-to-any’ communication.
Physical network	M	TESTA

9 M = mandatory to use or to comply with O = optional to use or to comply with.

Core application	M	The core application of Eucaris has to be used to connect to the other States. The following functionality is offered by the core: – Encrypting and signing of the messages; – Checking of the identity of the sender; – Authorisation of States and local users; – Routing of messages; – Queuing of asynchronous messages if the recipient service is temporally unavailable; – Multiple country inquiry functionality; – Logging of the exchange of messages; – Storage of incoming messages
Client application	O	In addition to the core application the Eucaris II client application can be used by a State. When applicable, the core and client application are modified under auspices of the Eucaris organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every State has to comply with the message specifications as set by the Eucaris organisation and this Council Decision. The specifications can only be changed by the Eucaris organisation in consultation with the States.
Operation and Support	M	The acceptance of new States or a new functionality is under auspices of the Eucaris organisation. Monitoring and help desk functions are managed centrally by an appointed State.

3.2. Functional and Non Functional Requirements

3.2.1. *Generic functionality*

In this section the main generic functions have been described in general terms.

No	Description
1.	The system allows the Registration Authorities of the States to exchange request and response messages in an interactive way.
2.	The system contains a client application, enabling end-users to send their requests and presenting the response information for manual processing

3.	The system facilitates 'broadcasting', allowing a State to send a request to all other States. The incoming responses are consolidated by the core application in one response message to the client application (this functionality is called a "Multiple Country Inquiry).
4.	The system is able to deal with different types of messages. User roles, authorisation, routing, signing and logging are all defined per specific service.
5.	The system allows the States to exchange batches of messages or messages containing a large number of requests or replies. These messages are dealt with in an asynchronous way.
6.	The system queues asynchronous messages if the recipient State is temporarily unavailable and guarantees the deliverance as soon as the recipient is up again.
7.	The system stores incoming asynchronous messages until they can be processed.
8.	The system only gives access to Eucaris applications of other States, not to individual organisations within those other States, i.e. each Registration Authority acts as the single gateway between its national end-users and the corresponding Authorities in the other States.
9.	It is possible to define users of different States on one Eucaris server and to authorise them following the rights of that State.
10.	Information on the requesting State, organisation and end user are included in the messages.
11.	The system facilitates logging of the exchange of messages between the different States and between the core application and the national registration systems.
12.	The system allows a specific secretary, which is an organisation or State explicitly appointed for this task, to gather logged information on messages sent/received by all the participating States, in order to produce statistical reports.
13.	Each State indicates itself what logged information is made available for the secretary and what information is 'private'.
14.	The system allows the National Administrators of each State to extract statistics of use.
15.	The system enables addition of new States through simple administrative tasks.

3.2.2. *Usability*

No	Description
16.	The system provides an interface for automated processing of messages by back-end systems/legacy and enables the integration of the user interface in those systems (customised user-interface).

17.	The system is easy to learn, self explanatory and contains help-text.
18.	The system is documented to assist States in integration, operational activities and future maintenance (e.g. reference guides, functional/technical documentation, operational guide, …).
19.	The user interface is multi-lingual and offers facilities for the end-user to select a preferred language.
20.	The user interface contains facilities for a Local Administrator to translate both screen-items and coded information to the national language.

3.2.3. *Reliability*

No	Description
21.	The system is designed as a robust and dependable operational system which is tolerant to operator errors and which will recover cleanly from power cuts or other disasters. It must be possible to restart the system with no or minimal loss of data.
22.	The system must give stable and reproducible results.
23.	The system has been designed to function reliably. It is possible to implement the system in a configuration that guarantees an availability of 98 % (by redundancy, the use of back-up servers, etc.) in each bilateral communication.
24.	It is possible to use part of the system, even during failure of some components (if State C is down, States A and B are still able to communicate). The number of single points of failure in the information chain should be minimised.
25.	The recovery time after a severe failure should be less than one day. It should be possible to minimise down-time by using remote support, e.g. by a central service desk.

3.2.4. *Performance*

No	Description
26.	The system can be used 24x7. This time-window (24x7) is then also required from the States' legacy systems.
27.	The system responds rapidly to user requests irrespective of any background tasks. This is also required from the Parties legacy systems to ensure acceptable response time. An overall response time of 10 seconds maximum for a single request is acceptable.
28.	The system has been designed as a multi-user system and in such a way that background

	tasks can continue while the user performs foreground tasks.
29.	The system has been designed to be scaleable in order to support the potential increase of number of messages when new functionality is added or new organisations or States are added.

3.2.5. *Security*

No	Description
30.	The system is suited (e.g. in its security measures) for the exchange of messages containing privacy-sensitive personal data (e.g. car owner/holders), classified as EU restricted.
31.	The system is maintained in such a way that unauthorised access to the data is prevented.
32.	The system contains a service for the management of the rights and permissions of national end-users.
33.	States are able to check the identity of the sender (at State level), by means of XML-signing.
34.	States must explicitly authorise other States to request specific information.
35.	The system provides at application level a full security and encryption policy compatible with the level of security required in such situations. Exclusiveness and integrity of the information is guaranteed by the use of XML-signing and encryption by means of SSL-tunnelling.
36.	All exchange of messages can be traced by means of logging.
37.	Protection is provided against deletion attacks (a third party deletes a message) and replay or insertion attacks (a third party replays or inserts a message).
38.	The system makes use of certificates of a Trusted Third Party (TTP).
39.	The system is able to handle different certificates per State, depending on the type of message or service.
40.	The security measures at application level are sufficient to allow the use of non accredited networks.
41.	The system is able to use novice security techniques such as an XML-firewall.

3.2.6. *Adaptability*

No	Description

42.	The system is extensible with new messages and new functionality. The costs of adaptations are minimal. Due to the centralised development of application components.
43.	States are able to define new message types for bilateral use. Not all States are required to support all message types.

3.2.7. *Support and Maintenance*

No	Description
44.	The system provides monitoring facilities for a central service-desk and/or operators concerning the network and servers in the different States.
45.	The system provides facilities for remote support by a central service-desk.
46.	The system provides facilities for problem analysis.
47.	The system can be expanded to new States.
48.	The application can easily be installed by staff with a minimum of IT-qualifications and experience. The installation procedure shall be as much as possible automated.
49.	The system provides a permanent testing and acceptance environment.
50.	The annual costs of maintenance and support has been minimised by adherence to market standards and by creating the application in such a way that as little support as possible from a central service-desk is required.

3.2.8. *Design requirements*

No	Description
51.	The system is designed and documented for an operational lifetime of many years.
52.	The system has been designed in such a way that it is independent of the network provider.
53.	The system is compliant with the existing HW/SW in the States by interacting with those registration systems using open standard web service technology (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509, etc.).

3.2.9. *Applicable standards*

No	Description

54.	The system is compliant with data protection issues as stated in Regulation EC 45/2001 (Articles 21, 22 and 23) and Directive 95/46/EC.
55.	The system complies with the IDA Standards.
56.	The system supports UTF8.

CHAPTER 4: EVALUATION PROCEDURE ACCORDING TO ARTICLE LAW.PRUM.17

1. Questionnaire

The relevant Council Working Group shall draw up a questionnaire concerning each of the automated data exchanges set out in Articles LAW.PRUM.5 to LAW.PRUM.16.

As soon as the United Kingdom believes it fulfils the prerequisites for sharing data in the relevant data category, it shall answer the relevant questionnaire.

2. Pilot run

With a view to evaluating the results of the questionnaire, the United Kingdom shall carry out a pilot run together with one or more other Member States already sharing data under Council Decision 2008/615/JHA. The pilot run takes place shortly before or shortly after the evaluation visit.

The conditions and arrangements for this pilot run will be identified by the relevant Council Working Group and be based upon prior individual agreement with the United Kingdom. The States taking part in the pilot run will decide on the practical details.

3. Evaluation visit

With a view to evaluating the results of the questionnaire, an evaluation visit shall take place.

The conditions and arrangement for this visit will be identified by the relevant Working Group and be based upon prior individual agreement between the United Kingdom and the evaluation team. The United Kingdom will enable the evaluation team to check the automated exchange of data in the data category or categories to be evaluated, in particular by organising a programme for the visit, which takes into account the requests of the evaluation team.

Within one month, the evaluation team will produce a report on the evaluation visit and will forward it to the United Kingdom for its comments. If appropriate, this report will be revised by the evaluation team on the basis of the United Kingdom's comments.

The evaluation team will consist of no more than three experts, designated by the Member States taking part in the automated data exchange in the data categories to be evaluated, who have experience regarding the concerned data category, have the appropriate national security clearance to deal with these matters and are willing to take part in at least one evaluation visit in another State. The evaluation team will also include a representative of the Commission.

The members of the evaluation team will respect the confidential nature of the information they acquire when carrying out their task.

4. Report to the Council

An overall evaluation report, summarising the results of the questionnaires, the evaluation visit and the pilot run, will be presented to the Council for its decision pursuant to Article LAW.PRUM.17.

ANNEX LAW-2

Passenger name record data as far as collected by air carriers:

1. PNR record locator,
2. Date of reservation/issue of ticket,
3. Date(s) of intended travel,
4. Name(s),
5. Address, telephone number and electronic contact information of the passenger, the persons who made the flight reservation for the passenger, persons through whom an air passenger may be contacted and persons who are to be informed in the event of an emergency,
6. All available payment/billing information (covering information relating solely to the payment methods for, and billing of, the air ticket, to the exclusion of any other information not directly relating to the flight),
7. Complete travel itinerary for specific PNR,
8. Frequent flyer information (the designator of the airline or vendor that administers the program, frequent flyer traveller number, membership level, tier description and alliance code),
9. Travel agency/travel agent,
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information,
11. Split/divided PNR information,
12. Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information,
13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields,
14. Seat information, including seat number,
15. Code share information,
16. All baggage information,
17. The names of other passengers on the PNR and number of travellers on the PNR travelling together,
18. Any advance passenger information (API) data collected (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),
19. All historical changes to the PNR listed in numbers 1 to 18.

ANNEX LAW-3

List of offences referred to in point (3) of Article LAW.PNR.20:

— Participation in a criminal organisation,

— Trafficking in human beings,

— Sexual exploitation of children and child pornography,

— Illicit trafficking in narcotic drugs and psychotropic substances,

— Illicit trafficking in weapons, munitions and explosives,

— Corruption,

— Fraud, including that against the financial interests of the Union,

— Laundering of the proceeds of crime and counterfeiting of currency, including the euro,

— Computer-related crime/cybercrime,

— Environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,

— Facilitation of unauthorised entry and residence,

— Murder, grievous bodily injury,

— Illicit trade in human organs and tissue,

— Kidnapping, illegal restraint and hostage-taking,

— Organised and armed robbery,

— Illicit trafficking in cultural goods, including antiques and works of art,

— Counterfeiting and piracy of products,

— Forgery of administrative documents and trafficking therein,

— Illicit trafficking in hormonal substances and other growth promoters,

— Illicit trafficking in nuclear or radioactive materials,

— Rape,

— Crimes within the jurisdiction of the international criminal court,

— Unlawful seizure of aircraft/ships,

— Sabotage,

— Trafficking in stolen vehicles,

— Industrial espionage.

ANNEX LAW-4

COOPERATION ON OPERATIONAL INFORMATION

FORM TO BE USED BY THE REQUESTED STATE IN CASE OF TRANSMISSION/DELAY/REFUSAL OF INFORMATION

This form shall be used to transmit the requested information and/or intelligence, to inform the requesting authority of the impossibility of meeting the normal deadline, of the necessity of submitting the request to a judicial authority for an authorisation, or of the refusal to transmit the information.

This form may be used more than once during the procedure (e.g. if the request has first to be submitted to a judicial authority and it later transpires that the execution of the request has to be refused).

Requested authority (name, address, telephone, fax, e-mail, State)	
Details of the handling agent (optional):	
Reference number of this answer	
Date and reference number of previous answer	
Answering to the following requesting authority	
Date and time of the request	
Reference number of the request	

Normal time limit under Article LAW.OPIN.42		
The offence falls under Article LAW.SURR.78(4) and	Urgency requested	☐ 8 hours
the requested information or intelligence is held in a database directly accessible by a law enforcement authority in the requested State	Urgency not requested	☐ 1 week
Other cases		☐ 14 days

Information transmitted under LAW.OPIN: information and intelligence provided
1. Use of transmitted information or intelligence ☐ may be used solely for the purposes for which it has been supplied or for preventing an immediate and serious threat to public security; ☐ is authorised also for other purposes, subject to the following conditions (optional):
2. Reliability of the source ☐ Reliable ☐ Mostly reliable ☐ Not reliable ☐ Cannot be assessed
3. Accuracy of the information or intelligence ☐ Certain ☐ Established by the source ☐ Hearsay-confirmed ☐ Hearsay- not confirmed
4. The result of the criminal investigation or criminal intelligence operation within which the exchange of information has taken place has to be reported to the transmitting authority ☐ No ☐ Yes
5. In case of spontaneous exchange, reasons for believing that the information or intelligence could assist in the detection, prevention or investigation of offences referred to in Article LAW.SURR.78(4)

DELAY – It is not possible to respond within the applicable time limit under Article LAW.OPIN.42
The information or intelligence cannot be provided within the given time-limit for the following reasons: It is likely to be given within: ☐ 1 day ☐ 2 days ☐ 3 days ☐ … weeks ☐ 1 month
☐ The authorisation of a judicial authority has been requested. The procedure leading up to the granting/refusal of the authorisation is expected to last … weeks

REFUSAL — The information or intelligence: **☐ could not be provided and requested at national level; or** **☐ cannot be provided, for one or more of the following reasons:**
A — Reason related to judicial control which prevents the transmission or requires the use of mutual legal assistance
☐ the competent judicial authority has not authorised the access and exchange of the information or intelligence
☐ the requested information or intelligence has previously been obtained by means of coercive measures and its provision is not permitted under the national law ☐ the information or intelligence is not held by law enforcement authorities; or by public authorities or by private entities in a way which makes it available to law enforcement authorities without the taking of coercive measures
☐ B — The provision of the requested information or intelligence would harm essential national security interests or would jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals or would clearly be disproportionate or irrelevant with regard to the purposes for which it has been requested.
If case A or B is used, provide, if deemed necessary, additional information or reasons for refusal (optional):
☐ D — The requested authority decides to refuse execution because the request pertains, under the law of the requested State, to the following offence (nature of the offence and its legal qualification to be specified) … which is punishable by one year or less of imprisonment
☐ E — The requested information or intelligence is not available
☐ F — The requested information or intelligence has been obtained from another State or from a third state and is subject to the rule of speciality and that State or third state has not given its consent to the transmission of the information or intelligence.

INFORMATION EXCHANGE UNDER ARTICLE LAW.OPIN.41 REQUEST FORM FOR INFORMATION AND INTELLIGENCE TO BE USED BY THE REQUESTING STATE

This form shall be used when requesting information and intelligence under Article LAW.OPIN.41

I — Administrative information

Requesting authority (name, address, telephone, fax, e-mail, State):	
Details of the handling agent (optional):	
To the following State:	
Date and time of this request:	
Reference number of this request:	

Previous requests				
☐ This is the first request on this case				
☐ This request follows previous requests in the same case				
Previous request(s)			Answer(s)	
	Date	Reference number (in the requesting State)	Date	Reference number (in the requested State)
1.				
2.				
3.				
4.				

If the request is sent to more than one authority in the requested State, please specify each of the channels used:	
☐ ENU/Europol Liaison Officer	☐ For information ☐ For execution
☐ Interpol NCB	☐ For information ☐ For execution
☐ Sirene	☐ For information ☐ For execution
☐ Liaison Officer	☐ For information ☐ For execution
☐ Other (please specify):	☐ For information ☐ For execution
If the same request is sent to other States, please specify the other States and the channel used (optional)	

II — Time limits

Reminder: time limits under Article LAW.OPIN.42

A — The offence falls under Article LAW.SURR.78(4)

and

the requested information or intelligence is held in a database directly accessible by a law enforcement authority

→ The request is urgent → Time limit: 8 hours with possibility to postpone

→ The request is not urgent → Time limit: 1 week

B — Other cases: time limit: 14 days

☐ **Urgency IS requested**
☐ **Urgency is NOT requested**
Grounds for urgency (e.g.: suspects are being held in custody, the case has to go to court before a specific date):
Information or intelligence requested

Type of crime(s) or criminal activity(ies) being investigated
Description of the circumstances in which the offence(s) was (were) committed, including the time, place and degree of participation in the offence(s) by the person who is the subject of the request for information or intelligence:

Nature of the offence(s)
A — Application of Article LAW.SURR.78(4) ☐ A.1. The offence is punishable by a maximum term of imprisonment of at least three years in the requesting State AND A.2. The offence is one (or more) of the following: ☐ participation in a criminal organisation, ☐ terrorism, ☐ trafficking in human beings, ☐ sexual exploitation of children and child pornography, ☐ illicit trafficking in narcotic drugs and psychotropic substances, ☐ illicit trafficking in weapons, munitions and explosives, ☐ corruption, ☐ fraud, including that affecting the financial interests of the Union, ☐ laundering proceeds of crime, ☐ counterfeiting currency, including of the euro, ☐ computer-related crime, ☐ environmental crime, including illicit trafficking in endangered animal species and varieties, ☐ facilitation of unauthorized entry and residence, ☐ murder, ☐ grievous bodily injury, ☐ illicit trade in human organs and tissue, ☐ kidnapping, illegal restraint and hostage-taking, ☐ racism and xenophobia,

☐ organised or armed robbery,
☐ illicit trafficking in cultural goods, including antiques and works of art,
☐ swindling,
☐ racketeering and extortion,
☐ counterfeiting and piracy of products,
☐ forgery of administrative documents and trafficking therein,
☐ forgery of means of payment,
☐ illicit trafficking in hormonal substances and other growth promoters,
☐ illicit trafficking in nuclear or radioactive materials,
☐ trafficking in stolen vehicles,
☐ rape,
☐ arson,
☐ crimes within the jurisdiction of the International Criminal Court,
☐ unlawful seizure of aircraft/ships,
☐ sabotage.

The offence therefore falls under Article LAW.SURR.78(4) → Article LAW.OPIN.42(1) (urgent cases) and 42(3) (non urgent cases) are therefore applicable as regards time limits for responding to this request

Or
☐ B — The offence(s) is(are) not covered under A.
In this case, description of the offence(s):

Purpose for which the information or intelligence is requested

Connection between the purpose for which the information or intelligence is requested and the person who is the subject of the information or intelligence

Identity(ies) (as far as known) of the person(s) being the main subject(s) of the criminal investigation or criminal intelligence operation underlying the request for information or intelligence

Reasons for believing that the information or intelligence is in the requested State

Restrictions on the use of information contained in this request for purposes other than those for which it has been supplied or for preventing an immediate and serious threat to public security
☐ use granted ☐ use granted, but do not mention the information provider ☐ do not use without authorisation of the information provider ☐ do not use

ANNEX LAW-5

Forms of crimes for which Europol is competent:

— Terrorism,

— Organised crime,

— Drug trafficking,

— Money-laundering activities,

— Crime connected with nuclear and radioactive substances,

— Immigrant smuggling,

— Trafficking in human beings,

— Motor vehicle crime,

— Murder and grievous bodily injury,

— Illicit trade in human organs and tissue,

— Kidnapping, illegal restraint and hostage-taking,

— Racism and xenophobia,

— Robbery and aggravated theft,

— Illicit trafficking in cultural goods, including antiquities and works of art,

— Swindling and fraud,

— Crime against the financial interests of the Union,

— Insider dealing and financial market manipulation,

— Racketeering and extortion,

— Counterfeiting and product piracy,

— Forgery of administrative documents and trafficking therein,

— Forgery of money and means of payment,

— Computer crime,

— Corruption,

— Illicit trafficking in arms, ammunition and explosives,

— Illicit trafficking in endangered animal species,

— Illicit trafficking in endangered plant species and varieties,

— Environmental crime, including ship-source pollution,

— Illicit trafficking in hormonal substances and other growth promoters,

— Sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,

— Genocide, crimes against humanity and war crimes.

ANNEX LAW-6

List of forms of serious crime with which Eurojust is competent to deal in accordance with Article LAW.EUROJUST.63:

— Terrorism,

— Organised crime,

— Drug trafficking,

— Money-laundering activities,

— Crime connected with nuclear and radioactive substances,

— Immigrant smuggling,

— Trafficking in human beings,

— Motor vehicle crime,

— Murder and grievous bodily injury,

— Illicit trade in human organs and tissue,

— Kidnapping, illegal restraint and hostage taking,

— Racism and xenophobia,

— Robbery and aggravated theft,

— Illicit trafficking in cultural goods, including antiquities and works of art,

— Swindling and fraud,

— Crime against the financial interests of the Union,

— Insider dealing and financial market manipulation,

— Racketeering and extortion,

— Counterfeiting and product piracy,

— Forgery of administrative documents and trafficking therein,

— Forgery of money and means of payment,

— Computer crime,

— Corruption,

— Illicit trafficking in arms, ammunition and explosives,

— Illicit trafficking in endangered animal species,

— Illicit trafficking in endangered plant species and varieties,

— Environmental crime, including ship source pollution,

— Illicit trafficking in hormonal substances and other growth promoters,

— Sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,

— Genocide, crimes against humanity and war crimes.

ANNEX LAW-7

Arrest warrant

This warrant has been issued by a competent judicial authority. I request that the person mentioned below be arrested and surrendered for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order.[10]

(a) Information regarding the identity of the requested person:	
Name:	
Forename(s):	
Maiden name, where applicable:	
Aliases, where applicable:	
Sex:	
Nationality:	
Date of birth:	
Place of birth:	
Residence and/or known address:	
Language(s) which the requested person understands (if known):	
Distinctive marks/description of the requested person:	
Photo and fingerprints of the requested person, if they are available and can be transmitted, or contact details of the person to be contacted in order to obtain such information or a DNA profile (where this evidence can be supplied but has not been included)	

(b) Decision on which the warrant is based:	
1. Arrest warrant or judicial decision having the same effect:	

[10] This warrant must be written in, or translated into, one of the official languages of the executing State, when that State is known, or any other language accepted by that State.

Type:	
2. Enforceable judgement:	
Reference:	

(c) Indications on the length of the sentence:	
1. Maximum length of the custodial sentence or detention order which may be imposed for the offence(s):	
2. Length of the custodial sentence or detention order imposed:	
Remaining sentence to be served:	

(d) Indicate if the person appeared in person at the trial resulting in the decision:

1. ☐ Yes, the person appeared in person at the trial resulting in the decision.

2. ☐ No, the person did not appear in person at the trial resulting in the decision.

3. If you have ticked the box under point 2, please confirm the existence of one of the following, if applicable:

☐ 3.1a. the person was summoned in person on … (day/month/year) and thereby informed of the scheduled date and place of the trial which resulted in the decision and was informed that a decision may be handed down if he or she does not appear for the trial;

OR

☐ 3.1b. the person was not summoned in person but by other means actually received official information of the scheduled date and place of the trial which resulted in the decision, in such a manner that it was unequivocally established that he or she was aware of the scheduled trial, and was informed that a decision may be handed down if he or she does not appear for the trial;

OR

☐ 3.2. being aware of the scheduled trial, the person had given a mandate to a legal counsellor, who was either appointed by the person concerned or by the

State, to defend him or her at the trial, and was indeed defended by that counsellor at the trial;

OR

☐ 3.3. the person was served with the decision on … (day/month/year) and was expressly informed about the right to a retrial or appeal, in which he or she has the right to participate and which allows the merits of the case, including fresh evidence, to be re-examined, and which may lead to the original decision being reversed, and

☐ the person expressly stated that he or she does not contest this decision;

OR

☐ the person did not request a retrial or appeal within the applicable timeframe;

OR

☐ 3.4. the person was not personally served with the decision, but

– the person will be personally served with this decision without delay after the surrender; and

– when served with the decision, the person will be expressly informed of his or her right to a retrial or appeal, in which he or she has the right to participate and which allows the merits of the case, including fresh evidence, to be re-examined, and which may lead to the original decision being reversed; and

– the person will be informed of the timeframe within which he or she has to request a retrial or appeal, which will be …… days.

4. If you have ticked the box under point 3.1b, 3.2 or 3.3 above, please provide information about how the relevant condition has been met:

……
……

(e) Offences:

This warrant relates to in total: offences

Description of the circumstances in which the offence(s) was (were) committed, including the time, place and degree of participation in the offence(s) by the requested person:

Nature and legal classification of the offence(s) and the applicable statutory provision/code:

I. The following applies only in case both the issuing and the executing state have made a declaration under Article 78(4) of the Agreement: if applicable, tick one or more of the following offences punishable in the issuing State by a custodial sentence or detention order of a maximum of at least three years as defined by the laws of the issuing State:

☐ participation in a criminal organisation,
☐ terrorism,
☐ trafficking in human beings,
☐ sexual exploitation of children and child pornography,
☐ illicit trafficking in narcotic drugs and psychotropic substances,
☐ illicit trafficking in weapons, munitions and explosives,
☐ corruption,
☐ fraud, including that affecting the financial interests of the Union,
☐ laundering of the proceeds of crime,
☐ counterfeiting of currency, including the euro,
☐ computer-related crime,
☐ environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
☐ facilitation of unauthorised entry and residence,
☐ murder, grievous bodily injury,
☐ illicit trade in human organs and tissue,
☐ kidnapping, illegal restraint and hostage-taking,
☐ racism and xenophobia,
☐ organised or armed robbery,
☐ illicit trafficking in cultural goods, including antiques and works of art,
☐ swindling,
☐ racketeering and extortion,
☐ counterfeiting and piracy of products,
☐ forgery of administrative documents and trafficking therein,
☐ forgery of means of payment,
☐ illicit trafficking in hormonal substances and other growth promoters,
☐ illicit trafficking in nuclear or radioactive materials,
☐ trafficking in stolen vehicles,
☐ rape,

☐ arson,
☐ crimes within the jurisdiction of the International Criminal Court,
☐ unlawful seizure of aircraft/ships,
☐ sabotage.

II. Full descriptions of offence(s) not covered by section I above:

(f) Other circumstances relevant to the case (optional information):
(NB: This could cover remarks on extraterritoriality, interruption of periods of time limitation and other consequences of the offence)

(g) This warrant pertains also to the seizure and handing over of property which may be required as evidence:

This warrant pertains also to the seizure and handing over of property acquired by the requested person as a result of the offence:

Description of the property (and location) (if known):

(h) The offence(s) on the basis of which this warrant has been issued is (are) punishable by/has(have) led to a custodial life sentence or lifetime detention order:

the issuing State will upon request by the executing State give an assurance that it will:

☐ review the penalty or measure imposed – on request or at least after 20 years,

and/or

☐ encourage the application of measures of clemency to which the person is entitled to apply for under the law or practice of the issuing State, aiming at a non-execution of such penalty or measure.

(i)	The judicial authority which issued the warrant:	
	Official name:	
	Name of its representative:[1]	
	Post held (title/grade):	
	File reference:	
	Address:	
	Tel. No.: (country code) (area/city code)	
	Fax No. (country code) (area/city code)	
	E-mail:	
	Contact details of the person to contact to make necessary practical arrangements for the surrender:	
	Where a central authority has been made responsible for the transmission and administrative reception of arrest warrants:	
	Name of the central authority:	
	Contact person, if applicable (title/grade and name):	
	Address:	
	Tel. No.: (country code) (area/city code)	
	Fax No. (country code) (area/city code)	
	E-mail:	

[1] In the different language versions a reference to the "holder" of the judicial authority will be included.

Signature of the issuing judicial authority and/or its representative:	
Name:	
Post held (title/grade):	
Date:	
Official stamp (if available):	