PRIVACY NOTICE
CONCERNING THE DATA PROCESSING
BY THE HUNGARIAN NATIONAL DATA PROTECTION AND FREEDOM OF INFORMATION AUTHORITY FOR THE PERFORMANCE OF OFFICIAL TASKS RELATED TO EU IT SYSTEMS (SIS, VIS, EURODAC, EUROPOL, TFTP) IN THE AREA OF JUSTICE AND HOME AFFAIRS

1. Designation of the controller

National Data Protection and Freedom of Information Authority (Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH; hereinafter: 'the Authority' or 'the NAIH')
Headquarters: 1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.
Telephone: 36 (1) 391-1400
Fax: 36 (1) 391-1410
E-mail address: ugyfelszolgalat@naih.hu

2. Name and contact details of the Data Protection Officer

The Authority's Data Protection Officer: Dr. Attila KISS
Direct contact: e-mail: dpo@naih.hu; telephone number: 36 (1) 391-1470.

3. Purpose of Data Processing

The purpose of data processing is to perform the official tasks related to the enforcement of the personal data protection requirements of the Authority as defined in the following legislative acts:

a) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II);
b) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);
c) Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System and the Government and amendment of other related law enforcement Acts and the Magyary Streamlining Programme;
d) Government Decree No. 15/2013. (28/I) on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System;
e) Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention;
f) Council Decision of 6 April 2009 establishing the European Police Office (Europol);
g) 2010/411/: Council Decision of 28 June 2010 on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program;
h) Section 38 (4) e) of Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter: 'the Privacy Act').

After the completion of the cases subject to individual procedures, data shall be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with—the provisions of Act LXVI of 1995 on public deeds, archives and protection of material private archives (hereinafter: 'the Archiving Act' with regard to preserving recording public deeds—Article 89 of the GDPR.

Brief descriptions of the specific data processing activities supervised by the Authority in accordance with the above legislative acts is included Annexes 1-4 of this Notice.

4. The Legal basis of data processing

The processing of data is based on Article 6 (1) (e) of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: 'the GDPR')[1], and is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Authority in view of the legislative provisions listed in point 3. Data processing related to the performance of these tasks and the exercise of competences shall be subject to the following legal provisions:

- Section 71 of the Privacy Act (in the course of its procedure, the Authority shall be entitled to process, to the extent and for the duration necessary for the procedure, personal data, as well as data that qualify as secrets protected by an Act and secrets obtained in the course of professional activities, which are related to the given procedure or which have to be processed for the purpose of concluding the procedure effectively);
- Section 27 (2) and 33–34 of Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: 'Code of Administrative Procedure') with regard to authority procedures;
- Sections 4 and 9 of the Archiving Act;
- Sections 10 and 13 Act CLV of 2009 on the protection of classified information (hereinafter: 'the Classification Act').

5. The scope and source of data processed provided to the Authority not by the data subject

- The **natural identification data** of the party or any other participants if provided to the Authority not by the party;
- Depending on the nature and subject matter of the case, other **personal data necessary to clarify its facts** including the **personal data of vulnerable natural persons** for the purposes of the GDPR, and **special data** under Article 9 (1) of the GDPR and **criminal personal data** under Article 10 of the GDPR.

When not made available to the Authority by the data subject, personal data may come to the knowledge of the Authority from the following sources:

• **The applicant, notifier or complainant**: the Authority processes, in addition to the personal data necessary to identify the person initiating the procedure, the personal data he or she voluntarily provides;

• **The Personal Data and Address Register maintained by the Ministry of the Interior**: if the Authority requires a statement in order to successfully conduct a procedure, but the person concerned is not available at the contact address available to the Authority, it may request the data from the Personal Data and Address Register;

• **The data controller or processor subjected to a procedure**:

- the Authority may need to know what personal data the controller processes in order to carry out its procedure. It may then require the controller to provide information of the data or to send a copy of the documents containing personal data to the Authority;

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

- in order to clarify the facts of a case and ensure the success of its procedures, the Authority may copy all or any part of the records kept by data controllers and copy or seize data carriers with personal data;

• **Other persons requested to assist, other participants in the procedure**:

- the Authority may request information from the persons or organs requested to assist to the extent necessary; in this regard, it shall process:
- the personal data necessary to identify the individual involved in the procedure (party, representative, witness, holder of the object of the inspection, others requested to assist), the personal data contained in evidence (data carriers) provided upon request by the Authority or voluntarily ;

• **The Data Protection Authority of another Member State**: where the complaint is not filed in Hungary, but the controller has its main establishment or single establishment in Hungary and the decision on the data processing objected to took place in the main establishment or single establishment of the controller, the Authority shall proceed as the lead supervisory authority. In such cases, the authority which the complaint was filed shall with shall send any documents and information, including personal data, necessary for conducting procedures.

6. The recipients, or categories of recipients, of personal data

6.1. With regard to the personal data contained in the files in the context of records management:

- **Hungarian National Archives** (Magyar Nemzeti Levéltár; Postal Address: 1250 Budapest, Pf. 3; Address: 1014 Budapest, Bécsi kapu tér 2-4.) (Hereinafter: MNL): the documents of cases that may not be selected for destruction in accordance with the Authority's records management policy and archiving plan shall be handed over to the MNL.

6.2. In relation to the disclosure of documents and the data necessary thereto:

- In the course of the given procedure, the Authority shall communicate data to **Magyar Posta Zrt.** ('the Post Office'; seat: 1138 Budapest, Dunavirág utca 2–6.) in the framework of communication with parties;
- the Authority shall provide data to **NISZ Nemzeti Infokommunikációs Szolgáltató Zrt** (seat: 1081 Budapest, Csokonai u. 3.) in the framework of electronic communication with parties (in case of regulated and central electronic administration services);
- **DotRoll Kft.** (seat: 1148 Budapest, Fogarasi út 3-5.) shall be involved as the data processor in connection with the data transmitted by the Authority through its electronic mail system.

6.3. In addition, the Authority shall exceptionally, in individual cases, communicate personal data to other organs that are not recipients within the meaning of Article 4 (9) of the GDPR for the sole purpose of conducting its own or another organ's public authority procedure. Typically such organs include:

- **The party subjected to data protection/data classification review procedure**: in the course of exercising its right of access, the party may, as required by law, become aware of personal data that has not been classified or protected as a secret. With regard to classified data, the rules of access shall be governed by the provisions of the act on the protection of classified information, according to which the right of access shall be granted by the classifier to the data subject[2].

[2] Based on Article 11 of 'the Classification Act.

- **Organs, persons, authorities and persons required during the procedure**: Where an authority, organ or person is required to assist in clarifying the facts or making a decision in the course of the procedure, the Authority may communicate personal data to the extent strictly necessary for the execution of the request to:
  - the Hungarian authority, organ, person or supervisory authority of another EU Member State under the GDPR required;
  - the supervisory authority of another EU Member State, the European Data Protection Board (hereinafter: 'the Board'), the Secretariat of the Board and the Commission of the European Union in procedures under Articles 56 and 60–65 of the GDPR;
  - the data controller and data processor examined in the given procedure or the recipient of the data transfer;
  - any other organ or person required.
- **Other Hungarian authorities with material and territorial competence**: if considering a request filed with the Authority receives falls within the competence another authority, the Authority shall transfer the case including personal data to that authority in accordance with Section 17 of the Code of Administrative Procedure.
- **Courts proceeding**: the court proceeding in actions related to the public administration activities of the Authority or initiated pursuant to Article 64 the Privacy Act may have access to and process the personal data in the documents of the action in accordance with the rules of procedure applicable to that case. In administrative actions against decisions of the Authority, the Authority shall submit the documents of the administrative case to the court together with the application submitted to it pursuant to Section 40 (1) of Act I of 2017 on the Code of Administrative Court Procedure.
- The **National Tax and Customs Administration of Hungary's** (hereinafter: 'the NTCA') competent directorate: if the party in a data protection procedure has failed to meet his or her payment obligations—procedural or data protection fines, procedural costs—under the final decision of the Authority, and so the Authority has ordered enforcement, the Authority shall request the NTCA to recover the monetary claim under Section 134 (1) of the Code of Administrative Procedure and Section 61 (7) of the Privacy Act. To the extent necessary and appropriate to comply with this request, the Authority shall transmit personal data to the NTCA.
- **Investigating authority**: if an investigating authority requests the Authority to transmit documents for investigation purposes, the Authority shall be obliged to provide them including the personal data therein.

In the event that, in the course of its procedures, the Authority has a well-founded suspicion of a criminal offence or an infraction and therefore it initiates criminal proceedings before the organ entitled to commence criminal or infraction proceedings under Section 70 of the Privacy Act, it shall forward the file including personal data necessary for submitting the report to the competent investigating authority.

7. Duration of storage of personal data

The Authority shall file the documents of a case in accordance with the legal requirements of the public service records management[3] and shall process them among the filed documents until selection for destruction as specified in the applicable filing plan or, failing that, until archiving. For archiving purposes, the Authority shall process the data along with

[3] Government Decree 335/2005 (XII. 29.) on the general requirements of public-service records management.

documents until selection for destruction or archiving. Thereafter, the Authority shall erase data (destroy documents), except for the data in documents to be transferred to the archives under the Archiving Act and in the personal data kept in the filing system under law, and the processing of the data shall cease with the transfer to the archive.

8. Rights of the data subject regarding data processing

8.1. Deadline

The Authority shall comply with a request for the exercise of the rights of the data subject within one month of receipt. The date of receipt of the request is not included in the deadline. The Authority may, if necessary, extend this time limit by a further two months, taking into account the complexity of the request and the number of requests received. The Authority shall inform the data subject of the extension of the time limit, indicating the reasons for the delay, within one month of receipt of the request.

8.2. Data subject rights concerning data processing

8.2.1. Right of access

The data subject shall have the right to request information from the Authority, through the contact details set out in point 1, whether his or her personal data are being processed, and, where that is the case, to know:

- what personal data,
- on what legal basis,
- for what purposes, and
- what period of time

the Authority is processing;
furthermore
• to whom, when, under what law, what personal data of his or hers the Authority has granted access, or to whom it has transferred personal data;
• from what source the Authority obtained his or her personal data (if not provided to the Authority by the data subject);
• whether the Authority applies automated decision-making as well as profiling and what its logic is. The Authority shall make available at the request of the data subject a copy of the personal data undergoing processing free of charge for the first time; thereafter it may charge a reasonable fee based on administrative costs.
In order to meet the data security requirements and protect the rights of the data subject, the Authority is required to verify the identity of the data subject and the person wishing to exercise his or her right of access; in order to ensure that, the provision of information and access to data, as well as issuing the copies thereof to the person concerned, shall be conditional on verifying his or her identity.

8.2.2. Right to rectification

The data subject may, through the contact details set out in point 1, request the Authority to rectify his or her personal data. Where the data subject can credibly demonstrate the accuracy of the rectified data, the Authority shall comply with the request within a maximum period of one month and shall inform the data subject through the contact details provided.

8.2.3. The right to block (restrict data processing)

The data subject may, through the contact details set out in point 1, request that the processing of his or her personal data to be restricted by the Authority (by clearly indicating

the limited nature of the data processing and by ensuring separate processing of other data) where:

- the accuracy of the personal data is contested by the data subject (in which case the Authority shall restrict the processing of the data for a period enabling it to verify the accuracy of the personal data);
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing (in this case restriction shall be for a period required verify whether the legitimate grounds of the controller override those of the data subject).

In an authority procedure in addition to the above, as per Section 28 of the Code of Administrative Procedure, where justified, the Authority shall, upon application or ex officio, order the confidential processing of the natural identification data and address of the party and other participants in the procedure if they may suffer seriously detrimental consequences due to their participation in the procedure; and, according to Section of the Code of Administrative Procedure, the Authority may, in order to protect the rights and interests of minors, adults having no or partially limited capacity to act, where any of the above is a party, witness, holder of the object of the inspection or a person under surveillance, order, even in the absence of such an application, the confidential processing of the data of the person affected and the restriction of the right to inspect documents.

8.2.4. Right to object

Through the contact details set out in section 1, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her if, in his or her opinion, the Authority processed his or her personal data inappropriately with regard to the purpose set forth in this privacy notice. In this case, the Authority shall demonstrate the compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

8.2.5. Right to erasure

With regard to the data processing described in this notice the data subject may exercise his or her right to erasure only if the data are not required for the exercise of the official authority vested in the Authority or for the performance of the Authority's tasks in the public interest. With regard to documents to be transferred to the archive, the erasure of data cannot be made without harming the integrity of the documents, and therefore a request for erasure in this respect cannot be fulfilled.

9. Right of remedy

If the data subject considers that the Authority has breached applicable data protection requirements when processing his or her personal data, he or she may lodge a complaint with the Authority (National Data Protection and Freedom of Information Authority, address: 1055 Budapest, Falk Miksa utca 9-11., postal address: 1363 Budapest, Pf. 9. E-mail: ugyfelszolgalat@naih.hu, website: www.naih .com), or may go to court to protect his or her data, and the court shall hear such cases as a matter of priority. In this case, the data

subject may bring the action before the regional court having territorial jurisdiction over his domicile (permanent address) or place of residence (temporary address), or the seat of the Authority, according to his choice. The regional court having territorial jurisdiction over the data subject's domicile or place of residence can be found at http://birosag.hu/ugyfelk relationship-portal/birosag-kereso. According to the seat of the Authority, the Budapest-Capital Regional Court has jurisdiction over the lawsuit.

Annex 1
Notice on the Schengen Information System (SIS)
http://naih.hu/schengeni-informacios-rendszer.html

1) The Schengen Area

It is one of the main achievements of the EU enabling the free movement of persons, which was originally established in an inter-governmental agreement between five Member States. By now the Schengen Agreement establishing the Schengen Area and the Convention implementing that Agreement have become ow been incorporated into the body of rules governing the EU, which agreements all Member State with exception of Bulgaria, Croatia, Cyprus, Ireland, Romania and the United Kingdom, have acceded to, and which certain non-EU States, Iceland, Norway, Switzerland and Liechtenstein, also apply.

The so-called Schengen acquis essentially abolished the internal borders of the region and strengthens the protection and control of the external borders. To this end, Member States apply common rules on external border controls and short-stay visas, and implement close cooperation between their police and judicial authorities, and have set up the Schengen Information System (SIS).

The Schengen Information System (SIS)

The Schengen Information System (SIS) is the largest information system in Europe set up in order to manage the security risks arising from the abolition of internal borders and the tightening of the control of external borders, in particular through the means of efficient data sharing.
The IT system set up at EU level is made up of three parts: the central system, the national systems and the communication infrastructure. The central part of SIS II is operated by the eu-LISA Agency, while the national parts are operated by each Member State. In Hungary, this task is carried out by the *Ministry of the Interior Deputy State Secretariat for Registers' Management* (BM NYHÁT) as the national N.SIS II Office. Additional information related to alerts entered into the system is handled by the SIRENE Bureau at the National Police Headquarters.
The SIS contains tens of millions of alerts (warrants). Immediate and direct access to the system is available to all police officers at local level, as well as to other law enforcement authorities and officials requiring data in order to perform their duties of protecting lawful order and law enforcement. The SIRENE bureaus are primarily concerned with exchange of data relevant for Cooperation in Criminal Matters or co-ordinate cross-border operations . In the course of these activities, they provide additional information on alerts and coordinate appropriate action on alerts in the SIS.
The SIS processes data in the following categories:

- persons wanted for surrender or extradition on the basis of a European or international arrest warrant;
- persons subject to a ban on entry and stay in the Schengen States;

- missing persons;
- persons wanted for their participation in legal proceedings;
- persons and objects subject to targeted or covert control;
- documents, vehicles other objects specified in the legislation, which are to be seized or used as evidence.

Operating as of 9 April 2013, the second generation system (SIS II) is able to process biometric data (fingerprints, photos), to share information on new categories of data (stolen aircraft, ships, containers, securities), to link certain alerts (e.g. persons and vehicles) and to store and share a copy of the European Arrest Warrant. The legal background of the SIS is Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen Information System and the Government and amendment of other related law enforcement Acts and the Magyary Streamlining Programmed) and Government Decree No. 15/2013. (28/I) on the detailed procedures of the exchange of information in the framework of the second-generation Schengen Information System.

3) SIS control, data protection

The SISII operates on the basis of strict data protection rules, which are regularly monitored by the European Data Protection Supervisor and by the data protection authorities of the Member States, the National Data Protection and Freedom of Information Authority in Hungary. Access to data is also restricted, and only by law enforcement, border, customs, judicial, visa and vehicle registration authorities may access them to the extent necessary and proportionate for the purposes set out in the EU Regulation and national laws.

In accordance with EU and Hungarian law, each person has the right to:

- to request access data related to him or her stored in the SIS;
- request that inaccurate or false data is corrected, rectified;
- request the erasure of data unlawfully processed;
- turn to the courts or other competent authorities for the protection of his or her personal dat rights.

The rights described above may be exercised by data subjects in any of the Schengen Member States. The examination of the lawfulness of data entered in the SIS shall be carried out in accordance with the national law of the Member State to which the request is made. Where the data was entered in the SIS by an authority of another Schengen State, the supervision shall be closely coordinated between the supervisory authorities of the two States concerned.

If anyone wishes to be informed whether his or her data are processed in the SIS, or he or she wishes to have the data processed in the SIS rectified or erased, he or she may submit a request to any government office, police station or Hungarian foreign representation by completing the standard form. Requests shall be dealt with at first instance by the SIRENE Bureau, which may, if justified, refuse to provide the information requested, but shall inform the applicant of the fact and the legal basis thereof. The decision of the SIRENE Bureau may be appealed against with the National Data Protection and Freedom of Information Authority.

Please click on this text for further information on the right to access personal data stored in the SIS.

In addition or instead, the citizen may, in accordance with the relevant legislation, have recourse to a civil court for the determination of unlawful data processing and for compensation for any resulting damage. The form for requesting data under Section 26 of Act CLXXXI of 2012 on the exchange of information in the framework of the second-generation Schengen

Information System and the Government and amendment of other related law enforcement Acts and the Magyary Streamlining Programme can be accessed on the following link: [click].

Annex 2

Notice *Visa Information System* (*VIS*)

https://naih.hu/vizuminformacios-rendszer--vis-.html

Established by Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (hereinafter: 'the VIS Regulation', the VIS is an IT system facilitating the exchange of data related to short-stay visas. The system stores data on short-stay visas issued by the Member States of the European Union and associated countries applying the common visa policy, facilitating the examination of applications for short-stay visas and the extension, revocation or cancellation of visas, the fight against visa fraud and abuse, checks on visas, and checks and identification of visa applicants and visa holders.

Access to the VIS for entering data is reserved exclusively to the duly authorised national authorities, and they must ensure that the use of VIS data is limited to that which is necessary, appropriate and proportionate for carrying out their tasks. They must also ensure that visa applicants or visa holders are not discriminated against and that their human dignity and integrity are respected in the use of the VIS. they not discriminate against applicants and visa holders, and that they fully respect the human dignity and the integrity of the applicant or of the visa holder.

In specific cases, national authorities and Europol may request access to data entered into the VIS for the purposes of preventing, detecting and investigating terrorist and criminal offences. Asylum authorities also have access to search the VIS on the basis fingerprints for the purpose of determining the EU State responsible for the examination of an asylum application and for examining an asylum application. Where the fingerprints of that person cannot be used or the search with the fingerprints fails, the search shall be carried out with the data referred to above.

Data processed in the VIS

If one applies for a visa from an EU Member State, the personal data given during the procedure will be added to the VIS by the national authorities. At given stages of the examination of the application, the following data required by the VIS Regulation will be added:

- Data under Article 9 of the VIS Regulation, which will be added when the visa application is lodged;
- Data under Article 10 of VIS Regulation will be added when a visa is issued;
- Data under Article 11 of the VIS Regulation will be added following the discontinuation of the examination of a visa application;
- Data under to Article 12 of the VIS Regulation will be added after a visa application has been refused;
- Data under Article 13 of the VIS Regulation will be added after a visa is revoked;
- Data under Article 14 of the VIS Regulation will be added after a visa is extended.

In summary, the data entered into the VIS allows the examining or proceeding authority to identify the details of the visa procedure (e.g. date, type of visa, etc.), as well as the applicant's name, the purpose of travel and stay, its duration, the photograph and fingerprints of the applicant.

Data is kept in the VIS for five years, but once the data subject acquires citizenship of any EU Member State, it is erased immediately.

The Rights of Persons

Visa authorities are obliged to inform the persons concerned of their rights and obligations in relation to the procedure. This information shall include as a minimum the identity and contact details of the controller responsible for processing the data, the purpose for which the data are processed in the VIS, the categories of data, the retention period, the right of access, the right of rectification and erasure.

In each Member State, the lawfulness of the processing of personal data by that Member State is supervised by the national data protection authority in accordance with Directive 95/46 / EC, which is carried out in Hungary by the National Data Protection and Freedom of Information Authority. The activities of the superisory authority shall be subject to the control of the European Data Protection Supervisor. In order to comprehensively enforce the data protection to be provided at the different levels, the so-called bodies, A Joint Coordinating Supervisory Authority has been established at EU level.

In accordance with EU and Hungarian data protection laws, individuals have the right to:

- receive, upon application, information on the data processed in the VIS
- request the correction or rectification of incorrect data
- request the erasure of unlawfully processed data
- turn to a court or data protection authority to protect their personal data rights and to recover damages resulting from their breach

Requests shall be submitted to a visa authority. The contact details of thee are available at http://www.kormany.hu/, and further information on further procedures can be requested at the Consular Service's central contact details:

Consular Service (Konzuli Szolgálat)

Cím: 1027 Budapest, Nagy Imre tér 4.

Telephone: 458-1000

Fax: 201-7323

E-mail: konz@mfa.gov.hu

The authority, if justified, may refuse to provide the information requested, but shall inform the applicant of the fact and the legal basis thereof. The decision of the authority may be appealed against with the National Data Protection and Freedom of Information Authority.

Annex 3

Notice on the EURODAC Sytsem

http://naih.hu/eurodac-rendszer.html

On 15 June 1990, the signatories to the Dublin Convention agreed to set up a system to prevent asylum seekers from submitting applications for asylum in several Member States.

The third generation of the Dublin Regulation, Regulation (EU) No 604/2013 of the European Parliament and of the Council (Dublin III Regulation), entered into force on 1 January 2014. This and its implementing regulation (Commission Implementing Regulation (EU) No 118/2014 of 30 January 2014 amending Regulation (EC) No 1560/2003) are the basis of the 'Dublin procedure'.

The range of states applying the Dublin procedure (32 European countries in all) is wider than the Schengen area and the European Union.

According to the principle of the Dublin Regulation the responsibility for examining an application for asylum shall lie with the Member State which played the biggest role in entering the „Dublin territory" of the asylum seeker either legally or illegally. However, the principle of family unity and wider range of rights granted for (unaccompanied) minors should be taken into account during the procedure.

The Dublin Regulation widely guarantees the right to information for the applicants. For proper information on the Dublin procedure the common leaflets drawn up by the European Commission and completed with additional Member State-specific information by the Member States shall be used. More information about the procedure can be found on the website of the Immigration and Asylum Office**.**

Since in most cases asylum seekers and irregular migrants do not possess valid travel documents or other appropriate documents to establish their identity, fingerprints constitute an important element in establishing the exact identity of such persons.

By *Council Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention* – which was replaced by the currently applicable *Regulation (EU) No 603/2013 of the European Parliament and the Council* on 20 July 2015 – the Member States created the so called Eurodac (EUROpean DActylographic Comparison) system. By the comparison of the fingerprints stored in the system Eurodac enables the countries applying the Dublin Regulation to determine whether a person staying illegally and/or applying for asylum in one of the countries of the "Dublin territory" has previously applied for asylum in another Member State or has entered the "Dublin territory" illegally. Based on the comparison of the fingerprints the Member States are able to determine which Member State is entitled and obliged to carry out the asylum or aliens policing procedure of the person concerned.

"Eurodac" consists of a Central Unit that was established within the European Commission and operates a computerised central database suitable for the comparison of fingerprints, and the electronic means of data transmission between the Member States and the central system.

What kind of data are collected?

The data stored into the Eurodac database depends on the data subject, of which there are three categories:

- **Category 1:** asylum seekers;
- **Category 2:** persons apprehended in connection with the irregular crossing of an **external** border of the "Dublin territory" and were not turned back;
- **Category 3:** persons found illegally present in a Member State.

1. Data collected on asylum seekers (over 14 years old)

- fingerprint data;

- Member State of origin, place and date of the application for international protection;
- sex;
- reference number used by the Member State of origin;
- date on which the fingerprints were taken;
- date on which the data were transmitted to the central system;
- operator user ID.

These data are stored in the system for ten years, and then they are automatically erased. If an asylum seeker acquires the citizenship of any Member State the data shall be erased immediately.

If a Member State grants **international protection** (refugee status or subsidiary protection) to an asylum seeker, his/her data shall be marked in the central database based on the Member States' instructions. However, these data shall be made available for comparison for law enforcement purposes for a period of three more years.

2. Data collected on persons apprehended in connection with the irregular crossing of an external border (over 14 years old)

- fingerprint data;
- Member State of origin, place and date of the apprehension;
- sex;
- reference number used by the Member State of origin;
- date on which the fingerprints were taken;
- date on which the data were transmitted to the central system;
- operator user ID.

Data can only be recorded and processed in the system if the data subject is over 14 years old and he/she was not turned back. These data are stored in the system for 18 months, unless the data subject has acquired the citizenship of any Member State, has been issued with a residence document by a Member State or has left the territory of the Member States. In these cases data shall be erased from the system as soon as possible.

3. Data collected on persons found illegally staying in a Member State (over 14 years old)

- fingerprint data;
- reference number used by the Member State of origin.

In this case the aim of recording and transmitting data can only be to check whether the person concerned has previously lodged an application for asylum in another Member State(s), and if so, when. These data are not stored in the system.

Fingerprinting and data transmission

The list of designated authorities which have access to data recorded in the central system of Eurodac for the purpose of facilitate the effective application of the Dublin Regulation.

In Hungary, the fingerprints of asylum seekers are taken by the Immigration and Asylum Office; the fingerprints of persons apprehended in connection with the irregular crossing of an external border (external Hungarian borderlines of the "Dublin territory" are the Hungarian-Serbian and the Hungarian-Ukrainian borderlines) and are not turned back are taken by the Police; the fingerprints of persons found illegally staying in Hungary are taken by the Immigration and Asylum Office or the Police.

The data processor is the Hungarian Institute for Forensic Sciences in respect of all three categories. The Institute is responsible for transmission of data to the Eurodac Central Unit, for receiving of data and for comparison of data.

In order to protect personal data, Member States which transmit data to the Eurodac system have to ensure that the procedure for taking fingerprints, and all operations relating to data process, data transmission, data storage or data erasure are lawful.

The data processing activities concerning Eurodac are supervised by the European Data Protection Supervisor in cooperation with the national supervisory authorities. In Hungary, the supervisory authority is the National Authority for Data Protection and Freedom of Information.

Access to Eurodac for law enforcement purposes

As a result of the efforts of the Hungarian presidency in 2011, the legitimacy and importance of Member States' needs to have access to Eurodac for law enforcement purposes was recognized by the European Commission in its communication on migration of 04 May 2011. This communication contained that the Common European Asylum System (CEAS) should have such a Eurodac database which continues to facilitate the effective application of the Dublin Regulation and at the same time – under very strict conditions – meets the needs of law enforcement authorities.

For **reasonable** law enforcement purposes, designated authorities of the Member States and the law enforcement agency of the European Union (Europol) may request the comparison of fingerprint data with the fingerprint data stored in the central system in order to establish the exact identity of the suspect or victim of a **terrorist offence or other serious criminal offence** and to obtain additional information about the person concerned. This excludes both the comparison of Eurodac data in relation to non-serious criminal offences and the systematic or mass comparison of data.

The requesting law enforcement authority receives a "hit/no hit" notification on whether the national asylum databases of the Member States contain any information about the person concerned. In case of positive result ("hit") further information about the person concerned can be requested in accordance with other legal provisions on exchange of information.

Hungarian authorities with access to Eurodac for law enforcement purposes

	NATIONAL ACCESS POINT	**VERIFYING AUTHORITY**
	Hungarian Institute for Forensic Sciences Dactyloscopy Department	**National Police Headquarters Directorate for Criminal Affairs**
Address	H-1087 Budapest, Mosonyi utca 9.	H-1139 Budapest, Teve utca 4-6.
Postal address	H-1903 Budapest, Pf. 314/4.	H-1903 Budapest, Pf. 314/15.
Telephone	+36-1-477-2161 +36-1-477-2150	+36-1-443-5500
Fax	+36-1-477-2185 +36-1-477-2196	+36-1-443-5569
E-mail	bszki@orfk.police.hu dachu@orfk.police.hu	bufoigtitk@orfk.police.hu
Web	http://www.bszki.hu	http://www.police.hu

DESIGNATED AUTHORITIES

	National Police Headquarters	National Tax and Customs Administration Directorate for Criminal Affairs	Counter Terrorism Centre
Address	H-1139 Budapest, Teve utca 4-6.	H-1122 Budapest Hajnóczy utca 7-9.	H-1101 Budapest, Zách utca 4.
Postal address	H-1903 Budapest, Pf. 314.	H-1525 Budapest, Pf. 52.	H-1903 Budapest, Pf. 314.
Telephone	+36-1-443-5500	+36-1-4568-110	+36-1-265-6200
Fax	+36-1-443-5733	+36-1-4568-148	+36-1-265-6209
E-mail	orfkvezeto@orfk.police.hu	bfoig @nav.gov.hu bun.elnokh@nav.gov.hu	tek@tek.gov.hu
Web	http://www.police.hu	http://en.nav.gov.hu/	http://tek.gov.hu

Rights of the data subject

Data subjects have the right to be informed on the identity of the data controller; on the purpose of the data processing; on who and for which purpose can access to their data; on how the right to information and to erasure and correction of data can be exercised. The information shall be provided for asylum applicants and for persons apprehended in connection with the irregular crossing of an external border at the time of fingerprinting and for persons found illegally staying in the territory of the Member State at the time of data transmission. For minors the information shall be provided in an age-appropriate manner. The common leaflets drawn up by the European Commission and completed with additional Member State-specific information by the Member States shall be used for providing adequate information on the procedure of taking fingerprints for the data subjects.

Every Member State is responsible for the processed and transmitted data and their quality and has to ensure that data processing comply with the relevant EU and national legislation.

If the authorities detect incorrect (e.g. false, inaccurate) data upon notification or ex officio, they shall take immediate action to correct the data while simultaneously informing the data subject. If during the proceeding initiated upon request the authority refuses to fulfil the request, the authority is obliged to inform the data subject about the reason for denial.

According to EU and Hungarian data protection provisions data subjects have the right to

- access Eurodac-stored information related to the person
- request that inaccurate or false data is corrected
- request the removal of its unlawfully processed data
- turn to the courts or another competent authority to request the correction or removal of inaccurate data or petition for compensatory damages

The request has to be lodged to the authority that carries/carried out the asylum or aliens policing procedure. (See: http://www.bmbah.hu and lt http://www.police.hu; Information can also be requested from the Central Office of the Immigration and Asylum Office and the General Directorate of Law Enforcement of the National Police Headquarters.)

	Immigration and Asylum Office	Nationa Police Headquarters Directorate for Criminal Affairs
Address	H-1117 Budapest, Budafoki út 60.	H-1139 Budapest, Teve utca 4-6.
Postal address	H-1903 Budapest, Pf. 314.	H-1903 Budapest, Pf. 314/15.
Telephone	+36-1-463-9100	+36-1-443-5553
Fax	+36-1-463-9169	+36-1-443-5733
E-mail	migracio@bah.b-m.hu	rendfoig@orfk.police.hu
Web	http://www.bmbah.hu	http://www.police.hu

The authority has the right to refuse requests but it is obliged to inform the person about the fact of and the reason for the refusal. The decision of the authority may be appealed against with the National Data Protection and Freedom of Information Authority.

Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the Eurodac Regulation is entitled to receive compensation from the Member State responsible for the damage suffered, except if that Member State proves that it is not responsible for the event giving rise to the damage.

Expected changes of the Eurodac system

The recent migration crisis conceived the need to establish a new system which can operate in crisis situations as well. In 2016 the European Commission put together a package of proposals to amend the Common European Asylum System and to reform the Eurodac system:

- Data relating to persons found illegally staying in a Member State would be stored as well. (Currently this data can only be compared with the data of asylum applicants stored in the system.)

- Beside of the fingerprints facial image as additional biometric identifier would be recorded and stored (long-term goal is the introduction of a facial recognition software), and the refusal of providing facial image or fingerprints would be sanctioned.

- Beside of the fingerprints personal data of the data subject such as the name(s), age, date of birth, nationality, other identity data and identity documents) would be stored in the system, and these data would be accessible in case of positive fingerprint or facial image result (“hit”).

- The age for taking fingerprints would be lowered from 14 to 6 years of age in order to identify unaccompanied minors and finding the families of children as soon as possible.

- The data retention period of asylum applicants remains the same at 10 years, but fingerprint data for illegally staying third-country nationals who do not claim asylum would be retained for 5 years (similar to the data retention period of the Visa Information System and the proposed data retention period for storing data in the to-be-established Entry/Exit System). Data would no longer be deleted for subjects who were granted a residence document by a Member State (in this case their data will be marked, so it may than be possible to pass back the person concerned to the Member State that issued the residence document) or left the territory of the Member States.

- Marked data of subjects who were granted international protection would be accessible for law enforcement purposes for a period of three years (there is no change), but this time limit would not be applicable in case of illegally staying persons who were granted a residence document by a Member State. For return purposes, the proposal amends the rules on sharing data with third countries, but it does not grant direct access to these for third countries.

Annex 4

Notice on the EUROPOL System

https://www.naih.hu/europol.html

Europol is the European Union's law enforcement agency whose main goal is to help achieve a safer Europe for the benefit of all EU citizens. It is done by assisting the European Union's Member States in their fight against serious international crime and terrorism.

Europol works closely with the criminal authorities of the 27 Member States of the European Union, as well as with the law enforcement agencies of the USA, Canada, Australia and Norway. As a result, Europol provides effective assistance to 13,500 cross-border investigations per year, mainly through its tools for data collection, analysis, sharing and coordination.

Europol also participates on a case-by-case basis in the work of the so-called Joint Investigation Teams, where it assists in the detection of crimes with specialized tools and information

In addition, Europol is assisted by some 145 liaison officers from Member States and partner countries, who maintain their offices at Europol's headquarters in The Hague, and promote faster and more efficient cooperation, personal contacts and the building of mutual trust.

Europol activities

Europol became fully operational on 1 July 1999, following the ratification by Member States of the Europol Convention. As of 1 January 2010, following the adoption of Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), replacing the Europol Convention, Europol became a full-fledged EU agency with a new legal framework and extended responsibilities.

Europol assists EU Member States in law enforcement activities, such as:

- illicit drug trafficking,
- terrorism,
- illegal immigrant smuggling, trafficking in human beings and sexual exploitation of children,
- counterfeiting and product piracy,
- money laundering,
- forgery of money and means of payment—Europol also acts as the Central Office for combating euro counterfeiting.

Europol's support to the Member States includes:

- facilitating the exchange of information and criminal intelligence between European law enforcement authorities through Europol's information and analysis systems and the Secure Information Exchange Network Application (SIENA),
- providing operational analysis and support to Member States' operations,
- drawing up strategic reports (e.g. threat assessments) and criminal analysis based on information and data from Member States or other sources or Europol,
- • providing expertise and technical support for investigations and operations within the EU, under the supervision and legal responsibility of the Member States concerned.

In addition, Europol also is active in promoting awareness of crime analysis and harmonization of investigative techniques in respect of organized crime at an EU level. This is supported by the Europol Information System (EIS), Europol's central criminal information and intelligence database. The purpose of the system is to link the ongoing investigations in the Member States in the case of serious criminal offenses (sanctionable with at least five years in prison according to the Hungarian Criminal Code) involving at least two Member States under the mandate of Europol, thereby orientating and supporting the operation and operational activities of national law enforcement agencies.

The practical benefit of EIS is that it can be used to determine whether other Europol Member States have information related to the domestic investigation in cases covered by Europol's mandate. In the event of a 'hit', the Member States' reporting authorities can contact each other via the national units and agree on the usability of the information. In Hungary, the Europol National Unit is located at the International Criminal Cooperation Centre (ORFK NEBEK Office) of the National Police Headquarters.

Control of Europol, Data Protection

Europol processes a vast amount of sensitive data about citizens and must ensure the personality rights of individuals when using these data. To supervise this, the Joint Supervisory Body (JSB) was set up. As a safeguard, Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), which set up both Europol and the Joint Supervisory Body (JSB), contains a number of provisions relating to personal data protection. The main task of the JSB is to ensure Europol complies with these data protection provisions. The Joint Supervisory Body, as an independent body, is made up of members seconded by the data protection authorities of the Member States, and its main task is to ensure that Europol complies with the data protection principles. In Hungary, as of 1 January 2012, the National Data Protection Authority has been carrying out the tasks of the national data protection authority.

The JSB is charged with reviewing Europol's activities to ensure that the rights of the individual are not violated by the storage, processing and use of the data held by Europol. One way in which the JSB fulfils this general task is by carrying out inspections of Europol.

Under the Europol Council Decision the JSB is also responsible for considering whether Europol is following the principles of data protection in a number of specific areas. These specific tasks include examining and commenting on the opening of specific analysis work files; monitoring the permissibility of the transmission of data originating from Europol; examining questions relating to implementation and interpretation in connection with Europol's activities as regards the processing and use of personal data; monitoring the transmission of personal data by Europol to Union institutions, bodies, offices and agencies, third bodies and non-Member States; and drawing up harmonized proposals for common solutions to existing problems.

The JSB is responsible for upholding the rights individuals have in relation to their personal information. This includes considering the appeals of individuals who have requested access to their information but who are not satisfied with Europol's response.

Persons' rights

According the Europol Council Decision:

- Under Article 30, a data subject is entitled to obtain information on whether his or her personal data are processed by Europol and to have such data communicated to him or her in an intelligible form, or checked.
- Under Article 31, a data subject shall have the right to ask Europol to correct or delete incorrect data concerning him or her.
- Under Article 33(2), a data subject shall have the right to request the national supervisory body to ensure that the input or communication to Europol of data concerning him or her in any form and the consultation of the data by the Member State concerned are lawful. (The request will be dealt with in accordance with the national law of the Member State in which they made the request.)

Moreover, data subjects have the right to ask the JSB, at reasonable intervals, to check whether the manner in which their personal data have been collected, stored, processed and used by Europol is lawful.

There is no charge for exercising these rights. A request should be made in writing to ORFK NEBEK Office, or in cases specified above to the NAIH. The request shall then be sent to Europol within one month of receipt. Europol is required to have fully dealt with a request within three months of receiving it.

However, Europol may refuse to provide such information to the extent that such refusal is necessary to:

- enable Europol to fulfil its tasks properly;
- protect security and public order in the Member States or to prevent crime;
- guarantee that any national investigation will not be jeopardised;
- protect the rights and freedoms of third parties.

When the applicability of an exemption is assessed, the interests of the person concerned shall be taken into account.

If one is not satisfied with Europol's decision, he or she may appeal to the JSB. He or she may refer the matter to the JSB if no response received to the request within three months. In case of a response by the ORFK NEBEK Office, an appeal may be lodged with the Authority, or it may be challenged before a court claiming remedy of damage inflicted through an unlawful data processing.

European Police Office (Europol)

Address: Eisenhowerlaan 73, NL-2517 KK The Hague, Netherland;

Tel: +31 70 302 50 00

Fax: +31 70 345 58 96

Web:https://www.europol.europa.eu/

Contacts: https://www.europol.europa.eu/content/page/inquiry-forms-209

Annex 5

The TFTP (Terrorist Finance Tracking Program) System

On the procedure for requesting information, rectification, erasure and blocking of personal data processed under the TFTP Agreement

General Information

The Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP Agreement) was signed by the parties on 28 June 2010, which aims to regulate, in the framework of an international agreement, the exchange of information between the European Union and the United States in the framework of the fight against terrorism. The agreement, which entered into force on 1 August 2010, has so far proved to be an effective tool for the authorities in the prevention of terrorist offenses, but according to the agreement, millions of financial data are processed and transmitted annually by the parties. Therefore, the TFTP Agreement, in accordance with EU and national rules, contains a number of data protection safeguards to protect the personal data of EU citizens. These include the right to information under Article 15 of the TFTP Agreement and the right to rectification, erasure and blocking under Article 16 thereof.

The procedure

Article 15 of the TFTP Agreement provides for EU citizens to request information on what personal data is being processed about them under the programme. In addition, according to Article 16 of the TFTP Agreement, data controllers may request the rectification, erasure and/or blocking of their data within the framework of the programme. However, under the TFTP Agreement, citizens may exercise these rights upon application to their national data protection authority, the National Data Protection and Freedom of Information Authority (NAIH) in Hungary, by completing the following forms and submitting annexes. The application will be forwarded by NAIH to the US Treasury Department, which is authorized to consider it.

Form A: For the purposes verifying personal identity, the form must be completed in full and signed. In addition, it is necessary to attach a copy of the applicant's driving license, passport, ID card, which contains his or her photo and signature. (List of documents acceptable to nationals of each Member State)

The above documents will be examined by NAIH for identity verification purposes, but shall NOT send them to the US Treasury Department, and shall retain them for 6 months from the end of the procedure, and then destroy them. (This procedure applies only to citizens of the European Union or to holders of valid residence permits issued by one of the Member States.)

Form B: Request for Information Pursuant to Article 15 of the TFTP Agreement. The form must be completed and signed in full.

Form C: Request for rectification, erasure or blocking under Article 16 of the TFTP Agreement. The form must be completed and signed in full.

Form D: Power of Attorney for NAIH to contact the US Treasury Department on behalf of the applicant and to process and transmit personal data related to the application. If the applicant

wishes to share other information or data with the NAIH and/or the US Treasury regarding the case, he may do so in a separate cover letter. He or she must also state in the letter whether NAIH may share these data with the US Treasury (without explicit power of attorney, the NAIH shall not share any data provided outside the forms with a third party).

Upon receipt of all annexes to the application, the NAIH shall transmit the B and/or C and D forms to the US Treasury Department and promptly notify the applicant of the latter's reply. However, due to the nature of the TFTP programme, the answer may be partial.