Council of the
European Union

Brussels, 30 October 2019
(OR. en)

13356/19

LIMITE

DAPIX 301
CRIMORG 141
ENFOCUSTOM 171
ENFOPOL 450
JAI 1089
N 65
ISL 57
CH 54
FL 71

NOTE

From:	Austrian delegation
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	11227/18; 13426/18; 14370/18; 5556/19
Subject:	Next generation Prüm (Prüm.ng) - Reports from focus groups / Report on face recognition

The initiative to reflect on the development of a next generation Prüm (Prüm.ng) was launched by the 'Council Conclusions on the implementation of the Prüm Decisions ten years after their adoption' (11227/18). Subsequently, the then Presidency started discussions within DAPIX by means of a questionnaire and presented a summary of the replies to its discussion paper on Prüm.ng (13426/18). DAPIX discussed in particular the intention to establish focus groups (14370/18) tasked to set out how to further develop the current data and information exchange mechanisms and to support the European Commission's Feasibility Study on improving information exchange under the 'Prüm Decisions'.

Delegations find in annex the final report of the focus group on face recognition. This report represents solely the opinions and views of the delegates participating in this group, based on their personal expertise. DAPIX is invited to discuss the report at its forthcoming meeting.

Development of Face Recognition for PRÜM next generation

PRÜM Focus Working Group Report

1st Expert Workshop Vienna, April 2019
2nd Expert Workshop Lisbon, June 2019
3rd Expert Workshop Wiesbaden, September 2019

Supporting Member States:			
	Austria (Chair)		Netherlands
	Germany		Poland
	Estonia		Portugal
	Spain		Romania
	Italy		United Kingdom

Table of contents

1 Introductory remarks

Based on the Council Conclusions of 16 July 2018 (11227/18) and the working methods adopted by DAPIX, focus groups were established, which were open to experts of all Member States. The first Focus Group meeting for Face Recognition (FR) was hold in Vienna in the second week of April 2019. The second meeting was hold in Lisbon in June 2019. The third and last workshop for face recognition as well as a combined FR, AFIS and DNA focus groups session took place in September in Wiesbaden.

The FR expert group decided to proceed both on the basis of written correspondence and several meetings in different supporting Member States. The aim was to submit to the Commission a document, commonly agreed upon by all participating national experts, which should contain the desired enlargement and further improvement of the currently successful Prüm cooperation network.

This document draws on the many years of experience of national experts with forensic biometrics. In support of the Commission, the focus group discussed preliminary results of the feasibility study on amending the current Prüm legislation, which was carried out by a consultancy firm on behalf of the Commission. Some proposals of these study were considered to be acceptable for further detailed discussions. Other proposals, in particular the proposal for a central data storage, were strictly rejected.

2 Face Recognition – possible usage as a new Prüm data type solution?

The expert group agreed that Face Recognition (FR) technology has advanced and has meanwhile become a highly suitable additional biometric tool in forensics. The use of FR technology might offer added value as a criminal investigation instrument for the identification of unknown perpetrators in addition to the already existing forensic DNA and dactyloscopic data types.

Not all Member States currently have the necessary technical requirements, such as a national central electronic image database with reference images or a national Face Recognition software. Numerous Member States are currently in the process of implementing such databases and FR software solutions in their central national law enforcement systems. Legal and technical prerequisites to link national FR databases for searches, namely in the proven way of Prüm online cooperation, should therefore be created as quickly as possible to enable the use of this investigation instrument at EU level.

The main objective of such an application will be the additional checking of images (e.g. taken by surveillance cameras) of unknown perpetrators of criminal offences against the national reference image databases, as provided for by national legislation for this kind of law enforcement cooperation.

A Prüm FR application should be planned and implemented in a decentralised network. The storage and use of both the reference and trace-images should be based on national legislation. Only searching in the EU partner databases and no permanent storage of transmitted data should be provided for. If a potential FR match candidate would be verified as a correct 'hit', further data processing and storage within the criminal investigation procedure should be foreseen.

The provision of 2nd step personal and/or case data such as names, crime could be carried out very quickly in case of a 'hit'. Such data content should never be provided immediately and automatically within the 1st step, but always by a separate follow-up request for a defined core data set after a match has been confirmed by a national expert of the requesting MS. This follow-up data exchange should be carried out in electronic form and according to technical solutions via encrypted network corresponding to the state-of-the-art.

3 System Architecture

3.1 Workflow-functionalities like PRÜM AFIS + 2nd Step

Core data exchange in case of a confirmed hit, after an online request from the searching Member State.

Experts considered the establishment of a 2nd step national contact point (NCP) as very important. Unlike the current Prüm legislation, a potential new Prüm legislation should make mandatory such a contact point. It should depend exclusively on national organizational and legal regulations, which competent national 2nd step NCP carries out the follow-up correspondence, and the NCP should only be notified by the Member States. Of course, this NCP must also have access to secure electronic communication channels where this follow-up information can be transmitted in electronic and encrypted form.

These 2nd step data requests should be possible in three different cooperation levels, which will entail different response timelines.

- 'Classical' follow-up data supply:

The 'classical' follow-up investigation correspondence, which should continue to exist, is carried out via the existing channels currently in use, i.e. Europol (Siena), Interpol (I-24/7), legal liaison officers network or SIRENE. It is not necessary for a national contact point to have direct access to these networks. However, it seems essential that a NCP should be able to forward and respond - if necessary also by secure routing on secure national networks - to the other Prüm 2nd step NCPs.

Only verified data, that is data confirmed as 'hit' by the national experts, will be retrieved and not also matching data of other match candidates, which could not have been confirmed as 'hit'.

This method of transmitting follow up data means a 2nd step data provision within days or weeks.

- Faster follow-up supply of 'core data'

In addition to the above possibility, an alternative request method should exist for the provision of pre-defined certain important data. These 'core data' should contain any available identification data, crime case data and offence information. They can be requested via the same secure network via which the 1step automated data exchange has already been carried out. A forensic confirmation by a national expert, who confirms a possible 'match' as a real 'hit' in line with nationally fixed forensic quality standards, is essential here. An authorised follow-up data request must be made immediately in order to provide the 'core data' available in a country.

Replying to such a follow up request may be subject to a supplementary authorisation in the requested Member State on the basis of national legislation or organisational concepts. However, the data transmission shall always been carried out in a structured, electronic and encrypted form on the same data network as the 1step data comparisons.

This method of transmitting follow up data means a 2nd step data provision within hours or days.

- Automated follow-up data supply

Automated data provision is possible between Member States which have implemented automated links to agreed 'core data' information in their national databases. In accordance with Article 4 of the Framework Decision 2006/960/JHA, these data have to be made available in certain time limits as soon as they are stored in databases, which are accessible by a law enforcement authority (LEA).

A human interface for an upstream forensic confirmation is a prerequisite in the requesting state in which the decision has been taken to query simultaneously with own 'core data'. However, the supply of data by the requested state is no longer dependent on an additional decision of an officer of the 2nd step NCP. If the requested data comply with the specified minimum data quality, which could be checked automatically by IT systems (e.g. required names, crime description, etc.), the follow-up data will be provided immediately in an automatic way to the requesting country. Only those data will be retrieved which have been confirmed as a 'hit' by the national experts and not also matching data of other match candidates.

This method of transmitting follow up data means a 2nd step data provision within seconds or minutes even if a partner country could not offer 24/7 duty service.

- 2ndstep 'core data'

Which data is suitable and necessary as 'core data' for rapid data transmission will depend on the type of data concerned. The exact definition of this 'core data' should be set out in the future legal act according to the respective data type of the cooperation and the technical possibilities.

The data types can differ according to the type of search and will consist of mandatory data contents and possible data types, which can only be provided if they are also structurally stored in a database in the requested state.

In an intensive discussion, the experts defined a set of 'core data' which should be exchanged in the case of all biometric data types. The amount of information needed deferred on the transaction type (Reference or Latent). The 'core data' set includes information on:

- Alphanumeric Personal Data,
- Information of biometrics acquisition,
- Additional biometric data information,
- Identity documents,
- Additional data (e.g. Technical, Alert or Warning Information etc.).

For reference databases, some data fields like family name, first name, date of birth, place and country of birth and gender, should be mandatory. Without this information, no 'core data' will be transmitted. All other information may be provided if available and also legally permissible. The detailed information on the Core Data fields for law enforcement purposes will be provided as Annex to this document.

- Necessary 3rd step information exchange

All these possibilities of accelerated data supply for identification purposes should not restrict the necessary 3rd step information exchange, which takes place in practice. In such a 3rd step information exchange, further detailed and investigative information can and must be made available as before, either in classical police cooperation or in classical judicial administrative assistance. However, delivering such information is not as urgent as the initial identification and subsequent use of personal data of identified suspects. If need be, exchanging such information should be possible at any time in the future via classical police and judicial cooperation.

3.1.1 In-depth discussion of 2nd & 3rd step supply– meeting Lisbon

The results and proposals of the first meeting regarding three different parallel possibilities of standardized 'core data' transmissions and an unchanged possibility to exchange further non-standardized information in a third step on classical police communication channels were confirmed. National authorities are currently overloaded with work and have to wait days and weeks to receive data, which they might need to decide on how to process a case. To speed up the process and to optimize their cases, 'core data' could be provided to Member States after confirmed hits.

The 3rd step information supply belongs to classical police cooperation over communication channels and is not within the scope of Prüm.

3.2 No central data base solution on EU level

All suggestions of the study contractor towards a data storage of personal or case data on central servers of the EU (e.g. sBMS)1) were unanimously and strictly rejected by all experts because of legal as well as of forensic and organizational reasons related to work processes and quality requirements of international criminal police cooperation and crime scene stain processing. Such proposals would undoubtedly jeopardize the successful and well-functioning Prüm cooperation and cannot create any operational benefits.

---

1 Study on the Feasibility of Improving Information Exchange under the Prüm Decisions published on Workshop 27th March 2019 – Area 4 of this study

3.3 Web-Service

The current Prüm SMPT (e-mail) communication is considered to be very well functioning, both in AFIS and especially in the DNA communication area, and must absolutely remain functional without restrictions. Nevertheless, faster, more modern web solutions can be expected, especially in the AFIS or /and Face Recognition cooperation through the development of additional web services.

The focus group is therefore encouraging the parallel development of web services. With a view to the most possible uniform communication platforms and interoperability, such a solution is recommended for all types of forensic data transmission, including accelerated 2nd step information exchange in all these forms of cooperation. It is essential that no big bang implementation should take place here so as to not disrupt the ongoing and well-functioning real operation. An open protocol has to be used as a future protocol service, which allows all transmission protocols in parallel and in interaction. For example, depending on the different technical development status and possible national updates of the systems, SMTP-SMTP, SMTP-HTTP and also HTTP-SMTP protocols for data transmission between the test states should be possible. In order to be able to implement such a technology with the least administrative effort, the experts would also allow for the use of a central simple 'router' or simple 'massage broker' on a central EU platform (e.g. euLISA server platform).

Prüm FR as a new, presently not existing application should be developed exclusively as a Web service solution as from the beginning. In this regard, also note the explanations under point 8.1 – XML Format.

3.4 Central Data Router (eu-LISA) with encryption-management

The possibilities of a central router service were regarded as useful only if they can contribute to a simplification of the current bilateral encryption management. They would also help to ensure that Member States would not have to gradually interconnect bilaterally by exchanging encryption data, but would be immediately connected to all operational Member States when they were connected to such a central service. Such a central router solution would also open up improved central statistical analyses.

Some Member States are not able to share data without encryption; therefore a data transfer in an encryption manner is necessary.

For reasons of data protection, some participants emphasized that, when using a central router service on euLISA level, no decryption and possibility of using the transmitted sensitive criminal investigation data content should exist on the central router service level. Clean data should be decrypted exclusively by designated recipients.

From a technical point of view, some participants confirmed the benefits of a central data router solution. Especially in terms of technical efforts, in terms of key management, server-availability or statistical reports, a central solution could reduce costs on national side. However some participants voiced concerns related to data protection. The technical experts also agreed that there is no implicit need for a central router. Because of many remaining legal issues, this topic should be finally decided at political level. Experts of those Member States, which have a more neutral position on this question and may also accept a central router solution as a possible alternative, could only accept such a solution as a 'simple' message router and only if an EU agency (euLISA) would be entrusted with providing the responsible central router service and not a private company. Additionally, it has to be legally clear that such an entrusted EU agency would not be allowed to accede the very sensitive content of transmitted data and, furthermore, that the use of data would not be allowed for other purposes than technical and statistical support of Member States .

4 Quota Control / Number of Candidates / Response time

4.1 Quota control

Experts discussed whether image searches should be restricted by a daily quota system.

From a technical point of view, problems are only conceivable if the server is extremely overloaded. As a rule, FR searches are never technologically restricted and, similar to dactyloscopic stain searches, restrictions result only from the limited availability of forensic experts who have to assess and evaluate the results. According to the license models, FR systems are not modelled in a way that separate costs are incurred for search quantities. The license costs usually depend on the size of the reference databases. Therefore, as many searches as desired can be carried out without additional costs.

Experts suggested that taking into account possible other license models (based on database size and / or number of searches per timeframe), which could trigger additional costs in the requested countries, a quota control for maximum searches as it exists in the AFIS area should be technically provided for all three transaction types to be planned. Whether this quota control is also demanded and defined by the Member States is their responsibility and, as in the AFIS area, should always be fixed bilaterally with quota lists. Such desired maximum search numbers usually trigger reciprocal restrictions when they are requested.

4.2 Number of maximum candidates should be defined

The number of needed candidates depends on the quality of the images and different thresholds of the systems. The investigation of a serious a crime or a terrorist offence may make it necessary to check more candidates as in a usual image exchange over Prüm. Nevertheless, a maximum number of possible hit candidates should be fixed in the act (e.g. maximum 100 candidates).

The experts also discussed the likely event that the list of 100 candidates does not show 100 different persons. The problem is that persons are often stored in the reference databases with several face images linked to several crimes. These will all show up in the candidate list, providing little additional information – a candidate list of length 10 could, for example, only consist of images belonging to one individual. This could violate national procedures regarding the manual review of face recognition search results since the number of individuals by the search would be below what was requested. It might also influence the reviewer, making it more likely for him to confirm that the individual with the largest number of available images is the target.

However, implementing consolidated enrollment (a person centric database) could be challenging and should not be mandated. Therefore, two options for returning the results should be allowed:

a) The candidate list shall consist of different persons. In case, there are multiple images to one person, the image with the highest matching value and the last one taken should be presented. There shall be an indicator that multiple images are available.

b) If option a) is not possible, the candidate list should consist of all the images produced by the search without any kind of grouping or indicator that there are multiple images for some individuals.

4.3 Number of candidates could be reduced by definition

The possibility of flexible queries was discussed. On the one hand, a requesting Member State should have the possibility to choose, how much reference images should be provided (up to the maximum number of candidates). Depending on the quality of data in the reference databases, sometimes 10 or 20 images could be enough. It might, however, become inevitable to check more images in the case of bad quality or a serious crime investigation. This flexible solution allows the querying Member State to conduct an on-demand search according to its resources and to prevent a work-overload. On the other hand, the respondent MS should also have the possibility to define thresholds based on experience with the own national FR system (national outgoing data quality control) when positive 'match' candidates are no longer to be expected. This should limit the risk of providing candidates which can no longer be considered as possible 'hit' candidates.

Scaling of the desired candidates between 1 and 100 from the searching state should be possible. No differentiation is required between these scaling options in the three transaction types.

The study contractor proposed a fixed list of 50 candidates, which was discussed in the last meeting in Wiesbaden. The experts hold that the candidate list should be scalable. The requesting country may set the length (1-100 candidates) of the candidate list.

4.4 Possibility for different search transaction types should be fixed.

Requests of trace images against reference images, furthermore also reference images against trace images and/or trace images against trace images or also reference against references images should be optional, if partner states have the technical setup.

When a requesting country sends a trace image, every possible hit from every database which is able to be searched should be provided. The information about the image source should be connected as information to the provided candidates.

4.5 Technical details into an implementing act

Technical details, such as the number of provided candidates, should be fixed in implementing acts and not in the basic legal act. This will make it possible to react flexibly after an operative test period. Especially in face recognition, where data exchange on European level is a completely new development, adaptations and specifications will be essential.

4.6 Response time

Some Member States have implemented their national forensic FR business case with asynchronous data processing functionalities. In addition, some of them have implemented micro-matching solutions to rank the list of candidates and need the whole data set of all candidates from all requested countries. Therefore, a maximum time period should be set within which incoming search requests have to be processed and answered to the requesting country. The experts recommended that the processing of incoming searches should be guaranteed within max. 15 minutes. Older systems may need more time, but the data exchange could be faster in the future.

4.7 Upper-bound restriction of data size in total per transaction

However, it is necessary to restrict the size of files per data transmission with regard to the total size of transmittable images. This concerns the processing capability of the FR systems themselves for very large resolutions, but above all possible restrictions of the network system with maximum upper limits there.

5 Image Quality

5.1 Specific database for latent/trace images

Participants discussed the possibility to distinguish between mug shots, which have often ICAO quality standards, of identified persons and trace images of unidentified persons in the search.

According to the current state of knowledge, not a single Member State has already set up its own trace image databases with images of unknown perpetrators, which could be used regularly as a search data pool in addition to a reference picture data pool. However, some Member States are already planning to set up such a trace-image data pool of unidentified offenders.

The experts agreed that the search technology as well as the workflow processes of such FR searches are very similar to the forensic and technical framework and preconditions of dactyloscopic trace searches (LT-TP). The planned processes can therefore be tightly linked to these proven trace search technologies and Prüm dactyloscopic stain search processes.

Taking into account the further developments mentioned and already underway, the planning and facilitation of further search transaction type possibilities such as reference image - reference image searches or also trace image - trace image searches, should be possible. These transaction types would correspond to the transaction types TP-TP and LT-LT searches in the Prüm dactyloscopic cooperation.

See explanation at point 4.4 (needs of three transaction types).

5.2 Image Quality

Since the main objective of the cooperation will be the identification of unknown persons on the basis of mostly poor data quality search images, searches in the reference databases of the Prüm partners must be possible with poor image quality. However, it makes sense to restrict the number of possible hit candidates in a similar way to that used in LT/TP searches for dactyloscopic data. It seems essential here that those specifications are only fixed in an implementation act in order to be able to allow for quality adjustments in line with increasing experience and the state-of-the-art.

No minimum quality of forensic search images is required. Prüm procedures do not provide for data storage but only database search processes. Therefore, it should be allowed to transmit and process very poor trace image qualities to carry out comparisons.

No technical problems are to be expected. In the worst case, FR systems could at least provide NoHits, or, as is usual anyway, positive or false positive matches. In any case, this is better than generally rejecting the search and thus excluding clarification possibilities.

A common standard for the reference database and the possibility to split the databases in different quality areas as proposed by the study contractor has been discussed by experts as well.

The proposed standards are reference data standards with ICAO norms. The quality requirements for images in national identification systems, which will be used for police / forensic cases, are usually much higher than low quality ICAO norms. The ICAO norms apply for single images in ID-documents, whereas the images in the police reference databases are stored in a much higher resolution. Search images are not necessarily taken in controlled conditions hence a quality restriction for search images would be counterproductive.

It is the responsibility of the requesting country which actions may result from a delivered match candidate list, irrespective of the quality of the images in the candidate list.

Splitting the database in different qualities would require disproportionate technical effort and has no apparent added value. A definition of data quality for national FR databases should be out of the scope of an amended Prüm legislation

5.3 Quality-check algorithms

Changeable thresholds in the searched reference databases as a possibility to technically support the provision of the most target-oriented list of match candidates was also considered.

Such output restrictions in the requested database could become effective if, due to the detected threshold and the experience with such threshold values of the FR software solution used, a correct candidate provision can no longer be expected. Such thresholds could therefore be varied to minimize the risk of providing false positive matches.

5.4 Micro matcher solutions

The use of micro matcher solutions for the preparation / ranking of the incoming candidates according to their biometric probability of conformity with the algorithms of the own FR system is recommended, but should not be binding.

6 Possible roles of EU Agencies

6.1 Possible role of eu-LISA

euLISA should develop an implementation guide regarding technical topics. A benchmark test-set should be created and benchmark tests should be performed together with national experts. To that end, a Member States' expert Advisory Board within euLISA should be established.

6.2 Possible role of Europol

There is common understanding at expert level that Europol should be granted operational use of the Prüm system in the case of future face recognition comparisons. Such an option would enable Europol to carry out independent comparisons from technical and organizational point similar like a further additional 'Prüm State'.

Of course, it makes no sense that Europol checks the biometric data stored by Member States at Europol against national databases. Member States and their forensic experts, who have to prove with their expertise the results also in their courts, can do this check efficiently by means of the existing Prüm online access.

Nevertheless, Europol also receives biometric data from third countries - such as biometric data on suspected terrorists or internationally active criminals. It may make sense for Europol to be able to compare such data with the national reference data or with the central EU databases of the interoperability system, once they would have established own biometric systems and hired own forensic experts for such data processing.

Granting Europol direct access rights to Member States' databases for the purpose of checking such data against the national databases is not a question that can finally be answered by the expert group. It is a political and legal question which must be assessed by the Member States, European Parliament and also by Europol itself. Of course, it would also have to be ensured that follow-up personal and case information data would never be sent from Europol to third countries without the prior information and consent of the Member States whose data would be concerned.

7 Verification

7.1 Human intervention for forensic confirmation and core data exchange

National and EU legislation regarding data exchange provide for expert verification. Human intervention is needed before any follow-up data exchange (even core data exchange) can be started. This is a data protection requirements. In accordance with national legislation, every Member State should designate experts on national level. Experts could be located in different organization units of the requesting Member State. For possible follow-up data provision after human verification see the explanations above.

8 Data format

Technical formats for communication platforms should be harmonized. One File Format for all data types maybe split over different verification processes. The use of a standard format should not change the whole Prüm system. Therefore, no complex changes in the national systems are needed.

8.1 Web Service / XML Format

Seeing the architecture as a common approach for the exchange of data in all 3 fields, web service might be the preferred solution. Also from a security perspective, web service should be the technical architecture for future new and updated implementations.

8.2 Data format of images– discussion meeting Lisbon

The most common data formats for images are Joint Photographic Experts Group (JPG), Tagged Interchange File Format (TIFF), Windows Bitmap (BMP), Graphics Interchange Format (GIF) and Portable Network Graphics (PNG). For the exchange over face recognition BMP and GIF have to low quality. Raw images provide the most information, which could be useful for 1:1 face comparisons, but this data format creates transfer problems because of the huge data amount. These possible formats are not used in all states. Instead, standardization of different formats on national level after conversion from other formats for the storage and also processing take place. The most common and best format in all countries is JPG.

In order to enable automated Prüm search processes, a single format must be defined in any case. This format should be JPG. Every conversion process brings a slight deterioration in quality. Cut-outs of trace images with more people also reduce the quality, but for the automatic comparison only cut-outs of the search face should be transferred so that the system focus on the right person. For the preparation of expert opinions, the use of the original format could be necessary. Data transfer for such individual cases should only be carried out in the classical police and justice cooperation data exchange and therefore does not have to be considered in the technical planning of the online comparison.

Additionally, technical solutions developed by euLISA for the implementation of the interoperability Regulations will be taken into account if feasible for the Prüm.ng system.

8.3 Metadata

Pre-binning (e.g. gender, regions etc.) can be initiated at national level when it is necessary to limit the available data pool of hits. It was noted that such metadata restrictions are already very error-prone at national level. At Prüm level, such metadata restrictions would make no sense at all. Regional or national searches were already carried out in advance before a Prüm search would be started.

After inclusion of further photo data sets of Prüm partner states, the extended reference data pool should be used as extensively as possible should be searched as much as possible cross-border searches in case of negative search results at national level.

Metadata restrictions would also trigger major system architectural problems, as each state would use different metadata restrictions. The search basis is therefore exclusively the image information and the search should only be based on this factor.

Therefore, no metadata restrictions should be planned for Prüm FR comparisons.

9 ANNEX

2nd Step Core Data / REFERENCE DATABASE / All Biometric Data Types

- **Alphanumeric Personal Data**
  - Family name (m)
  - First name (m)
  - Name of birth
  - Former names
  - Date of birth (m)
  - Place and country of birth (m)
  - Gender (m)
  - Nationality
  - Alias/Nickname
  - Status of identity (Identity confirmed or not)
  - Further identity information (e.g. description, marks, tattoos)
  - CRN – Criminal Reference Number
  - National Identification Number
  - Address/Contact Information
  - First name of parents

- **Information of biometrics acquisition (Face Image, dactyloscopic data, DNA-Profile)**
  - Date of biometric acquisition
  - Place of biometric acquisition
  - Reason of biometric acquisition (e.g. type of crime etc.)
  - Source of biometric (Database)
  - File number (s)
  - Responsible authority

- **Additional Biometric data information (depends on request)**
  - Additional Face Images
  - Dactyloscopic data
  - DNA available yes/no/unknown
  - DNA – Profile (match report after DNA-Hit)
  - Information on additional DNA data (e.g. Y-DNA, mt-DNA etc.)
  - DNA-Kit Information
  - EN/ ISO 17025 accreditation status

- **Identity documents (**e.g. number, type of document, issued authority, scan/image of document**)**

- **Other data**
  - Technical information (e.g. hash-value etc.)
  - Alert information (e.g. arrest warrant etc.)
  - Warning information (e.g. weapons, twins etc.)
  - Prior convictions
  - Free text

2nd Step Core Data / LATENT / All Biometric Data Types

- Date of biometric acquisition
- Place of biometric acquisition
- Reason of biometrics acquisition (e.g. crime, dead body)
- Source of biometrics (database)
- File number
- Responsible authority
- Free text

Additional Biometric data information (depends on request)

- Additional Face Images
- Dactyloscopic data
- DNA available yes/no/unknown
- DNA – Profile (Match report after DNA-Hit)
- Information on additional DNA data (e.g. Y-DNA, mt-DNA etc.)
- DNA-Kit Information
- EN/ ISO 17025 accreditation status