FREEDOMS

Under watchful eyes: biometrics, EU IT systems and fundamental rights

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

This report addresses matters related to the right to human dignity (Article 1), the right to integrity of the person (Article 3), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), the right to liberty and security of a person (Article 6), the respect for private and family life (Article 7), the protection of personal data (Article 8), the rights of the child (Article 24), the right to good administration (Article 41) and the right to an effective remedy (Article 47) falling under Titles I 'Dignity', II 'Freedoms', III 'Equality', V 'Citizens' Rights' and VI 'Justice' of the Charter of Fundamental Rights of the European Union.

Photo credit (cover & inside): © adobe.com

More information on the European Union is available on the internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2018

Print	ISBN 978-92-9491-924-3	doi:10.2811/29	TK-02-18-068-EN-C
PDF	ISBN 978-92-9491-925-0	doi:10.2811/136698	TK-02-18-068-EN-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Under watchful eyes: biometrics, EU IT systems and fundamental rights

Foreword

Europe's migration and security challenges have prompted the European Union (EU) to develop and enhance multiple large-scale information technology systems (IT systems). Such systems provide invaluable support to border management efforts, but also cause wide-ranging fundamental rights issues.

The persons affected – including both regular travellers and persons who may be in situations of vulnerability – typically do not fully understand the implications of the use of such systems. This report aims to at least partly fill this knowledge gap by analysing the fundamental rights implications of collecting, storing and using biometric and other data in EU IT systems in the area of asylum and migration. The findings are based on socio-legal research carried out by FRA in 2015-2016, which focused on three key instruments in this field, namely European Dactyloscopy (Eurodac), the Schengen Information System (SIS II), and the Visa Information System (VIS).

Legal, policy and technical developments are evolving rapidly. The European Commission has proposed amending the legal bases for Eurodac and SIS II, and is expected to propose amending VIS in 2018. In addition, four new IT systems are planned: the Entry-Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) and, most crucially, an IT system that seeks to ensure interoperability across existing and planned systems.

The EU Agency for Fundamental Rights has scrutinised various aspects of these developments, including in legal Opinions and other publications on Eurodac, ETIAS, interoperability and the treatment of persons being fingerprinted. This report complements these publications, as well as the opinions issued by the European Data Protection Supervisor, which focus on data protection. It adds a new layer to the analysis that combines fieldwork insights on the application of different EU IT systems and their use of biometrics in terms of key fundamental rights concerns.

The report highlights the importance of respect for the right to information and the obligation to respect human dignity when collecting biometric data. It analyses how the right to asylum and the rights of the child are affected. It also examines the reliability of the stored data; possibilities for persons to access, correct and delete the data; and the risk of unlawful access.

Michael O'Flaherty
Director

Country codes

Country code	Country
AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	Netherlands
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SK	Slovakia
SI	Slovenia
UK	United Kingdom

Acronyms list

AFIS	Automated fingerprint identification system
BCP	Border crossing points
CJEU	Court of Justice of the European Union (CJEU is also used for the time predating the entry into force of the Lisbon Treaty in December 2009)
Convention 108	Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
DAPIX	Council Working Party on Information Exchange and Data Protection
DMCP	Diplomatic missions and consular posts
EASO	European Asylum Support Office
ECHR	European Convention on Human Rights
ECRIS-TCN	European Criminal Records Information System
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry-Exit System
EU	European Union
eu-LISA	European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice
EUMS	EU Member States
Eurodac	European Dactyloscopy
ETIAS	European Travel Information and Authorisation System
FRA	European Union Agency for Fundamental Rights
FRANET	Network of Legal and Social Science Experts (FRA)
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
IT system	Information technology system
NGO	Non-governmental organisation
PNR	Passenger Name Record
SAC	Schengen Associated Countries
SIRENE	Supplementary Information Request at the National Entries
SIS II	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TDAWN	Travel Documents Associated with Notices
TFEU	Treaty on the Functioning of the EU
The Charter	EU Charter of Fundamental Rights
UNHCR	United Nations High Commissioner for Refugees
VIS	Visa Information System

Contents

Figures and tables

Key findings and FRA opinions

The information technology systems (IT systems) initially set up by the European Union (EU) for asylum- and migration-management are increasingly also serving internal security. Virtually all large-scale European IT systems have provisions allowing their use for immigration control and for fighting serious crime and terrorism. In the processing of data, these systems increasingly rely on biometric data – fingerprints and facial image. The biometric identifier serves to connect the individual to the information stored.

The impact of large-scale IT systems on fundamental rights remains largely unexplored territory. This report analyses how IT systems affect different rights enshrined in the Charter of Fundamental Rights of the European Union (Charter), both negatively and positively.

The use of IT systems entails both risks and opportunities for fundamental rights. IT systems can offer more robust and timely protection – for example, for missing children and victims and witnesses of crime – and can help prevent identity fraud and identity theft. At the same time, the weak position of the individuals whose data are stored in large-scale IT systems creates many fundamental rights challenges. They range from respect of human dignity when taking fingerprints and challenges in correcting or deleting inaccurate or unlawfully stored data to the risk of unlawful use and sharing of personal data with third parties. Based on FRA's research findings, this report presents suggestions – aimed at the EU and its Member States – on how to reduce the risk of IT systems undermining fundamental rights.

In the areas of asylum, borders and visa, the EU has set up three large-scale IT systems:

- SIS II – the Schengen Information System – to aid police and border checks;
- Eurodac – standing for European Dactyloscopy – to support the application of the Dublin Regulation;
- VIS – the Visa Information System – for visa processing.

Advanced plans exist to set up three new systems:

- EES – the Entry-Exit System for registering travel in and out of the EU (Regulation (EU) No. 2226/2017 already adopted);
- ETIAS – the European Travel Information and Authorisation System for conducting pre-border checks for visa-free travellers (European Commission proposal under negotiation);
- ECRIS-TCN – extending the European Criminal Records Information System to third-country nationals (European Commission proposal under negotiation).

At the end of 2017, the European Commission tabled legislative proposals to make these systems 'interoperable' by creating a common search portal. These proposals also suggest establishing a common identity repository (CIR) with core biographical data of persons whose data are stored in the different IT systems, and adding a multiple identity detector (MID) to create links between different identities of the same person stored in the CIR.

Providing information in an understandable and transparent manner

Article 5 (1) of the General Data Protection Regulation (GDPR) requires that third-country nationals are informed about the relevant aspects of their personal data being processed in a transparent, intelligible and easily understandable manner. FRA research found that authorities that collect personal data of asylum and visa applicants, as well as of migrants in an irregular situation, and then store these data in IT systems, find it challenging to provide information in an understandable manner. Rights holders are often not fully informed of all aspects of the data processing and have difficulties understanding the information they receive. This is particularly true when the information system at issue serves a number of purposes and processes. With interoperability, ensuring the right to information may become increasingly challenging.

Transparency about the purpose of fingerprinting encourages the persons concerned to cooperate with the authorities, thus preventing situations from escalating. Authorities often find it challenging to provide information covering all aspects of the processing of data of asylum applicants and apprehended migrants, as required by Article 29 of the Eurodac Regulation (Article 30 of the recast proposal), including the use of the data for the Dublin procedure and for investigations of serious crimes and terrorism. Challenges increase when fingerprints are collected in stressful situations. If authorities provide no or only limited information, asylum applicants and migrants in an irregular situation perceive EU Member States to be acting in a non-transparent manner, according to FRA research. This affects their willingness to cooperate with the authorities.

The European Commission carries out evaluations in Member States to assess the implementation of the Schengen *acquis*. Such 'Schengen evaluations' also cover large-scale IT systems. They are an important tool to ensure compliance with the duty to inform, which is included in the legal instruments of all the IT systems, although restrictions apply to certain data recorded in SIS II.

FRA opinion 1

The right to information must cover all purposes of the data processing in IT systems in the field of asylum and migration management, and must include information on how to exercise the right of access, correction and deletion. EU Member States should strengthen their efforts to provide information in an age- and gender-sensitive way, as well as in a culturally appropriate manner. Particularly in the context of processing biometric data for Eurodac, consideration could be given to complementing standard leaflets with short illustrative videos that inform people in an accessible way.

FRA opinion 2

EU Member States should foster a sense of transparency by providing information in full, covering all aspects of data processing in IT systems in the field of asylum and migration management. This may also positively influence people's willingness to cooperate. EU Member States should ensure systematic registration in Eurodac through effective information and counselling. This should be carried out individually as well as through outreach actions targeting asylum applicants and apprehended migrants – such as focus group discussions, information sessions and similar initiatives. Where the European Asylum Support Office (EASO) and Frontex support Member States in registering asylum seekers and migrants in an irregular situation in Eurodac, they should similarly provide effective information and counselling. If IT systems become interoperable, the European Commission – with the support of relevant Justice and Home Affairs (JHA) agencies – should develop tools and guidance to support EU Member States in ensuring full compliance with the right to information.

FRA opinion 3

When carrying out Schengen evaluations, the European Commission should systematically assess how Member States implement the right to information and whether it is effective. The assessment should look at whether the information given covers all purposes of the data processing, and how the person concerned can exercise his or her right of access, correction and deletion. In this context, visibility should be given in Schengen evaluation reports to good practices found in Member States.

Respecting human dignity when taking fingerprints

Biometric data must be collected in a manner that respects human dignity. Human dignity is inviolable and laid down in Article 1 of the Charter. It is the foundation for all fundamental rights in the Charter.

Individuals may be physically unable – due to disabilities for example – or unwilling to provide fingerprints. Although rare, asylum seekers and migrants in an irregular situation may refuse to provide fingerprints for Eurodac – a phenomenon which does not seem to occur in the context of VIS. People are reluctant to give their fingerprints for different reasons. Many do this to avoid being transferred, under the Dublin procedure, to an EU Member State in which they do not want to be. FRA's field-research also revealed, however, that some refuse out of fear that their biometrics will be shared with their country of origin. The willingness to provide fingerprints would increase if asylum seekers and migrants in an irregular situation felt treated fairly and had trust in the procedures, and if family re-unification under Dublin were to work smoothly.

According to FRA findings, disproportionate force has been used when fingerprinting asylum seekers and migrants in an irregular situation. Given the vulnerability of the people concerned and the obligation to use the least invasive means, it is difficult to imagine that using physical or psychological force solely to obtain fingerprints for Eurodac would be justified. To enforce the duty to provide fingerprints, EU Member States have in some cases also resorted to detention.

When the authorities have difficulties in taking fingerprints that meet set quality standards, they sometimes suspect the person of having injured his or her fingertips on purpose to avoid fingerprinting, as FRA research shows.

Fingerprinting often takes place in stressful situations – at night or following a large numbers of arrivals for example. In such situations, fingerprinting poses high demands on staff, increasing the risk of inappropriate police behaviour due to exhaustion or stress. This, in turn, may undermine the dignity of the person being fingerprinted. Fingerprinting persons in a vulnerable situation, including those with disabilities or those who have experienced gender-based violence, requires particular attention. According to FRA findings, however, training tends to focus on the technical aspects of fingerprinting, and less on the treatment of the persons being fingerprinted.

FRA opinion 4

Given that it entails a high risk of violating fundamental rights, EU Member States should avoid the use of physical or psychological force to address refusals to give fingerprints as observed for Eurodac. Where EASO and Frontex support Member States in registering asylum seekers and migrants in an irregular situation in Eurodac, they should similarly refrain from resorting to physical or psychological force to address such refusals.

Putting people under pressure to give their fingerprints must under no circumstances risk traumatisation or re-victimisation. Therefore, EU Member States should not coerce suspected victims of torture, victims of sexual or gender-based violence, victims of other serious crimes, or traumatised people, into giving fingerprints; nor should other people who are usually considered to be vulnerable be coerced into providing fingerprints. The FRA 2015 checklist to act in compliance with fundamental rights when obtaining fingerprints for Eurodac provides concrete guidance.

FRA opinion 5

Depriving individuals of liberty to pressure them into giving their fingerprints must remain an exceptional measure, respecting all requirements of EU law and the European Convention on Human Rights (ECHR). Before EU Member States resort to deprivation of liberty to obtain fingerprints, asylum applicants and migrants in an irregular situation must be provided with an effective opportunity to comply with the fingerprinting requirements.

FRA opinion 6

EU Member States should continue to train and issue guidance on the need to ensure full respect of the right to human dignity. Such training and guidance should be provided to their own staff as well as to staff of their service providers in charge of taking fingerprints. These measures should also focus on the treatment of vulnerable people, such as persons with disabilities and traumatised persons.

To reduce the risk of tensions, EU Member States should have sufficient well-trained staff for fingerprinting and avoid giving this task to police officers or border guards who apprehend persons entering the country in an irregular manner. Where relevant, Member States could consider setting up mobile fingerprinting units as this would reduce the risk of inappropriate police behaviour caused by exhaustion, stress and other factors.

Fingerprinting in a child-friendly and child-sensitive manner

Large-scale IT systems affect the rights of children in different ways. Article 24 of the Charter emphasises that the best interests of the child must be a primary consideration in all actions public authorities and private actors take concerning children. This also applies to fingerprinting. Field research shows limited efforts to inform children in a child-friendly and child-sensitive manner, in accordance with their age and maturity, although police and border guards often take extra time during the fingerprinting itself to adapt to the needs of the child. FRA research also points to allegations of incidents involving the use of force to fingerprint children. The risk of re-traumatisation for children is particularly apparent in such instances.

As a child grows, the accuracy of a biometric match diminishes. Taking young children's fingerprints affects the quality and reliability of future matches to those fingerprints. The risk of a wrong match increases when the fingerprints or facial images are compared more than five years after they were taken.

FRA opinion 7

EU Member States should never use force against children or deprive them of liberty to obtain their fingerprints. Officers should build up a relationship of trust with the child. Through internal guidance, instruction and training, EU Member States should ensure that children are fingerprinted in a child-friendly, as well as child- and gender-sensitive manner; that they are assisted by their parents (or guardians if they are unaccompanied); and that they are provided with child-friendly and child-sensitive information on the purpose and modalities of fingerprinting. Where EASO and Frontex support Member States in fingerprinting children, they should similarly, through such measures, build up a relationship of trust with the child.

To compensate for the decreasing reliability of fingerprints over time, EU Member States should ensure that matches based on biometric data collected from a child more than five years earlier are always subject to further careful verification by dactyloscopic experts, as well as checks against other available data.

Optimising the use of IT systems to trace missing children

Many unaccompanied or separated children who enter the EU subsequently go missing. Some of those missing may be subject to abuse and exploitation, including trafficking in human beings. IT systems could better support their protection, according to border guards interviewed. Interviewed experts pointed out, however, that the focus remains on perpetrators and that a more victim-centred approach would be needed.

Children avoid being registered or go missing for multiple reasons. These include lack of trust in family reunification under Dublin; fear of being prevented from reaching their intended destinations; and lengthy processing times for their asylum applications. Data processed on children could be used more effectively for child protection purposes. Interoperability may bring new opportunities to trace missing and abducted children, provided EU Member States more systematically create an SIS II alert when an unaccompanied child goes missing and referrals improve between police and child protection authorities.

FRA opinion 8

To support the detection of missing children or of child victims of trafficking in human beings, EU Member States need to record missing children systematically in SIS II. This requires functioning reporting mechanisms between reception centres and the police. To ensure that the data stored are used for child protection purposes – and not only for law enforcement – EU Member States need to put in place effective cooperation mechanisms between police and child protection authorities as well as guardians. This should be complemented by tailored training for practitioners who may encounter children at risk.

Ensuring that industry consults fundamental rights experts when designing new solutions

In technical terms, the state of the art of technology determines the options that the EU and its Member States have when creating new systems or improving existing ones. Industry and the scientific research community can play an important role in developing technical solutions that promote respect for fundamental rights, including the protection of personal data. They should continue to embed data protection by design and by default in the technical solutions they devise for IT systems.

FRA opinion 9

Whenever they fund research and development activities, the EU and its Member States should require contractors to involve experts on personal data protection and other fundamental rights. Scientific researchers and industry should pay attention to the effect of phenotypical characteristics, as well as age and gender, on the composition of test groups, to eliminate any risks of discriminatory outcomes of test results.

Strong safeguards to prevent unlawful access to data

The principle of purpose limitation – as mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the GDPR and Article 4 (1) (b) of the Police Directive – requires that personal data are processed only for specified purposes, which must be explicitly defined. By optimising the use of IT systems for combating irregular migration, as well as serious crimes and terrorism, there is a risk of function creep – meaning that the data may be used for purposes that were not initially envisaged. This risk is particularly high in the case of interoperability between IT systems.

Article 28 and Article 32 of the GDPR require EU institutions and EU Member States to take necessary measures to avoid that data are disclosed to, or accessed by, unauthorised persons or organs. Private actors, such as carriers, may in some instances access limited parts of the EES (Articles 13) and ETIAS (Article 39). If IT systems are made interoperable, personal data stored in one system will be used across all systems to ensure correct identification of a person. Ensuring purpose limitation in such scenarios is particularly challenging.

IT systems that include data on asylum applicants may be particularly attractive for hacking by oppressive regimes or persecuting agents. Strong data security safeguards must limit such risks.

FRA opinion 10

EU institutions and EU Member States need to put in place all reasonable safeguards to ensure that data stored in IT systems in the field of asylum and migration are not unlawfully accessed. As private actors will use some IT systems, effective firewalls must prevent them from seeing data they are not allowed to see.

EU institutions and EU Member States should monitor access to IT systems through log files. The log files should specify who accessed a particular system and for what purpose. National data protection authorities and the European Data Protection Supervisor (EDPS) should have access to log files on request. Authorities should only print and store hard copies of the data where doing so is duly justified, and adhere strictly to physical access control and retention rules.

The EU legislator and EU Member States must ensure that legislation on interoperable IT systems does not result in circumventing access rules included in the legal instruments establishing the individual IT systems.

Ensuring respect for the right to seek asylum

FRA research findings reveal that some people with injured fingertips are suspected of deception although they are not intentionally avoiding to provide fingerprints. A suspicion that a person wishes to deceive the authorities affects their right to asylum, protected under Article 18 of the Charter. The physical inability to provide fingerprints due to the texture of one's fingertips or a disability must not result in unequal treatment or discrimination prohibited by Articles 20 (equality before the law) and 21 (non-discrimination) of the Charter.

Many people seek to hide their identity when fleeing their country of origin to protect themselves. Others may be physically unable to obtain the documents necessary for legal entry, such as a passport and visa, when escaping conflict or persecution. Interpol runs two databases:

- one for stolen and lost travel documents, the Stolen and Lost Travel Documents (SLTD) database;
- one for individuals who are subject of an Interpol alert, the Interpol Travel Documents Associated with Notices (TDAWN) database.

Oppressive regimes may include information about political opponents in these Interpol databases to prevent them from leaving the country or to track their movements. These databases are to be included among the interoperable IT systems the EU is setting up.

Persons assessed to be in need of international protection but subject to an entry ban can still be issued a visa with limited territorial validity, according to Article 25 of the Visa Code. Such a visa allows them to cross the EU's external border and provides them with the possibility to seek safety.

FRA opinion 11

EU Member States should provide guidance to eligibility officers to ensure that the overall trustworthiness and credibility of asylum applicants is not undermined by an assumption that the inability to give fingerprints, or to only give low quality fingerprints, derives from an asylum applicant's unwillingness to provide fingerprints and a wish to hide their identity.

FRA opinion 12

EU Member State authorities should use information included in the Interpol databases on travel documents with caution. Records entered by third countries in the SLTD and TDAWN databases should always be carefully manually reviewed to avoid having such entries have an undue impact on the right to asylum.

Prohibiting the transfer of data to third countries

Article 18 of the Charter protects the right to asylum. Effective access to international protection also forms the basis of protection from *refoulement* as enshrined in Article 19 of the Charter and Article 78 of the Treaty on the Functioning of the EU.

Sharing personal data with third countries can lead to particular risks for persons in need of international protection. They or their families may be subject to retaliation measures, ranging from criminal sanctions upon return to persecution of family members. The legal instruments for the IT systems generally prohibit sharing information with third countries, which reveals that a person is, or has been, an applicant for international protection in the EU. In practice, such safeguards are not always systematically followed, FRA research shows.

Under certain conditions, and typically for return purposes, personal data stored in IT systems may be shared with third countries. To prevent harm, in the case of asylum applicants, information is normally only shared with the third country at the end of the asylum procedure. However, in specific circumstances this may also be done before the procedure is completed – for example, following rejection of the application by the administration but where an appeal to the court is still pending. Such an approach can put people at risk. Safeguards are required to avoid that such transfers endanger the safety of asylum applicants or of their family members.

At the same time, IT systems can also be used to confirm an asylum applicant's claimed identity, thus reducing the risk of a removal in violation of the principle of non-*refoulement*.

FRA opinion 13

EU Member States must take all necessary measures to prevent information that a third-country national has lodged a claim for international protection from being shared with third countries.

In case of rejected asylum applicants, EU Member States should in principle only share personal data with third-country authorities for the purpose of return when the claim has been rejected in the final instance and is no longer subject to review.

Evaluating carefully how access by law enforecement affects fundamental rights

All EU IT systems except for SIS II and ECRIS-TCN contain data on persons not suspected of having committed any crimes. Nevertheless, law enforcement authorities are allowed to access data stored in Eurodac, VIS, EES and ETIAS for the purposes of fighting serious crime and terrorism, provided they adhere to the safeguards specified in the legal instruments. One of these safeguards is the 'cascade system', which obliges EU Member States to first consult national databases that are directly linked to criminal investigations, and only then consult EU-level IT systems. When consulting EU IT systems, they must consult VIS before requesting access to Eurodac, because information on asylum applicants is particularly sensitive. This is to ensure that data sets on asylum applicants – a group particularly vulnerable to fundamental rights violations – are only consulted as a last resort.

Children's right to such protection and care which is necessary for their well-being, set out in Article 24 of the Charter, requires measures to prevent future stigmatisation of children for acts they have committed in the past. Article 40 of the Convention on the Rights of the Child requires giving special attention to the treatment of children alleged to have, or being accused of or recognised as having infringed the penal law. According to the Charter, the child's best interests must be a primary consideration (Article 24). Information on criminal records may have a disproportionate effect on the development of the child. In case of immigration-related offences, the criminal record could be the consequence of decisions taken by the child's parents.

FRA opinion 14

The EU and its Member States should carefully assess the fundamental rights impact of access by law enforcement to data stored in IT systems in the field of asylum and migration. These data systems typically concern people who are not suspected of having committed crimes. The EU legislator should ensure that any solution for allowing access to EU IT systems by law enforcement for the purposes of fighting serious crime and terrorism continues to require the police to first consult databases more directly linked to criminal investigations. This is best ensured through retaining the 'cascade system'. Any alternatives to the cascade system would need to achieve the same objective. This means that personal data not collected for purposes of criminal investigations should only be accessed by law enforcement, if the information necessary to fight serious crime and terrorism is not available in databases more directly linked to criminal investigations. This concerns especially persons who are particularly vulnerable, such as persons in need of protection.

FRA opinion 15

The EU and its Member States should consider either excluding from access by law enforcement information stored in ECRIS-TCN revealing that a child has a criminal record, or limiting the availability of this information to very serious crimes.

Applying apprehension policies in line with fundamental rights

In addition to serving their specific purposes, most IT systems also contribute to the control of irregular immigration. They may be consulted to find and apprehend migrants in an irregular situation. For example, the EES will produce a list of persons whose right to stay in the Schengen area has expired. This list of so-called 'overstayers' can be matched with other IT systems, which will be an easy exercise once systems are made interoperable.

FRA has previously highlighted that certain apprehension practices disproportionately affect fundamental rights of migrants in an irregular situation. Accordingly, FRA discouraged apprehensions near providers of essential services – such as schools or healthcare centres. Interoperability of information systems will make it more difficult for migrants in an irregular situation to report a crime to the police, either as victims or as witnesses, as the police will automatically see the person's irregular residence status and, in most cases, be obliged under national law to initiate return procedures. With an increased risk of apprehension, migrants in an irregular situation will be even more reluctant to approach the police, contributing to impunity for perpetrators.

FRA opinion 16

EU Member States are encouraged to continue to apply FRA's 2014 guidelines on the rights-compliant apprehension of migrants in an irregular situation, paying particular attention to new risks for migrants' fundamental rights that interoperability may create.

Improving data quality

Mistakes in the IT systems used in the field of asylum and migration management can have serious consequences for individuals. For example, the police may arrest a person or border guards may not let a person cross the border. In the case of asylum applicants, they may be suspected of having intentionally tried to provide a false identity, affecting the perceived trustworthiness of their whole asylum claim.

FRA research shows that EU IT systems contain inaccurate alphanumeric data, such as names or dates of birth, due to various reasons. According to the GDPR and Police Directive, EU Member States have the duty to verify the quality of personal data before they are made available to data users. Significant efforts are underway, including proposals to strengthen the role of eu-LISA in supporting Member States in improving data quality. Nevertheless, increased attention is needed to avoid having low quality data in the systems negatively affecting individuals' fundamental rights.

Biometric data connect a person to alphanumerical data stored in an IT system. The quality of the biometric identifier is, therefore, of paramount importance. Although rare, FRA field research did reveal individual incidents of Dublin transfers being carried out based on false biometric matches. Presently, data quality standards for collecting fingerprints in Eurodac, which mainly holds personal data on asylum applicants, are higher than standards for collecting biometric data in VIS, for which a "zero-failure to enrol initiative" is applied, following requests by Member States. This means that for VIS the individual Member States are responsible for controlling the quality, whereas for Eurodac this is centrally carried out by eu-LISA. However, fingerprints collected for Eurodac may be checked against VIS to see if an applicant requested a visa in the past. If IT systems become interoperable, a person's biometric identifier will connect the person to information contained in all IT systems, regardless of

the quality standard according to which it was collected. Interoperability is also foreseen to include measures for improved reporting and collection of statistics, which would enhance data quality.

A person's physical development over time may reduce the reliability of matches based on biometric data, particularly after longer periods. This may be particularly relevant to cases involving children, especially if data are retained for more than five years.

National authorities and experts attach a high degree of credibility to biometric data, and processing such data is technically complex. This makes it difficult for persons concerned to rebut errors in IT systems, and even more difficult to prove that a biometric match was incorrectly generated. FRA research shows that mistakes can occur when, for instance, a person's fingerprints are mistakenly linked to another person's alphanumeric data.

FRA opinion 17

The Council of the EU should continue to put data quality issues on the agenda of relevant working parties to promote the implementation of best practices identified by eu-LISA and other actors. This should include the following:

- *Relating to alphanumeric data, the development of EU-wide guidelines on cultural norms, addressing issues such as transliterations, naming cultures, dates of birth according to different calendars and different ways of reporting age. Such guidelines would contribute to better data quality.*
- *Relating to biometric data, reviewing quality standards for fingerprints stored in VIS, taking into account that asylum seekers' fingerprints may also be matched against VIS to determine the Member State responsible for processing their claims under the Dublin system.*
- *A collection of good administrative practices to limit mistakes, such as the use of electronic readers, search criteria, and the simplification of procedures.*
- *A collection of technical safeguards that reduce the risk of mistakes, such as automatic verification against other databases when data are inserted, and possibilities to use phonetic searches.*
- *Improving the collection of statistics on inaccurate and low quality data.*

The European Commission should include data quality issues in the Schengen evaluations to support the implementation of the recommendations and best practices eu-LISA develops.

EU Member States also need to pay particular attention to the quality of data stored in national databases, if these data are transferred to EU IT systems. They should, for instance, develop standardised procedures for verification of data stored in national IT systems.

FRA opinion 18

eu-LISA has an important role to play in monitoring whether EU Member States adhere to quality standards for biometrics. When supporting the development of quality control mechanisms for capturing as well as matching biometrics, eu-LISA should consider the following aspects, which have an impact on fundamental rights:

- *age – specifically, of children as well as older persons; guidelines on capturing and matching biometrics, notably facial images, of individuals going through rapid developmental changes;*
- *disabilities – such as the possible impact of a missing eye on algorithms for facial images; difficulties in accessing fingerprinting equipment for persons with disabilities;*
- *phenotypical characteristics in the context of facial recognition – reflection of light affects the quality of facial images of very fair-skinned persons, and not enough light affects the quality for very dark-skinned persons.*

FRA opinion 19

To reduce the risk of mistakes, EU Member States need to make efforts to involve the persons whose personal and biometric data are collected and used in verification procedures. They should be open to plausible arguments presented by the persons concerned that may indicate a false biometric match, or an administrative mistake – for instance, that the biometric identifier has incorrectly been linked to another person's alphanumeric data.

Effectively exercising the right of access, correction and deletion of personal data

Article 8 (2) of the Charter, as well as EU data protection law, provide for the right of access, correction and deletion of one's own data that are stored. The specific legal instruments regulating the IT systems also mirror this right.

In spite of frequent data quality issues, complaints about incorrect or unlawful data use are rare. There is a lack of awareness and understanding of how to exercise the right of access, correction or deletion of inaccurate data that are stored. The cumbersome nature of the processes, administrative hurdles, language barriers and lack of specialised lawyers also explain why few persons try to exercise these rights.

According to FRA findings, complicated procedures and administrative and language barriers may in practice prevent the persons concerned from exercising their right of access, correction and deletion. Such difficulties may be exacerbated if IT systems are made interoperable. The establishment of a 'one-stop-shop procedure' for receiving requests to access, correct and delete data could simplify procedures. According to FRA research, very few lawyers are specialised in seeking to enforce the right of access, correction and deletion of data stored in IT systems, making it even more difficult for the persons concerned to exercise their rights.

FRA opinion 20

EU Member States should raise awareness about the right of access to one's own data stored in IT systems in the field of asylum and migration. They should systematically make available information on how to exercise the right of access, correction and deletion of data stored in these EU IT systems on the websites of concerned ministries acting as controllers of the data, national data protection authorities, as well as service providers for visa applications.

FRA opinion 21

EU Member States should put in place simplified procedures to allow people to exercise their right of access, correction and deletion, removing administrative, language and other practical barriers. Persons exercising these rights should always receive a reply indicating the action taken. In the implementation of national programmes under the Asylum, Migration and Integration Funds and Internal Security Funds, EU Member States should consider giving priority to projects for the training of lawyers on how to exercise the right of access, correction and deletion of data stored in EU IT systems.

Introduction: Developments regarding large-scale EU IT systems, biometrics and fundamental rights

Why this report

The impact of large-scale EU information technology systems (IT systems) in the areas of migration and security on fundamental rights remains largely unexplored territory. Apart from data protection analysis – including publications by the European Data Protection Supervisor – no comprehensive research exists on how these systems affect individual rights. This report intends, at least partly, to fill this gap. It analyses the fundamental rights implications of processing biometric and other data in EU IT systems in the field of visas, borders and asylum, examining both positive and negative fundamental rights implications.

The EU Agency for Fundamental Rights (FRA) has been working on the subject of biometrics and large-scale EU IT systems since 2015. This report fills a gap in that it highlights the fundamental rights risks and opportunities in this field.

Given the sheer number of people who travel to the EU, it is difficult to imagine how decisions on whether to allow a person to enter the Schengen area could be made without the support of databases. As an illustration, in 2015, more than 50 million non-EU nationals visited the EU, accounting for more than 200 million border crossings at the external borders of the Schengen area.[1] Hence, the management of asylum, borders, and visa policies relies heavily on technology when decisions affecting a person are made.

The EU has set up three large-scale IT systems in the areas of asylum and migration and another three are in the making.

The existing ones are:

- SIS II – the Schengen Information System,[2] to aid police and border checks;
- Eurodac – standing for European Dactyloscopy,[3] to support the application of the Dublin Regulation;
- VIS – the Visa Information System (VIS)[4] for visa processing.

Advanced plans exist to set up three new systems:

- EES – the Entry-Exit System[5] for registering travels in and out of the EU;
- ETIAS – the European Travel Information and Authorisation System[6] for conducting pre-border checks for visa-free travellers;
- ECRIS-TCN – the European Criminal Records Information System for third country nationals.[7]

1 European Commission (2016b), p. 2.

2 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), OJ 2006 L 381/4 *(SIS II Regulation)*; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 2007 L 205/63 *(SIS II Decision)*.

3 Regulation (EU) No. 603/2013 of 26 June 2013 on establishment of Eurodac (recast) OJ 2013 L 180/1 (*Eurodac Regulation*); European Commission (2016), *Proposal for a regulation of the European Parliament and of the council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)*, COM(2016) 272 final, Brussels, 4 May 2016 *(Eurodac proposal)*.

4 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, OJ 2008 L 218/60 (*VIS Regulation*).

5 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ 2017 L 327/20 (*EES Regulation*).

6 European Commission (2016), Proposal for a regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final, Brussels 16 November 2016 (*ETIAS proposal*).

7 Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ 2009 L 93/33; European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information system (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011*, COM(2017) 344 final, 29 June 2017 (*ECRIS-TCN proposal*).

These IT systems are, or will be, centrally managed by eu-LISA for the whole EU. At the end of 2017, the European Commission tabled a proposal to make these systems 'interoperable' by creating a common search portal and, possibly, by establishing a common repository with core biographic data of the persons whose data are stored in the different IT system.

EU IT systems are used in a number of migration related processes: in the asylum process, in the visa application process, during border checks, when issuing residence permits, when apprehending migrants in an irregular situation, in the return procedures and for issuing entry bans. In addition, they are used for police checks and in the fight against serious crimes and terrorism.

They are also utilised beyond the original purpose. Initially created for asylum and migration management purposes, IT systems set up by the EU are also increasingly serving internal security. In addition, virtually all large-scale European IT systems have provisions allowing authorities to check a person's migration status.

The IT systems referred to in this report often store biometric data. The preferred biometric identifiers at the EU level are fingerprints and/or facial images. The report focuses on these and not on, for instance, iris recognition, which is a biometric identifier sometimes used at the national level.

Ultimately, it has to be acknowledged that what makes the use of biometrics special is not only that they connect the person to information stored in various systems. Rather, *biometrics are unique to the person* in question and are considered as the most reliable method to identify a person.

In addition, the systems that this report refers to can be described as operating in the 'background', *outside the realm of public scrutiny*. Various categories of third-country nationals – applicants for international protection, migrants in an irregular situation, visa applicants or everyday travellers – have difficulties in understanding how the systems function and how they influence decision-making.

Fundamental rights risks and opportunities

The use of IT systems entails both risks and opportunities for fundamental rights. IT systems can offer more robust and timely protection – for example, for missing children and victims and witnesses of crime – and can help in preventing identity fraud and theft. At the same time, there are many fundamental rights challenges, which essentially result from the weak position of the individual whose data are stored in large-scale IT systems. For instance, in case of difficulties in fingerprinting, a third-country national is easily suspected of trying to avoid the Dublin procedures; a false biometric match may in the worst case end up in a wrong Dublin transfer; inaccurate alphanumeric data can have many reasons, but there is a tendency among authorities to suspect identity fraud affecting the trustworthiness of asylum applicants. Inaccurate data can bar entry into the EU, or can lead to a person being detained. Unlawful access to data can endanger the safety of the person concerned.

The rights to data protection and respect for private life are very central to this report. According to Article 8 (1) of the EU Charter of Fundamental Rights (the Charter), everyone has the right to the protection of their personal data. Article 7 of the Charter guarantees the right to respect for private life, which mirrors Article 8 of the European Convention on Human Rights (ECHR). The European Court of Human Rights (ECtHR) has interpreted Article 8 of the ECHR as including issues of data protection.[8]

The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)[9] is the first and only legally binding international instrument laying down rules on automated data processing. It applies to the processing of personal data in the public and private sectors.[10] All EU Member States have signed and ratified the Convention. In 2016, a draft Amending Protocol was proposed which updates and modernises the rules of the Convention by ensuring consistency with the new EU data protection framework.[11] Data collection and surveillance may pose particular challenges to the rule of law, and have been included in the checklist produced by the Venice Commission.[12]

8 See, for example, ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987; ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.

9 Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981 (Convention 108).

10 Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981 (Convention 108), Art. 3 (1).

11 Council of Europe, Ad Hoc Committee on Data Protection (CAHDATA) (2016), 'Draft explanatory report', p. 2. See also Council of Europe, 'Modernisation of Convention 108 (CAHDATA)'.

12 Council of Europe, European Commission for Democracy through Law (Venice Commission), *Rule of Law Checklist*, adopted by the Venice Commission at its 106th Plenary Session, 11-12 March 2016, Study No. 711/2013, DL-AD(2016)007, 18 March 2016.

At EU level, the protection of personal data is regulated by the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR)[13] and – for police and judicial cooperation in criminal matters – by the Police Directive, also referred to as the Law Enforcement Directive (Directive (EU) 2016/680).[14] As of May 2018, the GDPR will apply, replacing Directive 95/46/EC[15] and the Police Directive should be transposed, replacing Council Framework Decision 2008/977/JHA.[16] Regulation (EC) No. 45/2001 applies when an EU institution, agency or body processes data.[17] This regulation will apply until a new legal framework is adopted.[18]

This report, however, takes a broader approach, analysing how IT systems impact on different rights enshrined in the Charter. In addition to the right to respect for private life and the right to protection of personal data (Articles 7 and 8 of the Charter), it looks at the right to human dignity (Article 1), the right to the integrity of the person (Article 3), the prohibition of torture and inhuman or degrading treatment or punishment (Article 4), the right to liberty and security of a person (Article 6), the rights of the child (Article 24), the right to good administration (Article 41) and the right to an effective remedy (Article 47).

Among the above-listed rights, only the right to freedom from inhuman and degrading treatment is an absolute right, allowing no derogations to it. Interferences with the other rights can be justified, but they have to respect the requirements of the Charter and of the ECHR. Under EU law, any limitation on fundamental rights guaranteed by the Charter must be in line with the requirements of Article 52 (1) of the Charter, in that limitations must be provided for by law, must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, respect the essence of the right, and be proportionate. The aim of any such limitation, therefore, needs to be carefully considered. The Court of Justice of the EU (CJEU) has underlined that all the above requirements must be complied with and that an objective of general interest is not, in itself, sufficient to justify an interference.[19]

These rights are analysed in seven chapters. Chapter 1 analyses the information provided to persons whose personal data will be stored in an IT system. This is followed by a chapter on respect for human dignity when taking biometric data. Chapter 3 analyses the access to and use of personal data stored in IT systems. Chapter 4 addresses the situation of persons in need of international protection. In Chapters 5 and 6, the impact of the data quality on fundamental rights and the right to access, correction and deletion of own data stored are examined. The last chapter focuses on the best interests of the child.

This report goes far beyond fundamental rights protection.

EU large-scale IT systems

According to eu-LISA, in 2016, Eurodac stored more than five million fingerprint datasets.[20] In 2016, SIS II included a total of more than 70 million alerts, out of which only 830,000 were alerts on persons (the rest being on objects, such as lost or stolen passports, identity cards, driving licenses, residence permits, travel documents, vehicles, boats, firearms, etc.).[21] By the end of September 2015, VIS stored 17 million visa applications.[22] The legal basis for Eurodac and SIS II are under revision, and a revision of the legal basis for VIS has been proposed.[23]

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

14 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89 (*Police Directive*).

15 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31 (*Data Protection Directive*).

16 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350/60.

17 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8/1.

18 European Commission (2017), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final, 10 January 2017.

19 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014.

20 eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice) (2017a), p. 4.

21 eu-LISA (2017d), Figure 3, p. 9.

22 eu-LISA (2016), p. 9.

23 European Commission (2016), *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, COM(2016) 655 final, Brussels, 14 October 2016, p. 18.

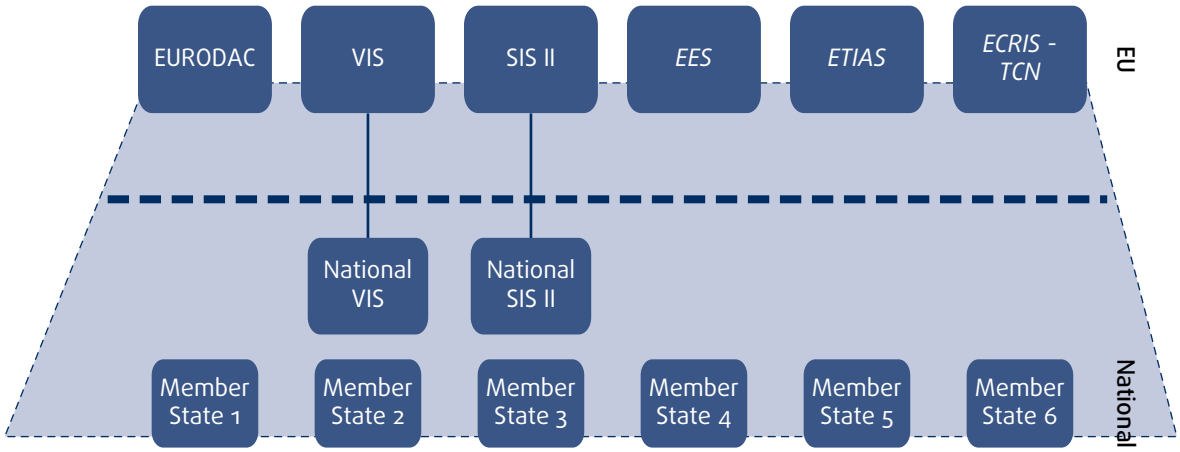
In addition, the European Commission has launched two legislative proposals on interoperability between EU IT systems. They cover IT systems in the areas of police and judicial cooperation, asylum and migration[24] as well as borders and visas.[25]

Table 1 illustrates the existing and planned systems that this report covers.

Within most EU Member States, national IT systems can directly communicate with a particular EU IT system: they are interoperable through a common search interface. The Eurodac index number may also form a part of the national registration number. These links support the authorities in their decision making as they gain a more complete picture about a person. Figure 1 shows the existing and the planned IT systems.

In addition to these large-scale IT systems, the EU has set up rules to enable national authorities to obtain information on incoming passengers from airlines and other transport companies (Figure 2). The Advance

Figure 1: EU and national IT systems in the area of justice and home affairs



Note: *Planned systems in italics*
Source: *FRA (2017)*

Passenger Information Directive (API Directive) requires each Member State to adopt legislation that obliges air carriers to provide information about the passengers that will cross that Member State's border.[26] Moreover, the Passenger Name Record (PNR) Directive obliges air carriers operating flights between a third country and one or more Member States to provide passenger data to the authorities of those Member States.[27] There is no central EU database collecting this data; rather, each Member State has its own designated authority to which the air carrier sends the data and through which Member States can exchange information.[28]

24 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, COM(2017) 794 final, 12 December 2017.
25 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final, 12 December 2017.
26 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ 2004 L 261/24 (*API Directive*).
27 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119/132 (*PNR Directive*).
28 PNR Directive, Art. 4 and 9.

Table 1: Existing and planned EU large-scale IT systems

IT system	Main purpose	Persons covered	Applicability	Legal instrument / proposal	Biometric identifiers
European dactylo-graphy (Eurodac)	Determine the Member State responsible for examining an application for international protection *Assist with the control of irregular immigration and secondary movements*	Applicants and beneficiaries of international protection, *migrants in an irregular situation*	28 EUMS + SAC	Regulation (EU) No. 603/2013 (Eurodac Regulation) *COM(2016) 272 final (Eurodac proposal)*	
Visa Informa-tion System (VIS)	Facilitate the exchange of data between Schengen Member States on visa applications	Visa applicants and sponsors	24 EUMS (not CY, HR, IE, UK)[1] + SAC	Regulation 767/2008/EC (VIS Regulation)	
Schengen Information System (SIS II) - police	Safeguard security in the EU and Schengen Member States	Missing or wanted persons	26 EUMS (not CY, IE)[2] + SAC	Council Decision 2007/533/ JHA (SIS II Decision) *COM(2016) 883 final (SIS II police proposal)*	
Schengen Information System (SIS II) - borders	Enter and process alerts for the purpose of refusing entry into or stay in the Schengen Member States	Migrants in an irregular situation	25 EUMS (not CY, IE, UK)[2] + SAC	Regulation 1987/2006 (SIS II Regulation) *COM(2016) 882 final (SIS II borders proposal)*	
Schengen Information System (SIS II) - return	*Enter and process alerts for third-country nationals subject to a return decision*	*Migrants in an irregular situation*	*25 EUMS (not CY, IE, UK)[2] + SAC*	*COM(2016) 881 final (SIS II return proposal)*	
Entry-Exit System (EES)	*Calculating and monitoring the duration of authorised stay of third-country nationals and identifying over-stayers*	*Travellers coming for a short-term stay*	*22 EUMS (not BG, CY, HR, IE, RO, UK)[3] + SAC*	*Regulation (EU) 2017/2226 (EES Regulation)*	
European Travel Information and Authori-sation System (ETIAS)	*Assess if a visa-free third-country national poses a security, irregular migration or public health risk*	*Visa free travellers*	*26 EUMS (not IE, UK)[3] + SAC*	*COM(2016) 731 final (ETIAS proposal)*	*None*
European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)	*Share information on previous convictions of third-country nationals*	*Third-country nationals with a criminal record*	*27 EUMS (not DK)[4]*	*COM(2017) 344 final (ECRIS-TCN proposal)*	
Interopera-bility – Common Identity Repository	*Establish a framework for interoperability between EES, VIS, ETIAS, Eurodac, SIS II and ECRIS-TCN*	*Third-country nationals covered by Eurodac, VIS, SIS II, EES, ETIAS and ECRIS-TCN*	*28 EUMS[5] + SAC*	*COM(2017) 793 final (Borders and visa inter-operability proposal)* *COM(2017) 794 final (Police cooperation, asylum and migration interoperability proposal)*	

Note: *Planned systems and planned changes within systems are in italics, or shown by a light blue background.*

 *Fingerprints;*  *Palm prints;*  *Facial image;*  *DNA profile.*

EUMS: EU Member States; SAC: Schengen Associated Countries, i.e. Iceland, Liechtenstein, Norway and Switzerland.

1 *Ireland and the United Kingdom do not participate in VIS. Denmark is not bound by the Regulation but has opted in for VIS. VIS does not yet apply to Croatia and Cyprus, and only partially applies to Bulgaria and Romania as per Council Decision (EU) 2017/1908 of 12 October 2017.*

2 *Cyprus and Ireland are not yet connected to SIS. Denmark is not bound by the Regulation or the Council Decision but has opted in for the SIS II, and must decide whether to opt in again upon the adoption of the SIS II proposals. The United Kingdom is participating in SIS but cannot use or access alerts for refusing entry or stay into the Schengen area. Bulgaria, Croatia and Romania cannot issue Schengen-wide alerts for refusing entry or stay in the Schengen area as they are not yet part of the Schengen area.*

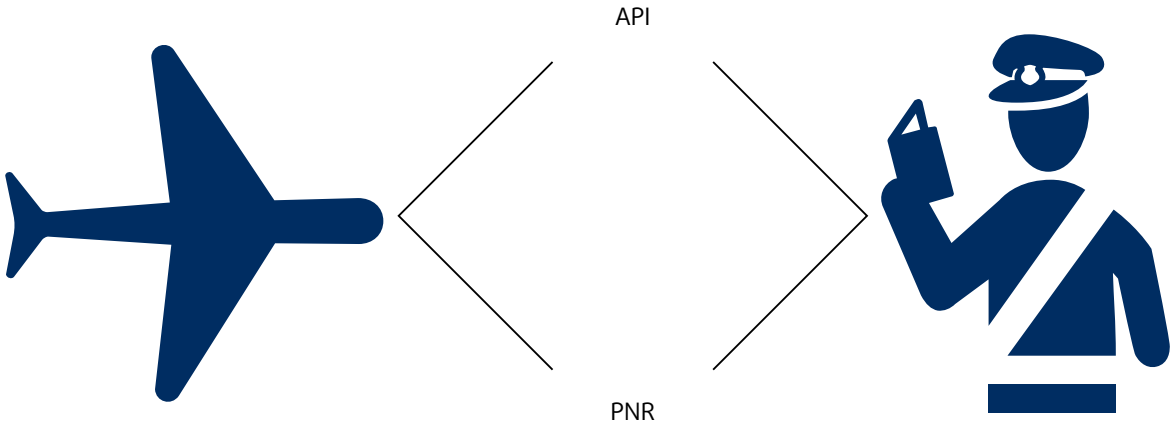
3 *Denmark may decide to opt in for EES and ETIAS.*

4 *ECRIS-TCN does not apply to Denmark. The United Kingdom and Ireland may decide to opt in.*

5 *Denmark, Ireland and the United Kingdom will take part as they participate in the IT systems made interoperable.*

Source: *FRA, based on existing and proposed legal instruments, 2018*

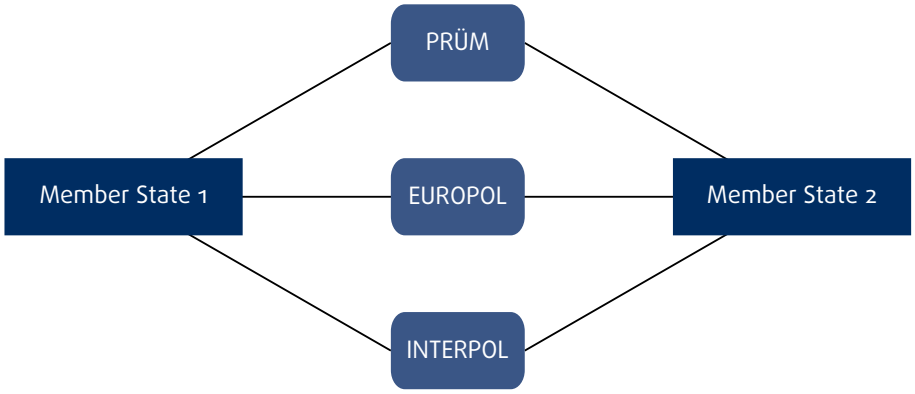
Figure 2: Mechanisms to share passengers' data



Source: FRA (2017)

Member States can also exchange personal data for purposes of criminal investigations outside the scope of EU managed IT systems. The Prüm information exchange platform has been set up for such purposes.[29] This mechanism lays down provisions under which EU Member States can on a case-by-case basis decide to grant each other access to their automated DNA analysis files, automated fingerprint identification systems and vehicle registration data. Member States can also exchange information included in Europol databases through the Europol Information System (EIS).[30] Law enforcement officials at INTERPOL's National Central Bureaus are also connected to INTERPOL databases (for example on Stolen and Lost and Travel Documents (SLTD) and Interpol's Travel Documents Associated with Notices (TDAWN).[31] Figure 3 illustrates such mechanisms to exchange personal data.

Figure 3: Information exchange mechanisms between EU Member States in the area of justice and home affairs



Source: FRA (2017)

29 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/1.

30 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/ JHA, 2009/934/ JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135/53, Art. 20 (2).

31 See the Interpol webpage on Border management.

Biometric data

Most EU-level IT systems include the processing of biometric data. Biometrics allow for the identification of an individual through one or more factors specific to the physical identity of a person.

The GDPR defines biometric data in Article 4 (14) as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".

Examples of biometric identifiers are fingerprints, retinal patterns, iris recognition, facial structure, voice, but also hand geometry, vein patterns or even some deeply ingrained skill or behavioural pattern. The definition of biometric data applies to photographs only when these are processed through specific technical means allowing the unique identification or authentication of a natural person (GDPR, Recital 51).

Fingerprints are presently used in EU IT systems in the areas of asylum and migration to carry out biometric searches. All planned IT systems foresee the possibility to undertake biometric searches also with facial images, as soon as technically possible to guarantee a reliable match.[32] In addition, palm prints and DNA are foreseen in the field of police cooperation, as Table 2 illustrates.

EU Member States also keep national databases on foreigners. The Member States connect to the European IT systems through national interfaces. When biometric matching is used, the automated fingerprint identification system (AFIS) communicates with the EU IT systems. It also stores the fingerprint templates. Annex I to the Eurodac Regulation prescribes the use of the technical standard "ANSI/NIST-ITL 1a-1997, Ver.3, June 2001 (INT-1)", and any of its future further developments, for the exchange of fingerprint data. This standard, developed by the US National Institute of Standards and Technology,[33] is widely used for AFIS purposes.[34] By central fingerprint matching, foreseen in EU IT systems, the use of AFIS becomes necessary. All EU IT systems that store or foresee to store fingerprints make reference to AFIS, with the exception of VIS (although used in practice) and ECRIS-TCN,[35] as Table 3 below shows. AFIS is gradually being introduced in SIS II to enable fingerprint searches. As of 5 March 2018, Austria, Germany, Luxembourg, Latvia, the Netherlands, Poland, Portugal and Slovenia have introduced AFIS.[36] ETIAS does not store fingerprints and consequently it does not refer to AFIS. According to the interoperability proposals, the shared Biometric Matching Service (BMS) includes those stored in AFIS in each IT system.[37] AFIS also enables the comparison of fingerprints with those in national databases.

Table 2: Biometric matching in existing and planned IT systems

IT system	Biometric matching to identify a person
Eurodac	Fingerprints as of the age of 14 years, and fingerprints and facial image as of the age of six years, according to Eurodac proposal (2016)
VIS	Fingerprints of visa applicants as of the age of 12 years
SIS II: police	*Fingerprints, palm prints, facial image and DNA profile (missing persons for protection reasons), according to SIS II proposal on police cooperation*
SIS II: borders and return	*Fingerprints, palm prints, and facial image, according to SIS II proposals on border checks and return*
EES	*Facial image, and fingerprints as of the age of 12 years*
ETIAS	*None*
ECRIS-TCN	*Fingerprints and facial images*
Interoperability (BMS, CIR & MID)	*Fingerprints and facial image*

Note: *Planned systems and changes in italics.*

Source: *FRA, based on existing and proposed legislation (2017)*

32 Eurodac proposal, Art. 42 (4); SIS II police proposal, Art. 42 (4); SIS II borders proposal Art. 28 (4); SIS II return proposal, Art. 13; EES Regulation, Art. 36 (b); ECRIS-TCN, Art. 6 (2).

33 See: Newton, E., Coleman, G., and Yuh, P. (2008).

34 See, for example,. Zhang, D. (2013), p. 283.

35 Eurodac Regulation, Art. 20 and Recital 32; Eurodac proposal, Art. 21 and Recital 42; EES Regulation, Art. 32 (2) (b). For SIS II see: Commission Implementing Decision (EU) 2016/1345 of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II), OJ 2016 L 213/15.

36 European Commission (2016f); eu-LISA (2018), 'AFIS for SIS II to be deployed this month', 2 March 2018.

37 Interoperability proposals, Recital 17.

Table 3: References to AFIS in legislative instruments of EU IT systems

	Eurodac	VIS	SIS II Decision and *police proposal*	SIS II Regulation and *borders proposal*	*SIS II return proposal*	*ECRIS-TCN*	*EES*	*ETIAS*
AFIS reference	yes	no	yes	yes	*yes*	no	yes	n/a

Note: *Proposed systems and proposed changes in italics.*
Source: *FRA (2017), based on EU legislation.*

At the national level, iris recognition has been used for automatic border controls or e-gates, for instance in the Netherlands and the United Kingdom. Palm prints are used in the law enforcement context, including apprehension of migrants in an irregular situation, for example, in Belgium, according to FRA field research. Experts interviewed by FRA noted that in Germany and Italy, prints of the full palms and sides of hands may be taken from asylum applicants at airports in case there are grounds for suspicion of fraud or if the person resists fingerprinting.

The facial image may reveal a person's phenotypical characteristics, but may also allow for automated phenotypical classification. Digital images of the face with sufficient image resolution and quality may be used in automated biometric matching. Some experts argue that fingerprints and iris recognition can reveal phenotypical origin and could be subject to automated ethnic classification.[38] When fingerprints are transformed and stored in the form of templates this makes it close to impossible to extract sensitive information.

The processing of facial images or fingerprints requires particular guarantees.[39] In EU law, under Article 9 (2) (g) of the GDPR, the processing of biometric data is only allowed where processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

Academic writers have argued that the increasing collection and storage of data is likely to affect societies and individuals in multiple ways.[40] This is particularly the case when biometric data are processed. Increasingly fast developing technologies could allow for matching of not only fingerprints but also facial images for surveillance purposes. According to some experts, curtailing privacy by processing large amounts of personal data, including biometric data, may affect democracy and society since privacy is a value inherent to a liberal democratic and pluralist society, and a cornerstone for the enjoyment of human and civil rights.

EU Member States are also obliged to include facial image and fingerprints in a chip in residence permits[41] and passports.[42] Regarding the latter, in 15 Member States[43] the fingerprints are stored in a database and in 13 Member States in a chip in the passport only.[44] Fingerprints of EU citizens are not stored in databases.

In a case concerning the lawfulness of storing fingerprints in biometric passports, the CJEU has indicated that central storage of biometrics would need to comply with more stringent requirements than their storage in the passport itself.[45] In *M.K. v. France*, the ECtHR concluded that retention of fingerprints solely for the reason of preventing future identity theft would, in practice, be tantamount to justifying the storage of information on the entire population, which is clearly excessive.[46]

38 De Hert, P. (2013), p. 391; Kindt, E. J. (2013), p. 320.
39 ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 68, 84 and 85; General Data Protection Regulation, Art. 9 (1); Police Directive, Art. 10.
40 Hallinan, D. (2015), pp. 268-270; Raab C. (2015), pp. 259-268; Goncalves, M. E. and Gameiro, M. I. (2014), p. 29.
41 Council Regulation (EC) No. 380/2008 of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, OJ 2008 L 115/1; Regulation (EU) 2017/1954 of the European Parliament and of the Council of 25 October 2017 amending Council Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, OJ 2017 L 286/9, Annex.
42 Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ 2004 L 385/1.
43 Belgium, Bulgaria, Spain, Estonia, Greece Finland, France, Croatia, Hungary, Lithuania, Latvia, Malta, the Netherlands, Slovakia and the United Kingdom.
44 Austria, the Czech Republic, Cyprus, Denmark, Germany, Ireland, Italy, Luxembourg, Poland, Portugal, Romania, Slovenia and Sweden.
45 CJEU, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17 October 2013, paras. 59-63.
46 ECtHR, *M.K. v. France*, No. 19522/09, 18 April 2013, para. 40.

Methodology

FRA has been analysing the fundamental rights implications of processing biometric data in large-scale EU IT systems since 2015, when the agency started working on a dedicated project on biometrics.[47] The research builds on different research methods and data collection, combining social and legal research. The research comprises a mapping of relevant practices and procedures in all EU Member States, carried out by Franet, as well as fieldwork research in six selected EU Member States based on the different migration challenges they face. Eticas Research and Consulting, and the Spanish Research Council (CSIC), Department of Demography, carried out the fieldwork research on behalf of FRA.

Legal research included a mapping of practices and procedures related to the use of databases in all EU Member States. Franet carried out this mapping during the first half of 2015. Authorities received a questionnaire and were asked to provide information on procedures and rules governing the use of databases at the national level. In addition, desk research assessed the extent to which civil society is active and aware of the issues in this field.

The fieldwork research included in-depth interviews carried out with practitioners (public officials and legal representatives, including immigration lawyers and NGOs), experts (fundamental rights, biometrics and IT experts) and asylum seekers and migrants (total, 286 interviews). In addition, three small-scale surveys were carried out with border guards (160 respondents) and staff processing visa applications at embassies and external service providers (132 respondents) and with visa applicants (584 respondents). The small-scale survey among border guards was conducted at border crossing points in six EU Member States, including the Zeebrugge port in Belgium, the airports Frankfurt in Germany, Barajas in Spain, Fiumicino in Italy and Arlanda in Sweden, as well as the border crossing point Terespol in Poland. The surveys among staff working at consulates and visa applicants were conducted in four countries including Algeria, Nigeria, Thailand and Ukraine. To contextualise better the results of the small-scale surveys, non-participant observations took place at the same locations where the surveys were carried out.

How the results of the field research are presented

The interviews are referred to in the form of anonymised quotes that are either representative of the research findings or illustrate differences when the answers differ significantly. The analysis refers to practitioners of Member State authorities as 'officers' or 'providers of legal assistance', whereas it refers to fundamental rights, biometrics or IT experts as 'experts'. The results of the small-scale surveys are represented in figures (percentages may not total 100 due to rounding) and described in the text. Where appropriate, reference is made to the findings from the non-participant observations. The conclusions are drawn from different research data and findings.

47 FRA (2015a), Annual Work Programme, Vienna, December 2014.

1 The right to information when personal data are processed

Charter of Fundamental Rights of the European Union

Article 41 – Right to good administration

1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union.

2. This right includes: [...]

(b) the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy [...].

This chapter analyses the information given to individuals when their personal data are processed in one of the three existing IT systems (Eurodac, SIS II and VIS). First, the chapter examines the information people receive when their personal data are collected, dealing separately with Eurodac and VIS. Following this, it analyses information provided when personal data are checked for specific procedures at border crossing points, when people are apprehended inside the country, or when people apply for a residence permit.

The research confirms past FRA findings that people lack awareness of data protection violations and available remedies.[48] Visa applicants do not seem to worry about what happens to their processed personal data, as an officer in charge of visa processing noted.

"Until now I have never had the case of someone asking." (Diplomatic missions and consular posts (DMCP), male, Algeria)

This chapter describes more extensively the challenges in the context of Eurodac. Considering the many serious worries that persons applying for international protection, or persons apprehended as a migrant in an irregular situation may have, their interest and ability to absorb and comprehend provided information is limited, particularly on data protection issues. Experts also noted a dissociation between the duty to inform asylum applicants and how they are informed in practice. This raises the question of how the quality of information affects procedures and on the trust in the system as a whole.

Disrespect of the duty to inform may have consequences for Member States. It may make decisions based on the data stored unlawful, as the following example illustrates. On 31 July 2014, the Court of Appeal of Paris overturned the decision on a Dublin transfer of an asylum applicant to Spain by the Prefect of the Paris Police because the asylum applicant was not informed of essential safeguards, such as the use of his fingerprints, the identity of the data controller and the recipients of the data.[49]

Furthermore, if a person does not have enough information about an entry in a database, this makes it very difficult for them to exercise the right to access and rectify the data.

48 See FRA (2010a); FRA (2012), FRA (2017a).

49 France, Administrative Court of Appeal, No. 14PA00421, 31 July 2014.

1.1. The principle of transparency

The right to good administration as set out in Article 41 (2) of the Charter includes the right of an individual to have access to their file. Article 41 of the Charter applies to EU institutions, bodies and other offices. It is based on the existence of the Union as subject to rule of law enshrining good administration as a general principle of law.[50] The right to good administration, according to the CJEU, reflects a general principle of EU law.[51] It also requires Member States to apply the requirements of the right to good administration in all procedures, including procedures for granting protection.[52]

The General Data Protection Regulation (GDPR) and Police Directive include provisions guaranteeing the **principle of transparency** and the right to information. Article 5 (1) of the GDPR states that "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". Controllers must take appropriate measures to provide information related "to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language".[53] According to Articles 13 and 14 of the GDPR and Police Directive, the person concerned should receive information on the identity and the contact details of the controller, purpose of the processing, retention times, the right to request access to stored data, and its erasure or rectification, as well as the right to lodge a complaint with a supervisory authority.

The right to information is included in the legal instruments for Eurodac,[54] SIS II,[55] VIS[56] and EES, [57] as well as the proposed system ETIAS.[58] As concerns SIS II, the right to information applies only in case of alerts on refusal of entry or stay,[59]and in the future it will also apply to alerts on return decisions.[60] The right to information regarding SIS II does not, however, apply in the context of police or judicial cooperation in criminal matters.[61] Even when the right to information applies, it can be restricted, since the Member State is under no obligation to inform the person if their data has not been obtained from the person in question or if the provision of information proves impossible or would involve a disproportionate effort.[62] Moreover, it can be restricted for certain reasons, such as public security or criminal investigations.[63]

Although persons must normally be informed when their data are collected, such information does not necessarily cover all the purposes for which data may be used. As an illustration, the person whose data are collected for Eurodac is not informed that it can also be used for apprehension and return purposes. Under the Eurodac proposal, personal data can be shared with third countries under certain circumstances, but there is no explicit duty to inform the data subject about this possibility. On the contrary, in the context of VIS, the right to information cover "the purposes for which the data will be processed."[64] Table 4 illustrates the main aspects of the right to information as guaranteed in the different instruments.

The right to information is also included in Article 46 of the interoperability proposals and applies when data are stored in the biometric matching service, the common identity repository or the multiple-identity detector.

Provision of information is not only a transparency requirement under data protection law, but it also promotes respect for the dignity of the person, as explained in Chapter 2. If a person understands the purpose of the data processing, it is easier to win their cooperation in the process. However, as illustrated in the following sections, information is sometimes incomplete, not understandable or misleading, and not provided in all situations.

50 Explanations relating to the Charter of Fundamental Rights, OJ 2007 C 303/17, Explanation on Art. 41.
51 CJEU, C-604/12, *H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General*, 8 May 2014, para. 49.
52 CJEU, C-604/12, *H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General*, 8 May 2014, para. 50.
53 General Data Protection Regulation, Art. 12 (1). See also: Police Directive, Art. 12.
54 Eurodac Regulation, Art. 29 and Eurodac proposal, Art. 30. Article 29 Data Protection Working Party (2017).
55 SIS II Regulation, Art. 42.
56 VIS Regulation, Art. 37.
57 EES Regulation, Art. 50.
58 ETIAS proposal, Art. 54.
59 SIS II Regulation, Art. 42 (1); SIS II borders proposal, Art. 48.
60 SIS II return proposal, Art. 13.
61 SIS II Decision; SIS II police proposal.
62 SIS II Regulation, Art. 42 and SIS II borders proposal, Art. 48.
63 *Ibid.*
64 VIS Regulation, Art. 37.

Table 4: The right to information when data are collected, existing and planned EU IT systems

		Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS II Regulation and** *borders and return proposals*	**EES Regulation**	*ETIAS proposal*	*ECRIS-TCN proposal*	*Interop. proposals (BMS, CIR and MID)*
Instrument has a provision on the right to information		yes	yes	no	yes, with restrictions	yes	*yes*	*no*	*yes*
Information must be provided in an understandable manner		yes	no	n/a	no	yes	*no*	*n/a*	*no*
Information must include that data can be used for:	determining the Member State responsible for the asylum procedure	yes	yes	n/a	n/a	n/a	*n/a*	*n/a*	*yes*
	apprehension and return purposes	no	yes	n/a	yes, with restrictions	yes	*n/a*	*n/a*	*yes*
	investigations of serious crimes and terrorism	yes	yes	n/a	yes with restrictions	yes	*no*	*n/a*	*yes*
Data subject must be informed about possible data sharing with third countries		no	yes	n/a	n/a	yes	*n/a*	*n/a*	*n/a*

Note: *Proposed systems and proposed changes in italics.*
n/a = not applicable.
Source: *FRA, based on existing and proposed legal instruments (2017)*

1.2. Information when taking fingerprints for Eurodac

Article 29 of the Eurodac Regulation and Article 30 of the proposal regulate the information to be provided to data subjects when storing their fingerprints in Eurodac. A central element is the duty to inform asylum applicants and apprehended migrants in an irregular situation that other Member States will check their fingerprints to determine the state responsible for examining an application for international protection as regulated in the Dublin Regulation. They must also be informed that this may result in a transfer back to the Member State of first entry, should the individual move on in an unauthorised manner. In addition, the information must include the fact that national authorities of other Member States as well as Europol have access to Eurodac, mention the recipients of the data, the obligation to have fingerprints taken, as well as the right to request access, rectification, erasure, and restriction of the personal data.[65]

65 Eurodac Regulation, Art. 29 and Eurodac proposal, Art. 30.

Implementation of Member State's duty to inform

EU Member States **rely predominantly on written information** to fulfil their duty to inform asylum applicants and other migrants whose fingerprints are taken and stored in Eurodac. Member States as a rule also have information on Eurodac available on their websites.[66]

The European Commission has developed standard leaflets providing information on the Dublin procedure.[67] Member States must use these leaflets and complete

66 For example, see: Sweden, Swedish Migration Agency, 'Fingerprints and Eurodac'; Finland, Finnish Immigration Service, 'Fingerprints and Eurodac'; United Kingdom, 'Fingerprints and Eurodac: found staying illegally in EU'.

67 Commission Implementing Regulation No. 118/2014 of 30 January 2014 amending Regulation No 1560/2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2014 L 39/1, Annexes X to XII.

them with their country-specific information.[68] The leaflet informs applicants about international protection on the Dublin procedure and that fingerprinting is an obligatory element of the procedure. In detail, the leaflet informs the applicant that:

- fingerprints will be taken again if they are of a poor quality;
- fingerprints are stored in Eurodac for 10 years;
- fingerprints may be checked against VIS;
- he/she has right of access, correction and deletion (including contact details to exercise these rights;
- Europol and national police authorities may access data for law enforcement purposes;
- the Eurodac Central System store the fingerprints and they are not shared with any third country that is not bound by the Dublin Regulation.[69]

In the six EU Member States covered by the field research, leaflets are available in the most common languages among asylum seekers in those countries. In Sweden, for example, leaflets are available in Arabic, English, French, Pashto, Persian, Russian, Somali, Swedish and Tigrinian.[70] Interpretation can also be organised, if needed, according to the authorities.

Authorities often obtain proof or confirmation that the information was provided. For example, in Italy, the applicant signs a form where the content of Article 29 of the Eurodac Regulation is translated into different languages. Some EU Member States also obtain proof when the asylum applicant is checked against VIS. In Finland, the VIS search results are marked in a dedicated form, every page of which the asylum applicant must sign.[71]

Pursuant to Article 29 (1) of the Eurodac Regulation (see also Article 30 (1) of the Eurodac proposal), information must also be **provided orally** "where necessary".

Findings from the field research indicate that practices vary. In Sweden, for example, the authorities provide some information orally when taking fingerprints, but full information is provided when the asylum application is registered. In Belgium, according to an expert, the officials who physically fingerprint the person are not trained to give information verbally. In Spain, when migrants are apprehended they are only informed that the fingerprints will be registered in a database, without specifying which database, the reasons, or other rights, unless the person asks.

"Of course, if one of them asks, they are told, it is not restricted information." (Border guard, female, Spain)

During the field research at the Terespol border crossing point in Poland, fingerprinting of asylum seekers was observed. The border guard officer asked if the person knew why they were having their fingerprints taken. Most of the observed persons affirmed this, but with no confidence. The officer interpreted their responses as an assurance that they had read the written information provided and that no further information was necessary.

Many interviewees were of the opinion that a **high number of arrivals affects the quality of the information provided**. Officials interviewed in Belgium, Germany and Sweden noted that work load impacts quality.

"The provision of written information should not be impacted, but the provision of oral information is impacted." (Swedish Migration Agency, female, Sweden)

Significant difficulties also emerged from the so-called hotspots at the EU-supported Greek and Italian processing centres that register and refer newly arrived people.[72] In Italy, officials explained that after a large number of arrivals disembarked, sometimes during the night and after dangerous and long journeys, the police officers in charge of fingerprinting would work in a rush, spending less time explaining the process to individuals.

"Of course! The higher the inflows, the less time we can dedicate to explanations." (Asylum and Immigration Office, male, Italy)

Some of the authorities interviewed pointed out that information given in the hotspots and, especially, in the reception centres, has improved thanks to NGOs and international organisations that distribute leaflets, even on the vessels before disembarkation. However, the information provided either does not focus on fingerprinting and its implications, or does not consider fingerprinting at all. Instead, they provide information on the asylum process and do not provide any specific information on Eurodac.

Although not specific to fingerprinting, in 2010, FRA published a report on the duty to inform asylum

68 According to Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, OJ 2013 L 180/31 (*Dublin III Regulation*), Art. 4; Eurodac Regulation, Art. 29 (3); and Eurodac proposal, Art. 30 (3).

69 Commission Implementing Regulation No. 118/2014 of 30 January 2014 amending Regulation No 1560/2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2014 L 39/1, Annex X, Part A.

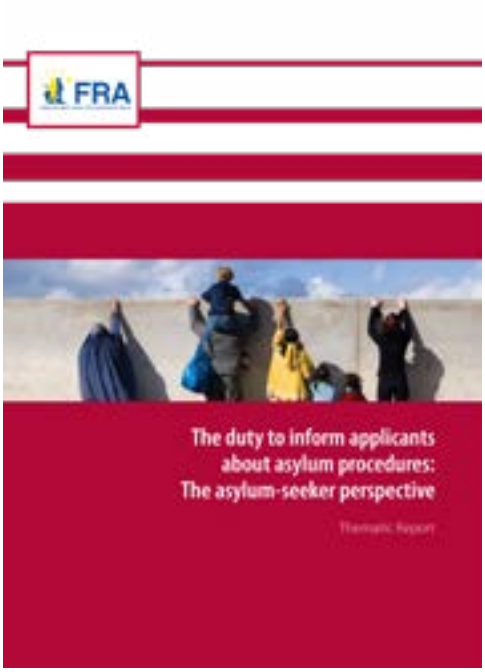
70 Sweden, Swedish Migration Agency (*Migrationsverket*), *Du kan inte välja vilket land som prövar din asylansökan (Dublinförordningen)*.

71 Finland, Asylum guidelines (*Turvapaikkaohje*), MIGDno/2013/700.

72 European Commission (2015a).

applicants on the procedure for international protection. The findings indicate that while states are providing information to asylum seekers on the procedure, such information is not always understood or does not make applicants aware of their rights and obligations. The evidence gathered from asylum applicants suggests that levels of trust in the source providing information and communication barriers – due to both language and technical jargon – emerge as recurrent obstacles to effective provision of information, which would equip applicants to take informed decisions at each stage of the procedure.

The starting point to enhance the effectiveness of information provided to asylum applicants is to listen to what they suggest.



Migrants' perspective: an impression of lack of transparency

Many interviewed migrants and asylum applicants were unaware of the reason they had to provide their fingerprints, whereas others said that officials had informed them about how the fingerprints and data would be used. Those who were not aware said that the authorities that took the fingerprints did not explain why it was necessary to provide fingerprints, for what procedure they would be used, or in what type of database they would be stored. In addition, they generally could not remember whether they had received information on their rights to access, correct and delete their data.

Incomplete or misleading information

Some interviewed asylum applicants and migrants pointed to the fact that the consequences of including fingerprints of persons having crossed the external borders in Eurodac are either not properly explained or are purposefully not revealed.

Several people interviewed who had transited other Member States mentioned that they had received contradictory information from the Hungarian authorities. One asylum applicant from Afghanistan explained that he gave his fingerprints because the Hungarian authorities had stated that collecting his fingerprints was only for security purposes, and because any person who declined to give their fingerprints would be deprived of their liberty until they complied with this obligation. It was only after he arrived in Sweden and provided his fingerprints again that he discovered the implications on the asylum procedure. The interviewee felt deceived. A Kurdish asylum applicant described a similar experience: the Hungarian authorities told him that providing fingerprints would not affect which country considered his asylum case and that he would be able to carry on with his journey.

Examples of incomplete information also emerged from asylum applicants registered in other EU Member States. An asylum applicant fingerprinted in Germany and interviewed in Sweden, explained that she was reluctant to provide fingerprints in Germany because she wanted to join her husband in Sweden. She provided her fingerprints in Germany after officials told her that having her fingerprints taken in Germany would not affect onward travel. Similarly, an Ethiopian woman interviewed in Sweden explained that she did not understand why the Dutch authorities took her fingerprints and that she was not informed about the purpose or the procedure for which they were collected. The authorities simply told her that she was imprisoned because she had come illegally to the Netherlands and used someone else's passport.

In Spain, migrants and providers of legal assistance described the information provided on the use of databases as non-transparent. Providers of legal assistance concluded that the main problem in Spain is the lack of information regarding the use of the fingerprints.

Incomplete information appeared to be more frequent when authorities registered individuals as **persons who irregularly crossed the EU external border but who were not immediately registered as asylum applicants**. This was either because the person did not apply or

because according to national procedures, the formal registration of an asylum application happens at a later stage. Testimonies collected from Germany, Greece, Hungary, Italy and Spain indicate that at this first stage, the person may be told that fingerprints will be used for purposes of public security and identification. Furthermore, they indicate that there is no mentioning that fingerprints included in Eurodac for a person apprehended as a migrant in an irregular situation are of relevance for the Dublin procedure.

In Sweden, for example, only after the authorities have taken the applicant's fingerprints and carried out a search, is the applicant informed that the authorities have checked their fingerprints in Eurodac, VIS and the national database, and what the results are. In Italy and Spain, the police or other authority physically taking the fingerprint do not specifically inform about the asylum procedure, as the immigration office deals with this. The Italian Scientific Police in charge of fingerprinting confirmed that officials did not typically provide information when enrolling fingerprints in Eurodac, which matches what interviewed asylum applicants said. In Italy, it is assumed that asylum applicants receive all necessary information from the immigration authorities or in the reception centres at a later point in time. Nevertheless, some asylum applicants also claimed not having received information upon transfers to a reception centre or during the asylum application procedures. In Spain, one asylum applicant explicitly stated that this lack of initial information was one reason for refusals to provide fingerprints, since it triggered distrust in the authorities. Migrants who transited through Greece explained that they were not provided information about the fingerprinting procedure, or at least not in an understandable way.

When carrying out field research in one of the hotspots in Sicily in summer 2016, the interviewers noted that officials provided no information before fingerprinting. Information on how to exercise the right to access is not publicly available. The national data protection authority recommended improving this situation, especially in relation to vulnerable persons, by providing leaflets in different languages and by making them accessible in the facilities where the identification procedure is implemented.

Information not understood or believed

Officials should provide information in an understandable and transparent manner, according to the Eurodac and Dublin regulations and proposals.[73] As an officer of a German data protection authority noted, it can be difficult to inform a person who is in Germany for the first time, does not speak the language and has other priorities so that they understand correctly, what exactly is going to happen.

The field research carried out in Italy concluded that when some information is provided, it is often not given in an appropriate manner that allows people to fully understand the meaning and implications of providing their data and of it being stored in the different databases. Providers of legal assistance in Sweden noted that despite the efforts made, the provision of information is not effective.

"I don't think I have ever met an asylum seeker who knew what happened or why it happened. […] Or what happens to them [the fingerprints]. Many of them ask, 'How long are they kept, the fingerprints? Who can see them? My employer – can they see from the fingerprints that I am an asylum seeker? You get many questions." (Provider of legal assistance, female, Sweden)

Legal language is used which is not understandable, as the following example from Poland shows.

"A foreigner, when they have obtained information, very often might confirm that they have understood it when they did not. Even from my personal experience, I know that the language has to be simple and the message has to be straightforward and descriptive. What I mean is, it should be explained why a certain activity has to be conducted. And so on. Because, even if the foreigner admits that they understand, they do not necessarily know what it is about. Even for very basic matters." (Asylum and Immigration Agency, female, Poland)

Finally, **information received from family, friends** or even smugglers may be **more trustworthy** than what the authorities tell. Previous FRA research shows that asylum applicants consider social networks, such as friends, relatives, acquaintances, other asylum applicants and fellow countrywomen and -men who they meet in reception centres and other places to be a valuable source of information, although these sources may not provide accurate or complete information.[74]

One asylum applicant interviewed in Belgium stated that they had received all information regarding the processes and procedures in different EU countries through social networks, smugglers and other migrants. Several interviewees mentioned knowing about the need to provide fingerprints from family members, acquaintances or smugglers before they reached Greece.

"We knew about it, [they were] for Dublin […] We asked before, we know everything about Europe." (Asylum seeker, Syrian male, Belgium)

An applicant from Syria stated that he was aware that giving fingerprints in Greece did not affect the

73 Eurodac Regulation, Art. 29 (1); Eurodac proposal, Art. 30 (1); Dublin III Regulation, Art. 4 (2); Dublin proposal, Art. 6 (2).

74 FRA (2010b), p. 29.

future asylum case in other EU countries. An asylum applicant from the Ivory Coast interviewed in Sweden, noted that he received a leaflet in French detailing his rights and obligations when the authorities took his fingerprints. Nonetheless, he was unaware in which database his biometric data would be stored. Only after discussing with fellow migrants did he understand that his fingerprints would be registered in an EU database.

"When it comes to fingerprints, I have not heard anybody say anything about that, I mean about the purpose. It was afterwards that I heard people who were together with me say that these fingerprints would be used in a European database." (Apprehended migrant, Ivorian male, Sweden)

In some cases, the misinformation appears to originate from the interpreter. Some migrants who transited through Greece were orally informed by the interpreter that the purpose of collecting fingerprints was related to security or law enforcement. Interpreters told an apprehended migrant from Iran, for example, that fingerprinting was a mandatory procedure because they were entering Europe.

"When they asked why we had to provide our fingerprints, they explained that this is the border between Asia and Europe and that you have to provide information about your fingerprints so they can trace your background and whether you are a criminal or not. So that they can identify you and get some information about your background in Iran, the problem in your work […]." (Apprehended migrant in an irregular situation, Iranian female, Belgium)

NGOs and civil society organisations play an important role in supporting the authorities in explaining the purpose of fingerprinting. As irregular migrants and asylum seekers may distrust information that public authorities provide, the civil society sector are increasingly handed the task of providing information. However, a court in France has ruled that the intervention of an association alone does not ensure the right to information, particularly on an individual's rights to access, rectify and appeal data.[75]

Language barriers are another important reason preventing a proper understanding of information. Some migrants and asylum seekers, having transited Greece in 2015, explained that there was a lack of interpreters. Procedures with asylum applicants and apprehended migrants are carried out with the help of interpreters, sometimes via telephone. The quality of the translation and the sound quality of the telephone connection affects how the duty to provide information is implemented.

75 France, Administrative court of appeal of Nantes, 12 July 2011, No. 10NT02532, Juris-Data No. 2011-018043.

1.3. Information when taking fingerprints for visas

One specificity of visa processing is the role of privately contracted service providers. According to Article 43 of the Visa Code, Member States may subcontract certain tasks to external service providers.[76] Typical tasks, which are outsourced, include the provision of general information on visa requirements, application forms and supporting documents required; data collection, including biometrics for the visa applications; collecting the visa fee; managing appointments for visa interviews; returning the passport with the visa or the refusal notification to the applicant.

Among the diplomatic missions and consular posts in Algeria, Nigeria, Thailand and Ukraine covered by this research, external service providers supported the visa application procedure in Abuja, Lagos, Bangkok, Kiev, and Lviv. The services were contracted out to the company VFS,[77] who in some cases, operated on behalf of more than one Member State.

The small-scale survey at DMCPs shows that service providers have received more training and written guidance on how to inform applicants than staff at DMCPs. Among the staff of service providers, 82 % said that they had received information about what information to provide to persons whose fingerprints are enrolled, and 52 % said that they had received training and/or written guidance on how to inform applicants about their rights. Whereas, among DMCP staff, only 64 % and 36 % respectively had received such information.

Implementation of the duty to inform

The VIS Regulation includes in Article 37 a duty to inform visa applicants and their sponsors **in writing**. Officials must provide this information when collecting data for the application form, the photograph and the fingerprints. It covers several but not all aspects.

According to Article 14 (4) of the Visa Code,[78] the information pursuant to Article 37 (1) of the Visa Regulation must be made available in the Schengen visa application form. The form is annexed to the Visa Code. It informs the visa applicant that the data collected in the application form, as well the photograph and fingerprints, are mandatory for examining the visa application and that the relevant Member State

76 A full list of external service providers is available on the European Commission website.
77 See VFS's website.
78 Regulation No. 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), OJ 2009 L 243/1.

authorities will process this data to decide on the visa application. The application form also informs the visa applicant:

- that the data are stored in VIS for five years, during which time national authorities, such as those carrying out checks on visas, immigration and relating to asylum, will have access to it, and the reasons why;
- that the applicant has a right to obtain information on their data stored in VIS, including which Member State transmitted the data, as well as the right to rectification and deletion of data and the right to a remedy;
- the consequences of false declaration;
- that the applicant is obliged to leave the EU before the visa expires.

In addition, it informs the applicant that under certain conditions, data may be used to prevent, detect and investigate terrorist offences and other serious criminal offences.

Compared with Eurodac, information to visa applicants rely more heavily on written information. Researchers for this project observed that at VFS in Algiers, which receives visa applicants for Spain, at the Belgian embassy in Algiers, and at VFS in Abuja and Lagos, reciving applicants from Belgium, Italy and Sweden that visa applicants receive information only as it is described in the visa application form. Similar information to the one included in the form may be available on webpages of the Ministries of Foreign Affairs.[79] Information can also be provided through posters or leaflets at the embassy or consulate or their service providers. Oral information – usually provided in the local language – focuses on the smooth and efficient fingerprinting process and not on information about the use and storage of the information.

Promising practice

Ensuring visa applicants' right to information

Inspired by FRA's project on biometrics in large EU IT systems, Sweden initiated a project on visa applicants' right to information. The Swedish project was set up because of the need to improve the awareness of consular staff on visa applicants' right to information. Recommended measures include providing information through the digital application process, in addition to including information on the application form. An additional option under consideration is to provide information on the receipt acknowledging that the visa application has been submitted.

Source: Swedish Migration Agency, 2017

Focus on the fingerprinting procedure

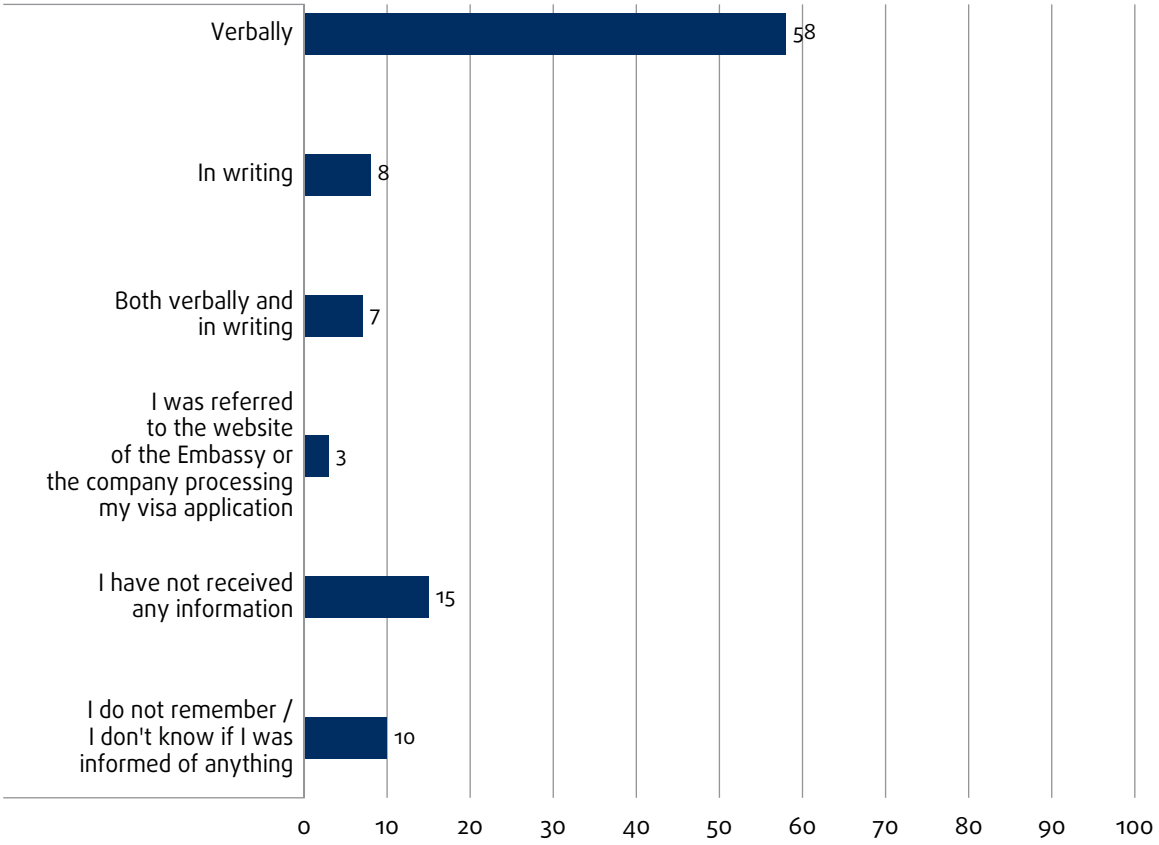
Non-participant observations carried out for this project indicate that the information provided when the visa application is submitted mainly covers the fingerprinting procedure, which is a fairly simple, straightforward, and intuitive procedure. Information may only be given orally, as observed at VFS Bangkok (working for the Italian embassy) or also through posters in the waiting areas, as in VFS Abuja (working for DMCPs of Belgium, Italy and Sweden). Information was usually limited to visual instructions on how to provide fingerprints (for instance, at the VFS office receiving applicants for Sweden in Bangkok but also at the German consulate in Bangkok), but not about why the data are processed or why they will be stored, which is provided in the visa application form.

Results of the small-scale survey FRA carried out among visa applicants showed that, at their most recent visa application for a short-stay visa, three in four of the surveyed visa applicants (76 %) received some form of information about how the fingerprinting process is carried out. In most cases, applicants indicated that information was only provided verbally (58 %), only in writing in 8 % of cases and both verbally and in writing in 7 % of cases. In very few cases, the applicants were referred to the Embassy's website (3 %) (Figure 4). However, as much as 25 % said that they had not received information or could not remember if they had received any.

Regardless of the mode of receiving the information (either verbally or in writing), most of the surveyed visa applicants said that they found the

79 See, for example, the Ministry of Foreign Affairs of the Czech Republic's Biometrics webpage.

Figure 4: Mode of receiving information on the fingerprinting process at last application for a short-term visa (%)



Note: *The results are based on the survey question "When you last applied for a short-term visa, in what way was information on the fingerprinting process provided to you?" (n = 543).*

Source: *FRA Biometrics project, Visa applicants survey, 2016*

information to be understandable (85–86 %) or partly understandable (7–10 %).[80]

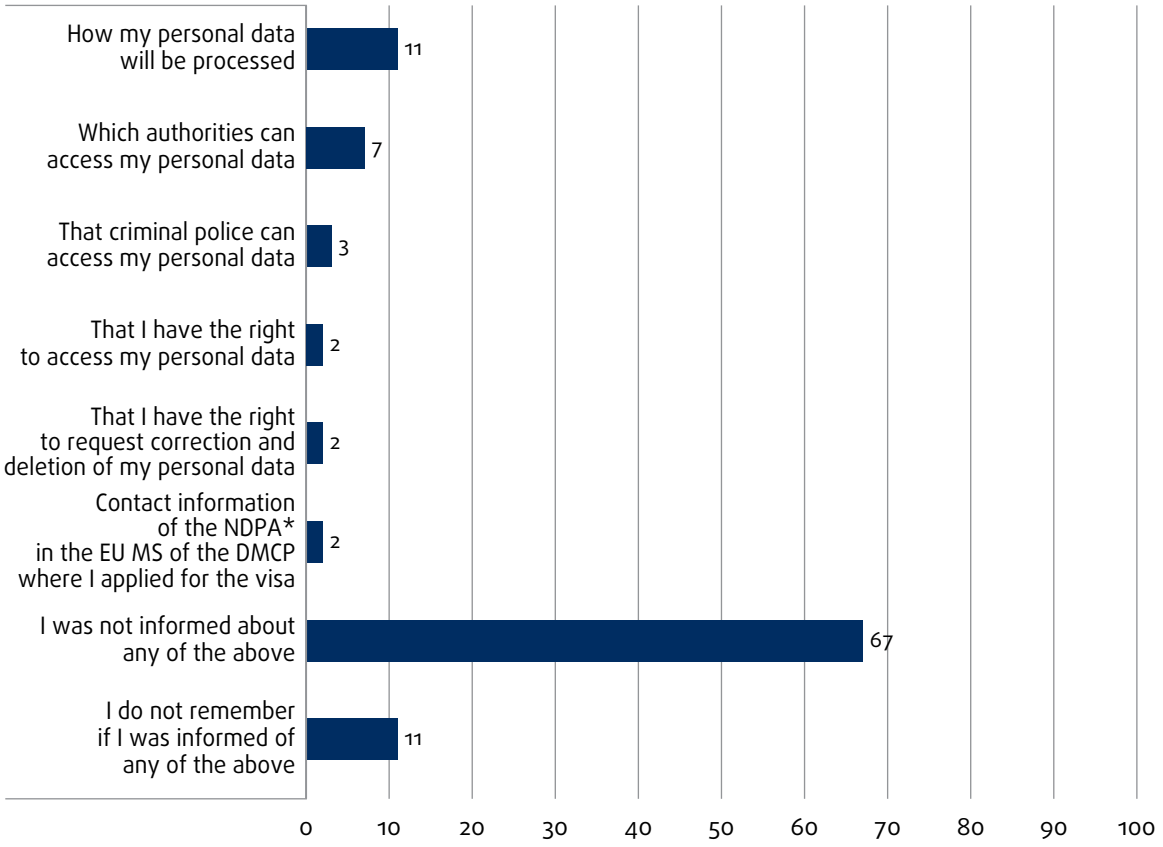
Apart from the fingerprinting process, most visa applicants interviewed either did not receive or did not recall receiving other information on how their personal data are stored. Only 11 % among the visa applicants interviewed said that they had received information about how the data will be processed and only 2 % reported to have received information about how they could access, correct or delete data, as shown in Figure 5. This illustrates that much information included in the Schengen visa application form passes unnoticed.

To address this gap, some Member States cover data protection aspects more prominently. For instance, Denmark informed FRA that it has a leaflet on VIS at its embassies.It informs that VIS will assist the visa processing, but that it can also be used when apprehending migrants in an irregular situation and by law enforcement authorities. It also includes information about the possibility to correct wrong data and the authority to turn to for data corrections. The European Commission has published different materials (a leaflet, factsheet and poster) with information on VIS.[81]

80 FRA Biometrics project, Visa applicants survey, 2016, questions "If you were informed in writing, did you find the information provided understandable?" and "If you were informed orally, did you find the information provided understandable?"

81 European Commission, E-library website.

Figure 5: Information provided to visa applicants by staff in charge of fingerprinting at last application for a short-term visa (%)



Notes: *The number of respondents varies for the replies, ranging from 570 to 574 persons. The results are based on the survey question "Thinking about the last time you applied for a short-term visa and provided fingerprints, what information were you given by the staff in charge of fingerprinting before your fingerprints were taken? Please tick all that applies."*

* *National Data Protection Authority.*

Source: *FRA Biometrics project, Visa applicants survey, 2016*

No special arrangements for children or persons with impairments

Pursuant to Article 24 of the Charter, the right to information is a precondition for the child to exercise its right to be heard in judicial and administrative proceedings affecting them, which is protected by Article 12 of the Convention on the Rights of the Child (CRC) and Article 24 (1) of the Charter. According to Article 12 of the GDPR, the controller must take appropriate measures to provide information on data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Pursuant to Article 21 of the Convention on the Rights of Persons with Disabilities,[82] State Parties must ensure that all persons with disabilities can enjoy the "freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice". This includes providing public information in accessible formats and technologies suitable for persons with disabilities.[83] Elderly people are more likely to suffer from, for instance, visual and hearing impairments, and the Charter also includes the respect for the elderly to lead a life in dignity and independence (Article 25).

There were no special arrangements for providing information for children or persons with disabilities. With respect to children, the provision of information is usually not altered to make it understandable. Usually, parents accompany their children and so they are not individually informed. Similarly, there is no special method of addressing issues of providing information to persons with intellectual disabilities or for people with visual or hearing impairments.

82 United Nations (UN) (2006), Convention on the Rights of Persons with Disabilities, 13 December 2006.

83 *Ibid.*, Art. 21 (a).

1.4. Information given to people when personal data are checked

This chapter looks at the information given to people when their personal data are checked against records in large-scale IT systems. It first examines information given to travellers when their documents are checked at the border. Then, it reviews information given to people apprehended within the territory and finally when people request a residence permit.

The legal instruments for the EU IT systems do not regulate the right to information when data stored is subsequently searched, with the exception of the Eurodac Regulation. Although the EU data protection framework does not confer a right to information when authorities are consulting already stored data, certain obligations could be derived from the right to good administration, for example, when a decision on the future of a third-country national is based on information processed in large-scale IT systems.

1.4.1. Checking IT systems at border crossing points

When third-country nationals cross the external borders of the Schengen area, they are checked against national databases and SIS II, as are EU nationals since April 2017. Visa holders are also checked against VIS.[84] In addition, with the entry into force of the Entry-Exit System (EES), an entry record of each third-country national will be created. Such record will include biometric data.

First line checks

Border checks are carried out in two steps. Every person crossing the border to the EU undergoes a 'first line check'. Checks against SIS II are mandatory and are carried out with alphanumeric data. VIS should be checked with the visa number in combination with the fingerprints.[85] According to the Commission evaluation of VIS, verification against VIS has been mandatory since October 2011, but the implementation of this obligation remains unsatisfactory and varies greatly between Member States.[86] Biometrics of third-country nationals may also be checked upon exit from the Schengen area.[87]

The traveller will typically not be informed that checks are made against SIS II during first line checks, although at several BCPs (border crossing points) leaflets are distributed,[88] which the European Commission has produced.

For VIS, only information necessary to carry out the procedure practically is usually provided, for example, the instruction to "place your finger here". Travellers do not ask any questions at borders. They have a submissive attitude to pass the controls without problems.

Some Member States have made additional efforts to provide information. Poland, for example, has produced leaflets that are distributed at the border crossing points with a description of the VIS regulations, requirements, and instructions on how to provide fingerprints.

According to the small-scale survey carried out among border guards, very few provide written information. Every second first line officer that was interviewed indicated that they never provide written information and another third of the first line officers did not answer this question.

Second line checks

During second line checks, travellers have the right to receive written information about the purpose of the second line check and its procedure, according to the Schengen Borders Code. They must be given written information in a language which they understand or may reasonably be presumed to understand.[89] The general duty to inform may include checks against IT systems, although such are not specifically mentioned.

Frequently, travellers only learn about the entry ban in SIS II during a second line check. Border guards undertaking the check cannot see the underlying reasons for an alert in SIS II without contacting the Supplementary Information Request at the National Entries (SIRENE) office.

Most of the border guards interviewed said that during second line checks they provide information about how to exercise the right of access, correction or deletion by directing the person to the relevant webpages. This may not necessarily be effective as illustrated by the

84 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ 2016 L 77/1, Art. 8; Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders, OJ 2017 L 74/1, Art. 1.
85 VIS Regulation, Art. 18 (1).
86 European Commission (2016d).
87 Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders, OJ 2017 L 74/1, Art. 1 (4).
88 European Commission (2013b).
89 Schengen Borders Code, Art. 8 (5).

following example. In Poland, the contact information of the controller and the national data protection authority is provided, but providers of legal assistance who were interviewed in the project said that people do not leave the border crossing point with knowledge that they have the possibility to access their personal data.

According to the results of the small-scale border crossing points (BCP) survey, when border guards refuse entry to somebody because they have an entry ban in SIS II, most often they also provide some information to the person concerned about possible next steps. Most commonly, border guards inform them about their rights and they tell them where they may receive legal assistance or complain about the decision.

Interpretation bottlenecks may sometimes occur which are not adequately handled. In Sweden, researchers observed the case of a woman referred to a second line check (as the picture looked different from her appearance) who did not speak Swedish and where her children acted as interpreters.

1.4.2. Information given to persons apprehended within the territory

A person who is apprehended within the territory may, for immigration control purposes and within police checks, be checked against data stored in Eurodac,[90] VIS,[91] SIS II,[92] and, in future, the EES.[93]

Almost half of the Schengen Member States have information leaflets on SIS II.[94] As a rule, they include information about the purpose of SIS II as well as possibilities to correct or delete incorrect data and the authority to turn to for data corrections. This was part of an EU-wide information campaign on SIS II and the rights of the persons it affects, led by the Commission in collaboration with the Member States and the EDPS. The campaign involved the production and distribution of posters, leaflets and video animation.[95]

The amount of information provided depends on the type of alert, with officers having significant discretion. For alerts in SIS II of a criminal nature, providing the individual with information about their personal data processing would disrupt police investigations. For this reason, it is very rare that officers will inform an individual that a search is being carried out. Such limitations are also in line with Article 13 (3) of the Police Directive.

Concerning the use of SIS II to store entry bans, during the FRA field research, several cases emerged where the person concerned was not aware that they had been issued an entry ban. For example, a Moroccan citizen only found out about the existence of an entry ban after he had married a Spanish citizen and could not enter Spain. A Swedish border guard told the researcher that they regularly have cases of people who thought that their entry ban had expired, whereas it had been prolonged without them being aware.

Sometimes the apprehended third-country national is informed that an entry ban exists, but not how to exercise the right of access, correction and deletion. The apprehended migrants will hear they have an entry ban but not much more, according to a police officer in Belgium.

"I'm not going to say that we tell them everything, but we do say that they have an entry ban in SIS, so they know [the migrants]." (Police, male, Belgium)

In case of families, there is also a risk that the communication will be directed to the male person only, and not to the wife and the rest of the family. A man apprehended in Melilla, Spain, was individually called to be informed about the reason to provide fingerprints and about what would happen next, whereas he would have preferred to go with his family.

1.4.3. Information given when checking IT systems before issuing a residence permit

When a third-country national applies for a residence permit, a mandatory check is carried out to see if there are any obstacles preventing the issuance. This includes a check in SIS II.[96] There is no explicit duty to inform the person that such a check is carried out, as generally there is no duty to inform when searches are carried out.

Residence permits are issued according to a uniform format common for all Member States.[97] They are not stored in EU IT systems. Rather, many Member States store them in national databases. The right to information is, in this context, regulated by national law and the GDPR applies.

90 Eurodac Regulation, Art. 17.
91 VIS Regulation, Art. 19.
92 SIS II Regulation, Art. 27 and SIS II Decision, Art. 40; SIS II borders proposal, Art. 29, SIS II return proposal, Article 12; and SIS II police proposal, Art. 43 (1) (b).
93 EES Regulation, Art. 26 and 27.
94 At least Austria, the Czech Republic, Denmark, Germany, Greece, Malta, Poland, Romania, Slovenia and Sweden.
95 SIS II Supervision Coordination Group (SIS II SCG), *Activity Report 2013-2015*, p. 13.
96 SIS II Regulation Art. 27 (3); SIS II proposal on border checks, Art. 29 (1) (d); SIS II return proposal, Art. 13; SIS II police proposal, Art. 43 (1) (d).
97 Council Regulation (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, OJ 2002 L 157/1.

Applicants for a residence permit are typically not aware that a check in SIS II is carried out, according to FRA field research. For example, an immigration officer interviewed in Sweden said that they do not inform residence permit applicants that their personal details will be checked in SIS II or the against the national database, *Misstankeregistret och brottsregistret* (MRBR).[98]

Similarly, a residence permit holder in Spain explained that she was not properly informed about why she should provide her fingerprints when the permit was issued and renewed.

"So, for example, I would like to know if my fingerprints eventually get erased or if I have any problems with my fingerprint in a different country, what the procedure is and how it ends? If in this case, I will be able to enter that country, or whether they will return me or even arrest me." (Regular migrant – other, Ukrainian female, Spain)

Conclusions

Ensuring that people understand the consequences when their biometric and other personal data are stored in large-scale EU IT systems is challenging for a number of reasons:

1) the duty to inform individuals focuses on the moment when fingerprints are collected and stored, not when the data are subsequently used to inform decision making;

2) the person or data subject often has more urgent priorities or is simply not aware of the importance that stored personal data may have for future decisions affecting them;

3) information provided on the purpose of processing biometric data remains technical and difficult to understand, with hardly any efforts to deliver it in a manner that is sensitive to the age, gender and background of the person concerned;

4) if IT systems are made interoperable, the provision of information must cover the different types of processing envisaged.

Providing adequate and understandable information on the purpose of fingerprinting for Eurodac appears most difficult, particularly if the information is collected in stressful situations. The consequences of a registration in Eurodac for asylum applicants or an apprehended migrants are not always explained or understood. If authorities do not provide information, or only provide partial information, asylum seekers and migrants in an irregular situation view this as the Member State acting in a non-transparent manner, according to FRA research. This will impact on their willingness to co-operate with the authorities. More transparency would foster trust and strengthen the credibility of the European asylum and migration procedures among concerned individuals and promote their cooperation.

Only very few visa applicants surveyed within the field research said that they have received information about the purpose of the data processing, or how to exercise the right of access, correction or deletion of data, in spite of such information being included in the visa application form.

The right to information must cover all purposes of the data processing, including how to exercise the right of access, correction and deletion. Neither for Eurodac nor for VIS are persons concerned fully informed, as research findings show. A major difficulty is that the information systems are used for a number of purposes and processes. If information systems are made interoperable, challenges will further increase. Should the minimum age of processing of biometric data in Eurodac be reduced to six years of age, particular efforts are needed to find appropriate ways to inform children.

In its FRA opinions 1–3, FRA suggests ways to improve the provision of information, making the process more transparent and the information provided better understood. In this regard, Schengen evaluations can play an important role to promote good practices.

98 Sweden, Registers of suspects and convicted crimes (*Misstankeregistret och brottsregistret*).

2 Respect for human dignity when taking fingerprints

Charter of Fundamental Rights of the European Union

Article 1 – Human dignity

Human dignity is inviolable. It must be respected and protected.

This chapter deals with the way officers take fingerprints from asylum and visa applicants and how the dignity of the person is respected. It examines how heavy physical work and the physical impossibility for some people of providing fingerprints, due to skin texture or disability, can impact on how people are treated when providing their fingerprint data. It describes how vulnerable persons, due to their physical or mental condition, as well as suspected victims of trafficking in human beings, are treated, and analyses how their dignity is affected.

The chapter also looks at people's unwillingness to provide fingerprints, which mainly occurs within the asylum procedure, and the reasons behind this. It discusses how asylum seekers have resorted to self-injury as a means to avoid fingerprinting, and the treatment of those suspected of having done so, even if they were physically unable to provide their fingerprints. It includes testimonies from asylum seekers and migrants of experiences of use of force and detention as part of the fingerprinting process. It analyses the impact on the right to asylum and how the principle of non-*refoulement* is affected, and how the use of coercive measures affect the right to physical integrity and the prohibition of torture, inhuman and degrading treatment or punishment.

2.1. Human dignity is inviolable

Article 1 of the EU Charter states that human dignity is inviolable and that it must be respected and protected. Article 1 is the foundation of all fundamental rights in the Charter. The CJEU has confirmed in its case law that the fundamental right to dignity is part of EU law.[99]

People may perceive the taking of their biometric features in an unpleasant way, as noted by an expert interviewed by FRA.

"[S]ome people might not feel comfortable that you are taking their body features and that you're making their body algorithmic [...] it can definitely humiliate people."
(Fundamental rights expert, female)

As shown in Table 5, a general clause on the right to dignity is included in VIS, EES and ECRIS-TCN.[100] Article 13 (1) (b) of the Eurodac proposal states that Member States must ensure that the data collected fully respect the human dignity of the person. SIS II does not include an explicit reference to the right to dignity. ETIAS is not included in the table since it does not contain fingerprints.

99 CJEU, C-377/98, *Netherlands v. European Parliament and Council*, 9 October 2001, paras. 70-77.

100 See also: Schengen Borders Code, Art. 7 (1) and Visa Code, Art. 39 (2) and Recital 6, which include references to the right to dignity.

Table 5: The right to dignity in EU legal instruments

Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS II Regulation and** *border proposal*	*SIS II return proposal*	**EES Regulation**	*ECRIS-TCN proposal*	*Interop. proposals*
no	yes	*no*	*no*	*no*	yes	*yes*	*yes*

Note: *Proposed legislation in italics*

Source: *FRA, based on existing and proposed legislation (2017)*

2.2. Treatment when taking fingerprints: general findings

In general, the officers interviewed within the FRA field research described the process of taking fingerprints as smooth and normal, although some problems relating to the quality of fingerprints or refusal to provide fingerprints emerged.

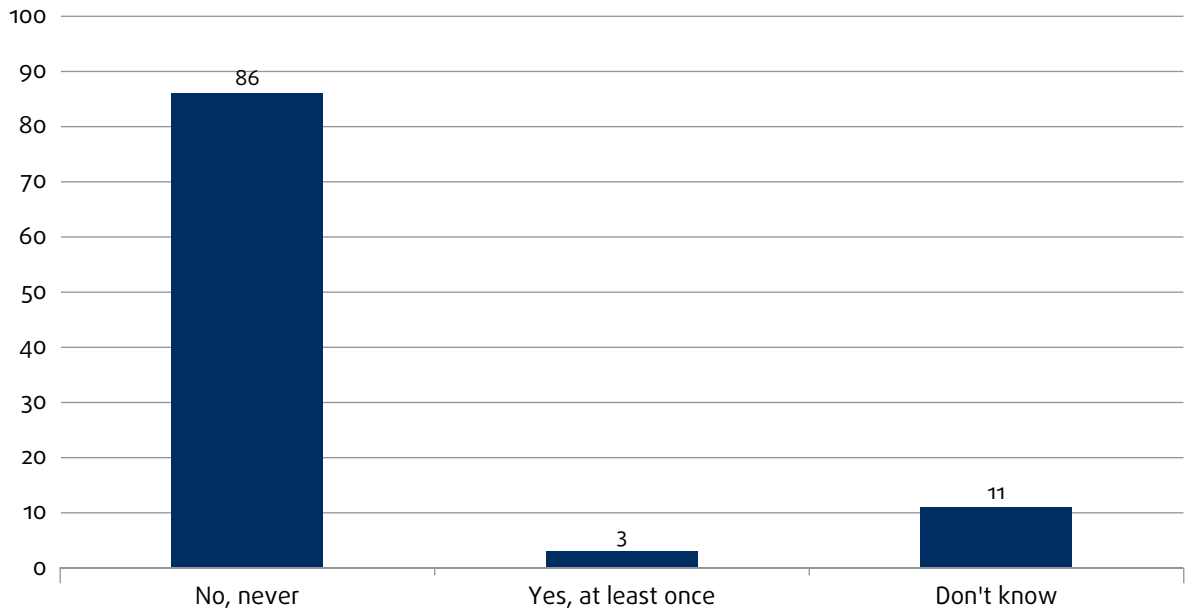
In the case of Eurodac, providers of legal assistance are not present during the fingerprinting, but their impression based on their contact with asylum seekers and apprehended migrants was that there were not too many problems. Some asylum seekers and migrants interviewed in Italy noted the kindness of the police officers during the enrolment procedure. Normally, food and medical support are provided before the fingerprinting process with newly arrived migrants. Nevertheless, the research also documented instances of disrespectful and even inhuman treatment when the person concerned refused or is believed to refuse the fingerprinting. As described in Section 4.5 some of these incidents are very serious.

Stress is likely to impact on fingerprinting, particularly on less experienced staff.

"If there are 40 people standing there and waiting, and you have one person who [for whom it is difficult to take fingerprints], then of course it can affect [how the staff act]. That is the way it is, unfortunately." (Immigration Agency, female, Sweden)

The collection of fingerprints from visa applicants at DMCPs is generally smooth and lasts about three to five minutes. In the small-scale survey FRA conducted at DMCPs or their service providers, visa applicants were asked whether they were ever treated disrespectfully when their fingerprints were taken. Although the large majority (86 % of the interviewed visa applicants) denied this, some 3 % said that they experienced disrespectful treatment at least once (see Figure 6).

Figure 6: Experience of disrespectful treatment while providing fingerprints (%)



Note: *The results are based on the survey question "In general, have you ever been treated disrespectfully, when your fingerprints were taken?" (n = 571)*

Source: *FRA Biometrics project, Visa applicants survey, 2016*

Fingerprints of visa holders should also be checked at border crossing points to verify that the person is the same as the one indicated in the visa.[101] Due to work pressure and other reasons, during first line checks in four of the six EU Member States covered by the research (Belgium, Germany, Spain and Sweden) such a verification is not systematically carried out. During the non-participant observations, a few instances of retaking of fingerprints were observed. If there are difficulties with the fingerprinting in the first line check, which should be carried out in about 90 seconds, the person is typically sent to a second line check.

2.3. Treatment of vulnerable people

During the **initial registration for Eurodac**, officers may be able to identify vulnerabilities. This could be by asking if there are any physical and/or mental illnesses or concerns that the persons to be registered want to share. In Germany, new arrivals fill in a form about themselves, which is available in different languages and can help identify vulnerabilities (respondents mentioned, for example, how they became aware of a traumatised child in this way). In case vulnerabilities are revealed, the registration process is carried out in a separate room to ensure a calm atmosphere. In Sweden, interviewed officers said that they try to pay attention to whether the asylum applicant is very quiet, confused, sad, afraid, or under the influence of alcohol or drugs. They then try to be very calm, and ask them to write things down, giving the applicant the opportunity to ask questions and to speak. Officers in several Member States said that it is common sense to understand when one needs to talk or to treat people slightly differently.

"So if you have a very, very old person in front of you who has very reduced hearing then I hope that you don't speak in the same way as you speak to someone who has perfect hearing, if that is what you mean. For me that is common sense." (Immigration Agency, male, Sweden)

Italy has a unit specialised in issuing residence permits for **victims of trafficking in human beings**. In Spain, a suspected victim may choose which out of three agents in the service will take the fingerprints. Then, only that person stays with the person to be fingerprinted and they close the door, so that the victim feels more comfortable. If needed, officers also can go to the victim's accommodation to take fingerprints.

Gender sensitive measures when enrolling fingerprints of women are rare. However, at one of the German Federal Offices for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge* – BAMF) field offices, respondents mentioned that women are enrolled by female officers.

In the small-scale survey that FRA carried out at DMCPs and their service providers, staff were asked whether specific measures are taken for seven different groups of vulnerable people and, if so, how often. The VIS Regulation prohibits discrimination based on, amongst others, disability and age.[102] As shown in Figure 7, the responses vary according to the type of vulnerability, with special arrangements being more frequent for older people and people with physical disabilities. Some 63 % and 61 % of DMCP officers and staff at service providers indicate that at least sometimes specific measures are taken for older people and for people with physical disabilities, respectively. For children, on the other hand, specific measures are never taken, as indicated by 44 % of DMCP officers and staff at service providers.

In such situations, DMCP officers and staff at their service providers most often ask the person accompanying the visa applicant to also be present during fingerprinting (64 %), or they carefully explain the procedure to the vulnerable person that is being fingerprinted (36 %).

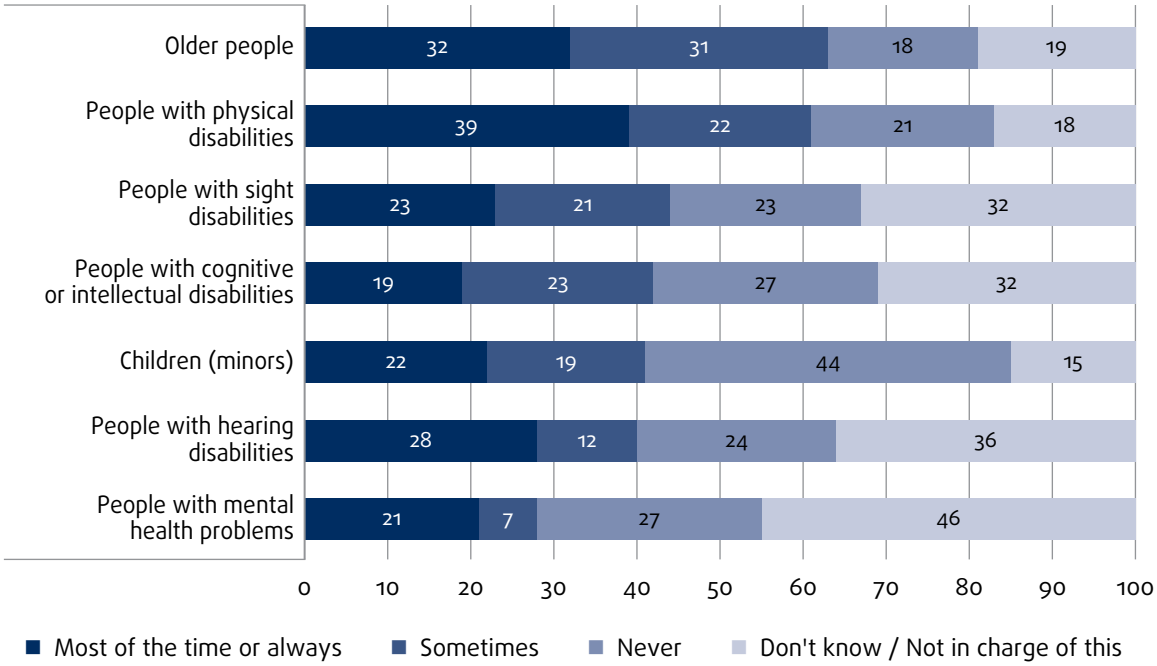
Observations during the field research, however, do not corroborate these findings. Observations at DMCPs and their service providers indicated that typically all applicants were treated the same, although wheelchairs and small steps for children were available in some DMCPs (VFS Lagos and Lviv). FRA observed a scenario where persons accompanying a visa applicant helped by pressing his hand onto the fingerprinting device. As the embassy staff were behind a glass window, they were unable to help. The set-up of service providers may allow face-to-face enrolment allowing the staff to better help during the enrolment.

Staff of DMCPs and their service providers participating in the small-scale survey were also asked if they received training or guidance on how to enrol fingerprints of vulnerable people. Service providers receive more training on treatment of vulnerable persons during the fingerprinting process than DMCP staff, as illustrated in Figure 8. Training of both groups include treatment of people with physical disabilities, older people and children, with 50–59 % of staff members reporting to have received some training in enrolling these groups. Training less often includes treatment of persons with hearing, sight or intellectual disabilities or mental health problems.

101 VIS Regulation, Art. 18.

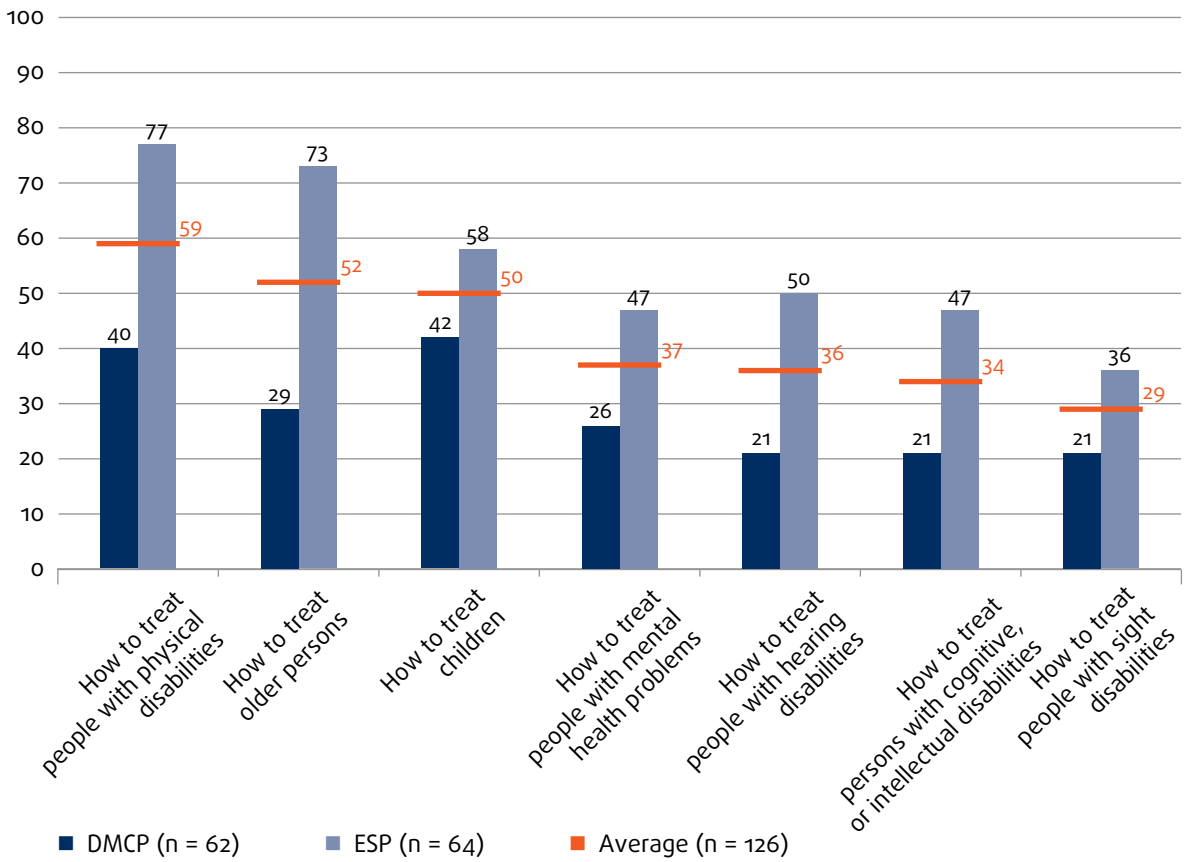
102 VIS Regulation, Art. 7 (2).

Figure 7: Frequency of taking specific measures for vulnerable people during the fingerprinting process (%)



Note: *The number of respondents varies for the replies, ranging from 90 to 115 persons. The results are based on the survey question "For which of these groups are specific measures taken and how often?"*
Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

Figure 8: Staff training and/or written guidance (guidelines, manuals) on enrolment of fingerprints of vulnerable people (%)



Note: *The results are based on the survey question "On which of the following issues have you received training and/or written guidance (guidelines, manuals)? Please select all that apply."*
Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

Visa applicants were asked if they thought that special adjustments should be made for people in a vulnerable situation during the visa application process, including when fingerprints are taken. About half of the surveyed visa applicants believed that special adjustments should be made for, in particular, people with physical disabilities, older people, and people with hearing disabilities. About one third of them believed that such adjustments should also be made for pregnant women and children.

2.4. Physical impossibility to provide fingerprints

In case a person cannot provide fingerprints, they could in certain situations risk facing negative consequences in comparison to persons who were able to provide fingerprints. The general principle of equal treatment in Article 20 of the Charter requires that comparable situations are not treated differently and that different situations are not treated alike, unless objectively justified. According to Article 21 of the Charter, discrimination based on any ground, such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation is prohibited.

The UN Convention on the Rights of Persons with Disabilities obliges States Parties to eliminate obstacles and barriers to accessibility to ensure that persons with disabilities have equal access to all aspects of life.[103] It prohibits all discrimination on the basis of disability (Article 5) and sets respect for inherent dignity and non-discrimination as general principles (Article 3 (a) and (b)). The European Court of Human Rights (ECtHR) has held that Article 14 of the ECHR protects against discrimination on the basis of disability.[104]

The legal instruments do not refer to equality before the law, with the exception of ECRIS-TCN in Recital 22, which also refers to the right to non-discrimination. The right to non-discrimination is also included in the VIS Regulation,[105] as well as the EES Regulation.[106] Age and disability are explicitly included among the listed discrimination grounds.

The VIS Regulation and the EES Regulation exempt persons who cannot provide fingerprints from the obligation.[107] Such a provision is absent in the Eurodac Regulation. However, it follows from the wording in Article 2 (4) of the Eurodac Regulation that Member States must not attempt to re-take the fingerprints or facial image of a child or a vulnerable person when the reason for non-compliance is related to the conditions of the fingerprints or facial image or the health of the individual.

Persons in wheelchairs may be unable to provide fingerprints of acceptable quality, because of the angle they will have to place their fingers on the machine. Moreover, if a person lacks an arm, fingerprinting altogether becomes impossible. Some people may be unable to provide fingerprints of acceptable quality because the fingertip texture is affected due to manual work, old age or impact of the weather.

By September 2013, 966,539 visa applicants in VIS were physically incapable of providing fingerprints, when applying for a Schengen visa, according to the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).[108] Figures for Eurodac do not exist.

Table 6: Equality before the law and the right to non-discrimination in the legal instruments

Rights	**Eurodac and** *Eurodac proposal*	**VIS**	**SIS II Decision and** *police proposal*	*SIS II return proposal*	**SIS II Regulation and** *borders proposal*	**EES Regulation**	*ECRIS-TCN proposal*	*Interop. proposals*
Equality before the law	no	no	no	no	no	no	yes	no
Non-discrimination	no	yes	no	no	no	Yes (Recital)	yes	yes

Note: *Proposed changes and legislation in italics.*

Source: *FRA (2017), based on existing and proposed legislation*

103 UN, Convention on the Rights of Persons with Disabilities, Art. 9.

104 ECtHR, *Glor v. Switzerland*, No. 13444/04, 30 April 2009; ECtHR, *Pretty v. the United Kingdom*, No. 2346/02, 29 April 2002.

105 VIS Regulation, Art. 7 (2).

106 EES Regulation, Recital 19.

107 VIS Regulation, Art. 8 (5); EES Regulation, Art. 17 (4).

108 eu-LISA (2016), p. 26.

Fingerprinting for Eurodac – physical impossibility to provide fingerprints causes suspicion

The physical impossibility to provide fingerprints for Eurodac may result in a suspicion that the asylum applicant is trying to avoid fingerprinting.

If it is physically impossible for the person to provide fingerprints, it is relatively rare that it is a case of deliberately damaged fingerprints, according to officers interviewed during the field research. Officers interviewed in Poland noted that there have been some cases involving persons arriving through Greece. In Spain, officers said that sub-Saharan Africans were most likely to have injured fingerprints, but this was not necessarily due to a deliberate injury, but due to the work they have done, the difficult journey on their way to Melilla/Ceuta, including stays in Mount Gurugú or attempts to jump the fence on the border with Morocco.

If officers fail to enrol fingerprints of an acceptable quality, they will re-take them until the quality is acceptable. In such cases of multiple attempts, the whole process that usually takes no more than a few minutes can last several hours. An asylum seeker in Sweden explained that due to the genetic skin texture of her fingers – her father had the same problem – the officer persisted in re-taking her fingerprints for an extended period of time, which make her feel like a criminal, in spite of the otherwise correct attitude of the staff.

Technology can also provide solutions in such situations. For people with rheumatic aches, deformed hands or similar conditions, the Swedish Migration Agency uses multispectral imaging technology (MSI) in such instances. Some officers also thought that the use of such technologies results in fewer asylum seekers deliberately attempting to damage their fingerprints.

Individuals can be requested to reappear to check that they have not purposefully damaged their fingerprints. For example, in Belgium, the individual has to reappear in two weeks. Such cases are typically handled as a case when it was temporarily impossible to take the individual's fingerprints. If fingerprinting is not possible, a note is attached to the file explaining the reasons for this. Alternative means of identification such as pictures or distinguishable marks (tattoos or scars) can be indicated instead. A Swedish provider of legal assistance explained that Iraqi forger works have burned fingertips, but that this does not affect the asylum procedure.

If the fingerprinting device is not working properly, an alternative method to capture the fingerprints is with ink on paper. This method does not disadvantage the individual and they can continue the process.

Fingerprinting for VIS

In general, visa applicants felt that they were treated respectfully when providing fingerprints. If fingerprints cannot be taken, the applicant receives products that moisten dry fingers and the device's screen is cleaned. In case of repeated failed attempts to capture fingerprints, the officers can cancel one of the ten fingerprints collected. There is also the possibility to lower the device's quality standards. At DMCPs where more visa applicants have damaged fingerprints due to manual work, the fingerprints may have to be retaken up to ten times, as noted during the non-participatory observation at the Polish VFS in Lviv.

Among the staff of service providers participating in FRA's small-scale survey, 87 % said that they had received training and guidance on what to do if it is physically impossible for the applicant to provide fingerprints, whereas 56 % of DMCP staff had received such training.

Physical impossibility to provide fingerprints may result in the application being processed without fingerprints. In FRA's small-scale survey, DMCP staff were asked if they think that decisions on applications with fingerprints are taken quicker or slower compared to those without fingerprints. Almost a third of them estimated that those applicants that cannot provide fingerprints will have to wait longer for the decision.

Fingerprinting for residence permits

A migrant interviewed in Spain said that she had difficulties in providing fingerprints both when applying for the residence permit in 2013 and renewing it in 2015. The scanner did not recognise the ridges in her fingers. Later she learned that her ridges are being naturally erased. She felt very nervous because the officer told her that the process failed. Although the officer mentioned an alternative way to get the residence card, the migrant's attention was on the fingerprints, as the officer indicated that the consequence could be expulsion from the country, and that other countries are very strict with fingerprinting and she could get into trouble there.

2.5. Unwillingness to provide fingerprints

Refusals to provide fingerprints happen mainly in the context of Eurodac and less in relation to borders, visas or return processes. Only in Poland, although rare, officers mentioned unwillingness to provide fingerprints by citizens from Eastern Europe and Central Asia, as they may possibly have a criminal record. However, these are rare occurrences, as most people are aware that providing fingerprints is integral to the asylum procedure.

"Asylum seekers are aware that if they are not following the procedure, they won't be let in." (Border guard, male, Poland)

Refusals to provide fingerprints for Eurodac are not common but do occur. A Polish officer estimated three cases of refusal per 400 applicants, although another said that refusals had never happened. Officers in Sweden and Germany said it happens about once a month. Avoiding or refusing fingerprinting happens more frequently in Spain, among arrivals in Ceuta and to some extent in Melilla as well as in Italy, where a police officer interviewed in 2016 said that 6 % of the arrivals refuse fingerprinting for Eurodac.

In 2015 and early 2016, refusals to provide fingerprints were relatively common among some nationalities in Sicily. Such refusals were based on the fear that processing the fingerprints in Eurodac would reduce their chance to move on to other EU Member States and stay there. In Lampedusa, in December 2015, approximately 200 Eritreans protested against the fingerprinting. The protests lasted for several weeks.[109] Other protests were reported in May 2016, among Sudanese, Somalis, some Yemenis and Eritreans.[110] According to data collected from the Immigration Office, in the hotspot of Pozzallo, the number of persons who refused to provide fingerprints amounted to 200 people out of around 7,000 people registered by June 2016. There were four or five cases in the hotspot of Trapani, out of around 4,000 people by June 2016.[111]

A frequent reason for refusing fingerprinting in Italy and Spain, is that these EU Member States are considered as transit countries and the intended destination country – where family members may be – lies further ahead. An Italian provider of legal assistance said that there is distrust in the family reunification procedures under the Dublin Regulation, as they take a very long time and relocation opportunities are limited. Nevertheless, the possibility of relocation changed attitudes.

"With the Dublin Regulation a lot of people didn't want to be fingerprinted, but with the new [relocation] procedure, it is the exact opposite." (Asylum and immigration Office, male, Italy)

When asylum seekers have been able to lodge the application in the intended destination country, reluctance to fingerprinting originates from the fear of being transferred back to the Member State of transit under the Dublin rules, particularly if they were badly treated when transiting. Another reason is not understanding the purpose of fingerprinting, for instance the belief that they would end up in a database for criminals, or that the fingerprints will be shared with the country of origin. In Poland, according to an officer this is mostly the case of applicants from the Caucasus.

Findings from the field research show that authorities have different ways of reacting to those who are hesitant to provide fingerprints. As a first step, the authorities would explain the purpose of the fingerprinting in a relaxed and friendly way. In some EU Member States, providers of legal assistance or cultural mediators may support the authorities in this, as explained in Section 1.2. A Swedish provider of legal assistance was, however, sceptical, and seriously concerned about the one-way communication. The authorities explain the reasons for providing fingerprints without listening to what the asylum seeker has to say. This suggests that the authorities are not open to statements that could possibly influence the interpretation of Dublin rules, which a provider of legal assistance in Sweden found worrying.

"[T]hey explain how it is, they explain how it works and how it should be, and then they have someone on the other side of the table who is trying to say something, but they are completely uninterested in listening to them. So they kind of just say that 'now it is like this, that fingerprints have been taken and that it is the same thing as an asylum application and now you have to go back to Italy' – 'Yes but I cannot go back to Italy' – 'Yes but this is the way it is'. And they don't take in [what the person says]. And I don't even know if you can call this persuasion, I mean, they make themselves into some form of machine that only delivers information, so that they can write in the protocol that they have said it." (Provider of legal assistance, female, Sweden)

Providing incentives for cooperation in case of resistance was also mentioned, such as a single cell or a telephone call in Germany for example.

109 According to an expert interviewed for this project, six people were then transferred to the Identification and Expulsion Centre (CIE) of Trapani Milo, five were fingerprinted and one resisted, spending two days on a chair in the police headquarter of Trapani Milo. For more information, see, Redattore Social (2015); See also: Commissione Straordinaria per la tutela e la promozine dei diritti umani, Senato della Repubblica (XVII Legislatura) (2017), p. 46.

110 See Repubblica (2016).

111 Data collected by the researcher from Immigration Offices-Section III (Pozzallo) and IV (Trapani).

Currently, the disembarkation takes place according to nationality to profile those considered easy to fingerprint. Such individuals are immediately taken to reception centres without having been identified. Other nationalities expected to resist fingerprinting, such as Eritreans and Sudanese are hold in the port or hotspot, such as Lampedusa. It takes 48 to 72 hours for the Scientific Police to complete the standard fingerprinting procedure in the hotspot.

As observed at the hotspot in Pozzallo (Italy), in 2016, if an individual refuses to be fingerprinted, it is noted down on the police registration form (*foglio-notizie*) with the date and time. Once the police have completed the fingerprinting for the day, they make a list with those who refused to give their fingerprints. An explanation of the purpose of fingerprinting is provided once again with the help of an interpreter. This process is video recorded to collect evidence for possible future procedures. Other actors, for example, staff from Frontex, EASO, or international humanitarian organisations, if present, may also help to explain.

"We try to convince them. I must say that the EASO in this respect manages to speak pretty well with guests and to convince them." (Asylum and Immigration Office, male, Italy)

Those who still refuse fingerprinting are given a two to three days reflection period in the hotspot. If the police cannot fingerprint the new arrivals, they make a record on the *foglio-notizie* and this is submitted to the prosecutor for a possible referral to the judicial authorities, while the people are transferred to reception centres. According to an officer, usually after the transfer the migrants change their minds and apply for asylum providing their fingerprints, as asylum is their only option to avoid being undocumented in Italy.

Registration in Eurodac

Persons in need of international protection may resort to self-harm to avoid fingerprinting with the aim of trying to reach their preferred country of destination. Cases of asylum seekers using acid, or other means to destroy their fingerprints or harming themselves to avoid registration in Eurodac have been known for several years.[112] Although rare, according to a German expert, spoofing – which is to falsify an identity by manipulating the fingerprint using silicone, for example – may occur.

Although EU Member States do not collect statistics on incidents of self-harm, one out of three EU Member States (Austria, Belgium, the Czech Republic, Denmark, France, Ireland, Malta and Sweden) reported to FRA in late 2015 that they are aware of such incidents. Examples of self-harm emerged from all six EU Member States covered by the field research. Some interviewees in Germany said that incidents of self-injury were more frequent a few years ago, particularly among Somali migrants. The use of scanners able to take high quality fingerprints contributed to the decrease of such incidents.

If the authorities suspect that the person has deliberately injured the fingertips, the asylum seeker may typically be asked to reappear, in Belgium, for example, as many as ten times, and in Germany, three times. According to a Swedish provider of legal assistance, in one case, an asylum applicant regularly had to reappear for fingerprinting for one year. The problem with fingerprinting did not affect the applicants' access to the asylum procedure.

An expert underlined that asylum applicants who burn their fingerprints or manipulate their bodies should not be viewed as fraudsters, since it is the "politics that force them to harm their bodies". Furthermore, UNHCR experts stated that self-harm is of great concern and emphasised that even if self-harm is often related to onward movements, it also comes from despair.

Other procedures

During border controls, border guards occasionally find deliberately injured fingerprints (with silicone or etching the lines). An officer in Germany said that in this case, the fingerprint will nonetheless be taken, if necessary after repeating the process two or three times. At Barajas airport, they have had two to three cases as far as the respondent can remember. One police officer explained that this was more frequent some years ago, during the nineties before they were scanned. If there is suspicion that a visa applicant has deliberately inured the fingertips, the Spanish authorities informed that the embassy or the consulate has the right to call the applicant for an interview. No cases of deliberately injured fingerprints have been encountered at Swedish DMCPs, since applicants cannot obtain their visa if they refuse.

Apprehension of migrants in an irregular situation can be violent and stressful and the officers interviewed complained of a heavy workload. A useful approach would be to have different staff in charge of fingerprinting, which may not be possible during night shifts (Belgium).

"At night for example, we are just with one crew. So that's two people doing all the work. Maybe exhaustion could be a factor, and like I said, maybe they have been fighting with that person, maybe violence was used, they might have spit or cursed at them, all kinds of things can happen. It's mostly the first intervention that gives the stress when taking fingerprints." (Police, male, Belgium)

112 See, for example, Feng, J., Jain, A.K. and Ross, A. (2009).

2.5.1. Impact on asylum and the principle of non-refoulement

Article 31 (8) (i) of the Asylum Procedures Directive envisages the possibility to examine applicants who refuse to give fingerprints for Eurodac in an accelerated manner and/or through a border procedure or in transit zones. Refusal to provide fingerprints does not affect the Member States' duty to respect the principle of non-*refoulement*. It is the cornerstone of the right to asylum set forth in Article 18 of the Charter, as well as a core element of the prohibition of torture, inhuman or degrading treatment or punishment under Article 3 of the ECHR, as explicitly guaranteed by Article 19 of the Charter. Save for the very exceptional situation as specified in Article 21 (2) of the Qualification Directive (2011/95/EU),[113] under EU asylum law, the prohibition of *refoulement* is absolute, meaning that it applies to everyone, independent of the person's status or behaviour. Member States are bound by the principle of non-*refoulement*, regardless of whether or not the individual concerned has requested asylum.[114]

In the Netherlands, the District Court in The Hague stated that declaring the case not admissible because an asylum seeker had manipulated the fingertips so that these could not be taken, without considering the substance of the application, is unlawful.[115]

Nevertheless, officials interviewed during the field research explained that a refusal to provide fingerprints or a deliberate injury affects the asylum procedure. Officials interviewed in Belgium stated that the application would be rejected if the person did not cooperate and there was suspicion of fraud. In Germany, if an individual does not cooperate with the authorities this can lead to the suspension of the asylum process, according to Section 30 (3) of the Asylum Procedure Law.[116] In Sweden, the asylum process does not proceed.

In Poland, refusing to provide fingerprints is interpreted as a withdrawal of the will to submit an application. For persons applying for asylum at the border, the effect is a refusal of entry, according to interviewees in Poland and Spain – the two countries where research at the land border took place.

"It is explained to them that if they seek asylum but do not cooperate, they are not entitled to asylum. […] They do not end up rejected, in the end they go along because they want to avoid rejection." (Border guards, male, Spain)

If access to the procedure is granted, suspicion of avoiding fingerprinting through self-harm can also affect the credibility of the asylum applicant, as a Swedish officer noted.

Promising practice

Safeguard against impacting the trustworthiness of the asylum applicant

Unless the asylum seeker confirms that they have deliberately destroyed their fingerprints, the Swedish Migration Agency will not document any suspicions so as not to impact on the trustworthiness of the applicant.

2.5.2. The right to physical integrity and the prohibition of torture, inhuman and degrading treatment or punishment

Some EU Member States allow for the use of coercive measures to take fingerprints.[117] Use of force must be lawful. This means that it has to be provided for by law, not just in an internal instruction. Such law must be sufficiently precise to enable a person to understand it and predict its application in practice.

None of the legal instruments regulating the EU level IT systems explicitly prohibit the use of coercive measures. The proposal for a revision of Eurodac states in Article 2 (3) that Member States may introduce administrative sanctions, in accordance with their national law, for non-compliance with the fingerprinting process or with the capturing of their facial image. The sanctions shall be effective, proportionate and dissuasive.[118] Article 2 (2) of the Eurodac proposal also requires that the authorities fully respect the dignity and physical integrity of the child when taking their fingerprints and facial images. However, children and other vulnerable persons are exempt from

113 Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted (recast), OJ 2011 L 337/9. This provision implements in EU law Article 33 (2) of the 1951 UN Convention Relating to the Status of Refugees. It contains exceptions regarding refugees who constitute a danger to the security of a country or being convicted in final instance for a particularly serious crime, or who constitute a danger to the community.

114 See ECtHR, *Hirsi Jamaa and Others v. Italy*, No. 27765/09, 23 February 2012, para. 133. Also, the non-*refoulement* provisions included in Articles 4 and 5 of the Return Directive (2008/115/EC) applies to all migrants in return proceedings.

115 Netherlands, District Court The Hague (Rechtbank's-Gravenhage) (2011), Case No. AWB 09/31022, ECLI:NL:RBSGR:2011:BQ7082, 15 March 2011.

116 For details, see the Rechtslupe webpage on fingerprints in the asylum procedure.

117 European Commission (2014b), p. 1.

118 Eurodac proposal, Art. 2 (3).

administrative sanctions where enrolment of the fingerprints or facial image is impossible due to the conditions of the fingertips or face. The Member State authorities may retry taking the fingerprints if the child refuses to comply, only if it is fully justified and if there are no medically related reasons for the child's refusal.[119]

Article 3 of the ECHR always prohibits actions that cause feelings of fear, anguish or inferiority capable of humiliating and debasing a person. In assessing whether a public authority's conduct attains a minimum level of severity to come within the scope of Article 3, attention must be paid to all surrounding circumstances. The ECtHR attaches particular importance to injuries caused to persons who were subject to physical force.[120] This means that techniques that pose a danger to the individual's physical integrity and health must be avoided. Furthermore, use of force which aims to punish an individual for not giving their fingerprints would never be allowed.

Use of force that does not amount to inhuman or degrading treatment or punishment prohibited by Article 4 of the Charter and Article 3 of the ECHR can still raise fundamental rights concerns, particularly in light of Article 3 of the Charter, which enshrines the right of everyone to respect their physical and mental integrity. When force is used to compel a person to do something, the circumstances of each individual case must be assessed to determine whether the use of force was necessary and proportionate, and would thus still constitute lawful interference in light of the standards set forth in Article 52 (1) of the Charter.

Before resorting to sanctions or coercive measures, officers must provide asylum seekers and migrants in an irregular situation with the opportunity to comply with the duty to provide fingerprints. The person must be thoroughly informed, prepared and given enough time to decide whether or not to give their fingerprints. This will limit the question of whether coercive measures should be used to take fingerprints to exceptional cases.

Table 7 shows whether the instruments regulating IT systems contain specific references to the right to integrity and to the prohibition of torture, inhuman or degrading treatment or punishment. Two instruments – VIS[121] and the EES[122] – as well as the Eurodac proposal[123] include the right to physical integrity regarding children. Article 2 (2) of the Eurodac proposal also says that fingerprints shall be taken in a child-friendly and child-sensitive manner.

Table 7: The right to physical integrity and prohibition of torture in EU legal instruments

Rights	**Eurodac Regulation** and *proposal*	**VIS**	**SIS II Decision** and *police proposal*	**SIS II Regulation** and *borders proposal*	*SIS II return proposal*	**EES Regulation**	*ECRIS-TCN proposal*	*Interop. proposals*
Physical integrity	no *yes*	yes	no	*no*	*no*	yes (Recital)	*no*	*yes*
Prohibition of torture	yes	no	no	*no*	*no*	no	*no*	*no*

Note: *Proposed changes and proposed instruments in italics.*

Source: *FRA, based on existing and proposed legal instruments (2017)*

The European Commission has issued a guidance paper on how to implement the duty to take fingerprints[124] on which civil society commented.[125] The Commission encouraged biometric registration – if necessary by the use of force – during the registration at hotspots.[126] Italy issued a circular letter in 2014, according to which the authorities may use force when fingerprinting for Eurodac purposes.[127] A flyer distributed by the Italian Ministry of Interior states that "the police authorities will obtain pictures and fingerprints anyway, even with the use of force".[128]

In October 2015, FRA complemented these initiatives by producing guidance to assist EU Member States and EU agencies in avoiding fundamental rights violations when promoting compliance with the duty to provide fingerprints.[129] FRA underlines that authorities should secure compliance with the obligation to provide

119 Eurodac proposal, Art. 2 (4).
120 For example, ECtHR, *R.L. and M.-J.D. v. France*, No. 44568/98, 19 May 2004, para. 68, and *Rehbock v. Slovenia*, No. 29462/95, 28 November 2000, para. 72.
121 VIS Regulation, Art. 7 (2).
122 EES Regulation, Recital 19.
123 Eurodac proposal, Art. 2 (2).
124 European Commission (2015b).
125 European Council of Refugees and Exiles (ECRE) (2015); Statewatch (2015).
126 European Commission (2016c).
127 Italy, Ministry of Interior (2014), Circular letter 400/A/2014/1.308 issued on 25 September 2014, which authorises the use of force when asylum seekers refuse to have their fingerprints taken.
128 Italy, Ministry of Interior, flyer for migrants entering Italy.
129 FRA (2015b).

fingerprints for Eurodac through effective information and counselling, carried out individually as well as through outreach actions targeting migrant communities. The guidance includes a ten-point checklist.

The purpose is to acquire fingerprints of an acceptable quality. The hand needs to be relaxed during the fingerprinting process to produce good quality fingerprints. According to Spanish authorities, the use of force may lead to bad quality fingerprints. Therefore, despite law allowing the use of force, it is not used in practice in Spain.[130] Experts from Belgium and Spain noted that the use of force would affect the quality of the scanned fingerprint, and the effectiveness of the measure is questioned.

"One thing is clear: you cannot force someone to provide fingerprints, because you won't achieve a sufficient quality." (Immigration and Asylum Office, Spain)

Allegations or reports of incidents involving the use of force to take fingerprints for Eurodac emerged from several EU Member States in FRA's research. Experts consulted were concerned about the risk of re-traumatisation because of forced fingerprinting, particularly in the case of children. Several asylum seekers interviewed told that they had been subject to the use of force along the route, or that they had witnessed this happening to others in Austria, Bulgaria, Hungary, Greece, Italy and Poland, as the following examples show.

A Syrian couple, having transited **Austria**, explained that the authorities separated the adults from the children and that the police threatened the mother that she would not be able to see her children until she had provided her fingerprints. The couple claimed not having received any explanation as to why it was necessary to provide their fingerprints. The Austrian NGO *Diakonie Flüchtlingsdienst* also reported observing fingerprints taken roughly and coercively in Initial Reception Centres (*Erstaufnahmestellen*) and police detention centres in Austria.

In another situation, an 18-year-old asylum applicant said he escaped the queue for fingerprinting when he transited through **Bulgaria**. The police chased him threatening to kill him. He also said that police officers gave the person next to him in the queue an electric shock because he had not alerted them that he was escaping.

"When we were in the Bulgarian police station […] I was standing in the queue and I was the last guy. Five persons before me went for fingerprints. […] [w]hen they told me 'You, come here', I didn't listen to him and I ran away. There were more police after me, they stood up and they told me 'we'll shoot you'. But I managed to run away. […] There were more guys with me in the Bulgarian police station, and when I ran away from the police station they used an electrical shock on that guy, asking him why he did not tell them that I was running away." (Asylum applicant, Afghan male, Italy)

Several asylum applicants reported witnessing the use of force in **Hungary** during June 2015. After seeing the police beatings, they unwillingly accepted to give their fingerprints.

Two persons arriving in Sicily in **Italy** in 2015 reported to have suffered from or witnessed denial of food, water and shelter until they agreed to fingerprinting. In France, 38 mainly Sudanese migrants complained to the prosecutor in Pau that officers subjected them to torture and inhuman and degrading treatment after they refused to give their fingerprints upon arrival in Italy. Allegedly, they had been mistreated, beaten, arbitrarily imprisoned, blackmailed and/or deprived from water and food.[131] A provider of legal assistance explained that a client had received electroshocks. Furthermore, some officers confirmed the reports that use of force had happened in practice.

"First there is advice, then threats, then prolonged detention, then standing on a chair, maybe at night, in the office of the Scientific Police, then forcing through pressure on the arm to put the hand on the machine collecting fingerprints." (Provider of legal assistance, male, Italy)

The use of such strategies have been also reported for children and other vulnerable categories. An unaccompanied child in **Spain** explained that the police officer grabbed his arm forcefully and took his

130 European Commission (2014b), p. 1.

131 France, Le Monde (2018).

fingerprints. He said that he was not aware what was happening to him and why his fingerprints were taken.

In **Greece** an interviewee reported witnessing how a woman was beaten because she refused to take her veil off when having her photo taken.

"One woman who also had children, she was a Muslim, and they said 'you have to take that off' [indicates that he means her veil], and then take a photo, and this woman wouldn't do it [didn't take her veil off], and then I saw pah pah pah [that they beat] her as well. Because she didn't want to take it off, because there were a lot of people there and she was a Muslim, Afghan I think." (Migrant in an irregular situation, Iranian male, Sweden)

An Iranian interviewee pretended to be deaf when he was being registered in **Greece.** When the interviewee had his fingerprints taken, he explained that the police beat him for one or two hours, because he did not speak or hear and because he did not follow the correct procedure for having his fingerprints taken. He assumed that the police tried to see if he was indeed deaf by shouting loudly into his ears and by beating him. Even after they believed that he was deaf, they did not treat him in a better way.

Civil society actors have also reported on the use of force. According to ProAsyl, a German NGO, refugees had experienced the use of force when officers took their fingerprints in Bulgaria in 2015.[132] Also in 2015, the Berlin Centre for Torture Victims reported that 58.5 % of the patients had expressed humiliating and/or inhuman coercive measures when officers collected fingerprints. These included patients who had travelled through Bulgaria, Hungary and Italy.[133] During the period when an increased number of people crossed the border, asylum seekers experienced the use of force in Hungary and were beaten for refusing to provide fingerprints, according to Amnesty International.[134] Some asylum seekers interviewed by MigSzol reported similar experiences.[135] In addition, asylum seekers were denied water until they agreed to provide their fingerprints, according to Aida and the Hungarian Helsinki Committee.[136] During the same period, allegations of abusive behaviour also emerged in Italy. Amnesty International details experiences of migrants who had been coerced to give their fingerprints in Italy due to threats of violence, and who were subjected to beatings, the use of electrical batons, and even sexual humiliation when they refused to provide their fingerprints.[137] Also Oxfam, the Dutch Council for Refugees, the ECRE and others raised concerns over such practices.[138] The Italian Senate's Commission for the protection and promotion of human rights held two hearings on Amnesty International's report until December 2017.[139]

The EU allowed the use of force, but did not define it,[140] which led to fear for further legitimisation among civil society actors.[141] In a report on the progress of the implementation of the hotspots in Italy, the European Commission highlighted the need to improve the rate of fingerprinting to reach 100 % and encouraged Italy to adapt its legal framework to allow, when necessary, for the use of force to compel asylum seekers to have their fingerprints taken.[142]

On the other hand, according to the police in Taranto, coercive measures were allegedly not used. On a visit of the Commission for the protection and promotion of human rights to the hotspot in Taranto, the police reported that coercive methods or the use of force are not applied in fingerprinting procedures. The employees of international organisations present there reported that they observed moments of tensions in the past, but did not directly witness any violence by the authorities.[143]

Possible use of force for identification and registration must pass the proportionality test.[144] A German police officer expressed this as:

"In the last resort, breaking resistance. By literally taking them down and taking the prints." (Police, female, Germany)

Instances of disproportionate use of force in Belgium, Germany and Sweden did not emerge from the field research, although, the use of coercive measures are not prohibited. Providers of legal assistance were not aware of the use of force during registration procedures in Germany. Instead, interviewees pointed to the fact that migrants may experience harsh treatment in other states along their route to Germany. Officers in Belgium did not think that use of force was used as an encouragement to provide fingerprints, nor had providers of legal assistance interviewed registered

132 ProAsy (2015), p. 6.
133 Veigel, S. and Wenk-Ansohn, M. (2015) pp. 187, 189–191.
134 Amnesty International (2015).
135 MigSzol (2016), pp. 51–52.
136 Aida and the Hungarian Helsinki Committee (2016).
137 Amnesty International (2016).
138 Oxfam (2016), pp. 2 and 25–26; Dutch Council for Refugees, ECRE, Italian Council for Refugees, Greek Council for Refugees, ProAsyl (2016), *The implementation of the hotspots in Italy and Greece*, 2016, pp. 24, 51.
139 Commissione Straordinaria per la tutela e la promozine dei diritti umani, Senato della Repubblica (XVII Legislatura) (2017), p. 54.
140 Council of the European Union (2014).
141 Veigel, S. and Wenk-Ansohn, M. (2015), pp. 192.
142 European Commission (2015c).
143 Commissione Straordinaria per la tutela e la promozine dei diritti umani, Senato della Repubblica (XVII Legislatura) (2017), p. 54.
144 In, for instance, Germany in the Law on Residency (Article 49 and Article 62) but also the StPo (Article 81 b and Article 163 b) and in Poland in the Act on Border Guards of 1990 (Article 23).

any cases of use of excessive force. Testimonies from Poland and Sweden noted that the presence of a large number of police officers compels the person to comply with the obligation to provide fingerprints. In Sweden, the Migration Agency, in charge of fingerprinting asylum seekers can request the assistance of the police if they expect that the use of coercive measures could become necessary. One officer interviewed said that they had requested such assistance and another one said that their office had not yet done so.

In Spain, if a detained asylum seeker continues to refuse fingerprinting, they are sent before a judge in accordance with the Aliens Law (*Ley de Extranjería*). The judge usually orders the fingerprinting to be carried out, and the police takes the fingerprints in front of the judge where the detainees no longer resist. Nevertheless, some asylum applicants interviewed in Spain reported having been treated disrespectfully and roughly, but not subjected to the use of force.

2.5.3. Deprivation of liberty

Asylum seekers or migrants in an irregular situation who refuse to provide fingerprints or who are suspected of having deliberately destroyed them to avoid fingerprinting may in practice be detained. Destroyed fingertips will heal or improve sufficiently after a period of recovery, allowing them to be collected and checked against other databases.

An individual's refusal to provide fingerprints can be seen as unwillingness to cooperate in the establishment of their identity or in following the order of a police officer. This can be a legal ground for detaining asylum seekers or migrants in all the Member States that participated in the field research.[145]

As it currently stands, EU law does not envisage the possibility of depriving an individual's liberty to capture their fingerprints. The Eurodac proposal will, if adopted, change this. According to proposed Article 2 (3), Member States may introduce administrative sanctions, in accordance with their national law, for non-compliance with the fingerprinting process and capturing a facial image. The sanctions must be effective, proportionate and dissuasive. In this context, detention should only be used as a means of last resort to determine or verify a third-country national's identity.

Detention is a major interference with the right to liberty set forth in Article 6 of the Charter and in Article 5 of the ECHR. Strict safeguards exist to prevent unlawful or arbitrary deprivation of liberty. Under EU law, any limitation on the right to liberty must be in line with the requirements of Article 52 (1) of the Charter. This means that limitations must be provided for by law, must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, respect the essence of the right, and be proportionate.

To be lawful, it must be possible to subsume any deprivation of liberty under one of the grounds listed in Article 5 of the ECHR, as interpreted by the ECtHR. Pursuant to Article 6 (3) of the TEU and Article 52 (3) of the Charter, the ECHR has to guide the interpretation of the right to liberty and security set forth in Article 6 of the Charter.

The ECtHR has usually analysed the deprivation of liberty of asylum seekers or migrants in an irregular situation in the frame of Article 5 (1) (f) of the ECHR, which permits detention to prevent unauthorised entry or for the purpose of deporting or extraditing a person. Specific safeguards against arbitrary detention are included in the EU return and asylum acquis.[146] Taken together, under EU law and the ECHR, deprivation of liberty for immigration-related reasons can only be a measure of last resort, and an assessment needs to be made in each individual case to determine whether all pre-conditions required to prevent arbitrary detention are fulfilled.

If the person is deprived of liberty under Article 5 (1) (b) of the ECHR – to secure the fulfilment of any obligation prescribed by law – detention is only lawful if a person had a chance to comply voluntarily and clearly refused to do so. Offering an opportunity to comply voluntarily requires that individuals are put in a position – through effective information and counselling in a language they understand – to understand the rationale for collecting fingerprints, the manner in which fingerprints will be processed and the consequences for not giving fingerprints, so that they can make an informed decision. For the ECtHR, there must also be a balance between the right to liberty and the fulfilment of the obligation.[147] Factors to consider when drawing such a balance include the nature of the obligation arising from the relevant legislation, including its underlying object and purpose; the person being detained and the

145 See, for example, Germany, Law on Residency, Art. 49 and 62; StPo, Art. 81 b and 163 b and Poland in the Act on Border Guards of 1990, Art. 11.

146 Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ 2008 L 348/98 (*Return Directive*), Art. 15-17; Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast), OJ 2013 L 180/96 (*Reception Conditions Directive*), Art. 8–9 and 11.

147 ECtHR, *Göthlin v. Sweden*, No. 8307/11, 16 October 2014, para. 58.

particular circumstances leading to detention; and the length of the detention.[148]

To determine or verify an asylum applicant's identity or nationality, Article 8 (3) (a) of the Reception Conditions Directive (2013/33/EU) envisages the possibility of deprivation of liberty – provided all conditions set forth in EU law and in the ECHR are fulfilled. It can, however, be questioned if the taking of fingerprints serves this purpose. Surely, it would do so, when the asylum applicant has moved on after completing registration in one EU Member State, since a link can be established between an asylum applicant present in one EU Member State and a past Eurodac entry in another. Based on such links, biographic data can be obtained from the EU Member State of first registration. Whether fingerprinting at first entry helps determine the identity or nationality of a person – and thus can justify deprivation of liberty under Article 8 (3) (a) of the Reception Conditions Directive – is more difficult to conclude, except for those few cases where the individual returned to the EU a second time.

Aside from the specific situation of individuals held in Italian hotspots,[149] most testimonies of individuals deprived of their liberty for fingerprinting purposes relate to migrants in an irregular situation. In Belgium, an apprehended migrant in an irregular situation, who was 15 years old at the time, explained:

"They told me that if I refused I would be kept in custody for 24 hours and then in the morning at 7 am, I would go before a judge at the youth court." (Accompanied child, Moroccan male, Belgium)

An expert interviewed in Belgium believed that the authorities would simply detain the person if they thought that they had purposefully damaged the fingertip to give the fingers time to heal. A provider of legal assistance in Belgium had met people in the closed centres who had severely damaged fingerprints:

"That is in itself a reason within the Belgian law to confine people, if you are not willing to provide identification and supply fingerprints, you can be locked up in a closed centre for sure." (Provider of legal assistance, female, Belgium)

Similarly, in Germany, a person can be held in temporary police detention (*Gewahrsam*) for the maximum duration, which is the "end of the following day".

148 ECtHR, *Petukhova v. Russia*, No. 28796/07, 2 May 2013, paras. 58-59; and *Vasileva v. Denmark*, No. 52792/99, 25 September 2003, para. 38.

149 See ECtHR, *Khlaifia and Others v. Italy*, No. 16483/12, 15 December 2016, for an analysis of the status of individuals kept in the first reception facility in Lampedusa.

Conclusions

Individuals may be physically unable – for example, due to disability – or unwilling to provide fingerprints for storage in a large-scale IT system. In these cases, challenges may emerge when collecting biometric data in a manner that remains respectful of human dignity.

The physical impossibility to provide fingerprints must not result in discrimination or unequal treatment. Therefore, the design of the physical environment need to be suitable for persons with disabilities. EU Member States should design fingerprinting booths and gates so that they are suitable for persons with disabilities.

There are different reasons why people are reluctant to give their fingerprints. Although many do this to avoid being transferred under the Dublin procedure to a Member State in which they do not want to be, it is also possible that asylum applicants have had bad experiences with giving fingerprints to the police in their country of origin. They may also fear that authorities may share their fingerprints with their country of origin, which could endanger family members. In case of asylum applicants, their willingness to provide fingerprinting may increase if they felt they were being treated fairly and if family reunification procedures under the Dublin procedure worked smoothly.

In some cases, persons unwilling to provide fingerprints resort to self-harm, for example, by injuring their fingertips. Incidents of injured fingertips decreased as the technology developed. As biometric data other than fingerprints are increasingly used, the question emerges of whether in future, people could inflict more serious harm on themselves to avoid, for example, having their facial image captured.

In many cases, it is difficult to prove if an individual intentionally damaged their fingertips, or if it was impossible for them to provide fingerprints because of a history of hard labour, for example. A person belonging to a nationality suspected of injuring their fingertips, but who may be physically unable to provide fingerprints, may be suspected of self-injury. They may be at heightened risk of discrimination compared to a nationality not connected to self-injury.

In case of fingerprinting for Eurodac, the use of coercive measures – meaning use of force or deprivation of liberty – to obtain fingerprints, though not common, does occur, particularly in Member States that the migrants and asylum seekers transit. The process of taking fingerprints is usually outside external scrutiny, as providers of legal assistance are not present when fingerprints are taken.

Public officers may not be aware of the legal limits of necessity and proportionality concerning the use of force. Given the vulnerability of the people concerned and the obligation to use the least invasive means, it is difficult to imagine a situation in which physical or psychological force solely to obtain fingerprints for Eurodac would be justified. Officers must avoid the risk of traumatising or re-victimising asylum seeks and migrants.

FRA research showed that transparency about the purpose of the fingerprinting procedure may strengthen the willingness of the persons concerned to cooperate with the authorities, thus preventing situations from escalating. If fingerprinting takes place in stressful situations when large numbers of asylum seekers arrive, this may pose particularly high demands on staff. However, according to FRA findings, training tends to focus on the technical aspects of fingerprinting, and less on the treatment of the person who is fingerprinted.

Human dignity is inviolable. FRA opinions 4–6 suggests steps that the relevant actors can take to avoid the risk of authorities taking fingerprints in an unlawful manner. FRA opinion 7 gives guidance for fingerprinting children.

3 Access to and use of personal data stored

Charter of Fundamental Rights of the European Union

Article 8 – Protection of personal data

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Many actors can access, directly or indirectly, the information stored in IT systems. Data may be shared with private persons or third countries. Therefore, the risks for unlawful sharing and further use are very real. Illegal access and hacking are additional threats to the protection of personal data. This chapter describes the risks of unauthorised access and further use of information in violation of data protection law, as well as measures to prevent such risks.

EU IT systems increasingly serve purposes that were not originally envisaged. This chapter analyses the impact of such 'function creep' on the principle of purpose limitation. Most IT systems are being redesigned to fulfil two horizontal purposes to:

- help Member States fight terrorism and serious crime;
- enforce immigration law.

The chapter analyses the trend among law enforcement authorities to dismantle some of the safeguards accompanying access and the effects of this on fundamental rights, including the rights of the child. It also discusses possibilities to strengthen the identification of missing persons and victims of crime through increased access to IT systems. Furthermore, it discusses how increased access to data about migrants in an irregular situation, combined with the EU-wide applicability of entry bans and of return decisions, could drive migrants further underground and disproportionately impact on their fundamental rights.

Purpose limitation and data minimisation

The **principle of purpose limitation** requires personal data to be processed only for specified purposes that must be explicitly defined.[150] This principle is mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the GDPR and Article 4 (1) (b) of the Police Directive. According to these, personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.[151] The person concerned should be able to foresee the purpose for which their data will be processed.[152] In its ruling invalidating the Data Retention Directive, the CJEU pointed to the fact that the directive did not expressly provide that access and that the subsequent use of the data must be strictly limited to the purpose of combating precisely defined criminal offences, but instead relied on EU Member

150 See also Article 29 Data Protection Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013.

151 See also Directive 95/46/EC (*Data Protection Directive*), Art. 6 (1) (b), and Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8/1, Art. 4 (1) (b).

152 CJEU, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, opinion of Advocate General Kokott delivered on 18 July 2007, para. 53.

States to define the procedures. According to the CJEU, the legislator failed to lay down objective criteria for limiting the number of persons authorised to access and use the data to what is strictly necessary to the objective pursued.[153] In *Tele2*, the CJEU underlined that national legislation must be based on objective criteria defining the circumstances and conditions under which the competent national authorities are to be granted access to the data.[154]

Each IT system has been set up for a specific main purpose, for example, to help implement the Dublin procedure or the visa application process. IT systems may also have additional purposes. Apprehending and returning migrants in an irregular situation and fighting serious crimes and terrorism – two important EU priorities – are add-on purposes for IT systems that were initially designed for other reasons, such as Eurodac[155] and VIS,[156] as Table 8 shows. For others, such as SIS II, these additional purposes are two of the primary purposes.

Table 8: Primary and additional purposes in the legal instruments on existing and planned IT systems

IT system	Primary purpose	Additional purposes	
		Apprehension and return	Fighting serious crimes and terrorism
Eurodac Regulation and *proposal*	Application of the Dublin Regulation	yes	yes
VIS	Support the visa application process and border checks	yes	yes
SIS II: Decision and *police proposal*	Safeguard security in the territories of the Member States	no	n/a
SIS II: Regulation and *border proposal*	Processing alerts on entry and stay	n/a	no
SIS II: return proposal	*Processing of alerts on return decisions*	*n/a*	*no*
EES	Registration of entry and exit of third-country nationals	yes	yes
ETIAS	*Pre-border checks*	*no*	*yes*
ECRIS-TCN	*Information exchange on previous convictions of third-country nationals in other EU MSs*	*no*	*n/a*
Interop. proposals	*Ensure the correct identification of the person*	*n/a*	*n/a*

Notes: *Proposed systems and proposed changes in italics.*
n/a = not applicable
Source: *FRA, based on existing and proposed legal instruments (2017)*

The legal instruments clearly define the type of authorities who can search the IT systems. Member States are obliged to notify the European Commission the name of the authorities entitled to access the IT system. The European Commission makes this information publicly available.[157] Table 9 gives an overview of the type of authority allowed to search the IT systems.

153 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, paras. 61-62.
154 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 119.
155 See Eurodac Regulation.
156 See Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2008 L 218/129.
157 For instance, see: eu-LISA (2017b); eu-LISA (2017c).

Table 9: Purpose of access to carry out searches in IT systems per type of authority

Purpose of search	Visa issuance	Border checks	Fighting serious crime and terrorism	Combating irregular migration	Return procedure	Dublin procedure
Eurodac	n/a	n/a	Police and Europol	Police	Immigration authorities	Asylum authorities
VIS	Visa and border authorities	Border authorities	Police and Europol	Police	Immigration authorities	Asylum authorities
SIS II Regulation and Decision *Police, borders and return proposals*	Visa and border authorities	Border authorities	Police and Europol	Police	Immigration authorities	n/a
EES	Visa and border authorities	Border authorities	Police and Europol	Police	Immigration authorities	n/a
ETIAS	*n/a*	*Border authorities*	*Police and Europol*	*n/a*	*n/a*	*n/a*
ECRIS-TCN	*n/a*	*n/a*	*Police, Europol, Eurojust (and European Public Prosecutor's Office)*	*n/a*	*n/a*	*n/a*
Interop. proposals	*Visa and border authorities*	*Border authorities*	*Police and Europol*	*Police*	*Immigration authorities*	*Asylum authorities*

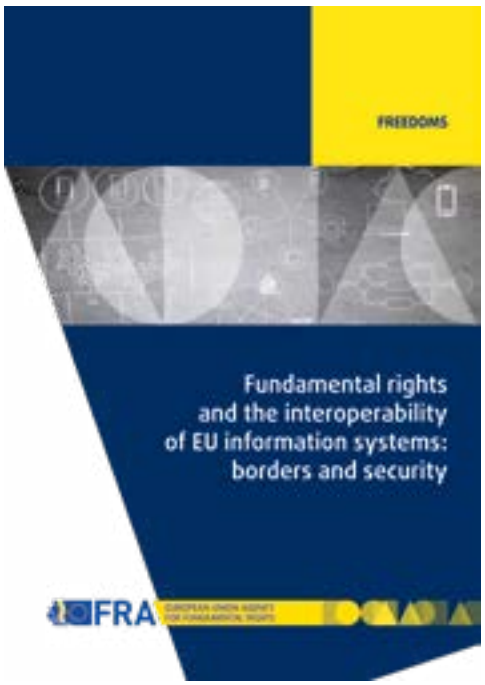
Note: *Proposed systems and proposed changes in italics.*
n/a = not applicable.

Source: FRA, based on existing and proposed legal instruments (2017)

FRA research shows that instances of unauthorised access occur. For example, two court cases in Bulgaria[158] and the Netherlands[159] involved unauthorised access to SIS II and subsequent sharing of the information with third parties, which was in both cases punished with disciplinary measures. Officers interviewed in the field research mentioned unauthorised instances of access to SIS II and to some extent to VIS, often with the aim of unlawful sharing with third parties.

Such 'function creep' may also happen if fingerprints – taken for whatever purpose – are included in searches done for criminal investigation purposes. This was the case in Ireland, when an audit by the Data Protection Commissioner revealed that fingerprints taken in the context of asylum or visa applications were included in all fingerprint searches carried out during police investigations, irrespective of whether there was any reason to believe that the immigrant or asylum seeker was involved in a crime.[160]

In July 2017, FRA published its report on interoperability and highlighted the importance of reflecting the purpose limitation of the legal instruments in the technical solutions for the various IT systems. The current compartmentalised nature of the EU databases acts as a safeguard against their use for unauthorised purposes. When moving towards interoperable IT systems, solutions need to retain safeguards against unauthorised access specific to each system and its purpose.



158 Bulgaria, Regional Directorate of Internal Affairs district 4, Ordinance No. 3 from 22 August 2013, issued by the head of Sofia (*Заповед, рег. № 3 – 318 от 22.08.2013 г., издадена от началника на 04 РУП при Столична дирекция на вътрешните работи*); the appeal was rejected by the Administrative Court – Sofia (*Административен съд – София*), Decision No. 7660 of 5.12.2013 on administrative case No. 9526/2013 (*Решение № 7660 от 5.12.2013 по адм. д. № 9526/2013*).

159 Netherlands, District Court Alkmaar (*Rechtbank Alkmaar*), Case No. AWB 10/2526, ECLI:NL:RBALK:2011:BU9499, 15 December 2011.

160 Ireland, Data Protection Commissioner (2014).

Closely linked to the principle of purpose limitation is the **principle of data minimisation**. Article 5 (1) (c) of the GDPR and Article 4 (1) (c) of the Police Directive, as well as Article 5 (c) of Convention 108 and Article 5(4) (c) of the draft Modernised Convention 108, spell out the principle of data minimisation whereby personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Convention 108 is in the process of being modernised to better reflect the new technological advancements and to ensure better compatibility with other updated international and European instruments, such as the EU GDPR and Police Directive.

The reference to 'necessity' under the GDPR goes beyond the wording of Directive 95/46/EC, which under Article 6 (1) (c), requires that data are 'not excessive' in relation to the purposes. This reflects the phrasing used in Article 5 (c) of Convention 108.[161]

The current trend in EU IT systems is to process more biometric as well as alphanumeric data, illustrated by the proposed legal changes to Eurodac and SIS II. Eurodac will contain biographic data and the type and number of the travel document, as well as facial images and fingerprints,[162] whereas all SIS II alerts may include fingerprints and, in some cases, palm prints (dactylographic data).[163] In addition to biographic data, the alerts for return decisions will include a reference to the decision giving rise to the alerts, the action to be taken, the type and number of the identification document and a colour copy of it.

The principle of data minimisation is also relevant as the same data that is included in EU databases is often stored in national IT systems leading to multiple storage of personal data on the same person. In addition, personal data may also be physically stored, for example, by keeping hard copies of dactyloscopic cards. In one instance, FRA observed that biometric data were collected twice from the same person. After having filed an asylum application at the Fiumicino airport in Rome, the applicant was checked against Eurodac and also had their index fingerprints taken in hard copy, which were then stored. The legal instruments on the EU IT systems do not foresee the practice of archiving hard copies of fingerprints in parallel to having them included in the EU databases.

Following the principle of data minimisation, in VIS, previously collected fingerprints should be reused if the applicant applies for a Schengen visa within 59 months.[164] FRA field research showed that fingerprints are often retaken by service providers who do not have the possibility to search VIS for previous applications.

Fingerprints are usually collected when apprehended as a migrant in an irregular situation, and then a second time if the person is fingerprinted for Eurodac. While this may be interpreted as going against the principle of data minimisation, this procedure ensures complying with possible stricter quality standards when fingerprinting for Eurodac. It also acts as a safeguard to reduce the risk of mistakes, which could occur if attaching fingerprints taken in the past.

3.1. Safeguards to ensure legal access

Protection from unauthorised access to personal data is enshrined in both the Council of Europe Convention 108 and EU law. Article 7 of Convention 108 requires the use of appropriate security measures to protect personal data against unauthorised access, alteration or dissemination. It also acknowledges that it is the data controller's duty to have a record system that tracks who has accessed the data and when.[165] Similarly, Article 5 (1) (f) of the GDPR lays down the principle of 'integrity and confidentiality', according to which personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". Articles 28 and 32 of the Regulation ensure that the processor and controller take the necessary measures to avoid data being disclosed to or accessed by unauthorised persons or organs.

In the *Digital Rights Ireland* case, the CJEU has clarified that EU legislation providing for the collection and retention of personal data must impose sufficient guarantees to protect personal data effectively against the risk of abuse and against any unlawful access and use of that data.[166] The quantity and sensitive nature of the data must be taken into account. The need for such safeguards is all the greater where personal data are processed automatically and where there is a significant

161 See: Convention 108, Art. 5 (c): "Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored".
162 Eurodac proposal, Art. 12.
163 SIS II police proposal, Art. 20; SIS II return proposal, Art. 4; SIS II borders proposal, Art. 20 (2).
164 Visa Code, Art. 13 (3).
165 See for example ECtHR, *I. v.. Finland*, No. 20511/03, 17 July 2008.
166 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 54 with further references.

risk of unlawful access to those data.[167] On this matter, the CJEU highlighted the need to have in place rules that would "serve to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality".[168]

Depending on the IT system, as illustrated in Table 10, a significant number of authorities may have the right to query IT systems. The larger the number of actors with access, the higher the risk of unlawful use. Member States are taking a number of measures to mitigate risks.

Spatial and electronic access control

To ensure lawful access, authorities provide spatial and electronic access controls as well as safeguards against unauthorised manipulation changes, transfers or loss of data, including by encryption and back-up routines. Member States have a number of data security safeguards in place to ensure that only persons authorised to access the data can do so. Typically, users are granted access rights based upon the pre-defined level of access – what they are legally authorised to access to perform their tasks. The hierarchy typically approves and documents the type of access granted to an officer. In some instances, the approval could be dependent upon completed training and/or a reliability assessment, such as access to VIS by local staff. Such measures are not always in place.[169] For example, in Lithuania, any staff member of a relevant institution could obtain access to Eurodac upon the consent of the head of their unit.[170]

Encryption could protect against illegal access. A number of advanced encryption methods and tools have been implemented for the protection of biometric data – principally fingerprint minutiae templates – in a manner that permits comparisons to be made in encrypted space. However, because of the computational demands of such encryption and the reduced performance of systems implementing such methods, they currently tend not to be used in large-scale IT systems.[171]

Personal data that are unlawfully accessed or shared may have serious implications for other fundamental rights beyond data protection rights. Interoperable databases are likely to become more attractive for those trying to access personal data by illegal means, such as organised crime groups or even hackers linked to foreign states. Large amounts of personal data are highly attractive for a range of criminal activities as well as state sponsored hacking by hostile regimes. The risks resulting from information leaks are particularly high for persons in need of international protection.

In addition to these electronic access control measures, there are also spatial access controls, such as locking of rooms, implementing standardised work practices and procedures and providing guidance to the employees.

Access control becomes more challenging when **private actors** can access the IT system. Two planned IT systems – the proposed ETIAS (Articles 14 and 39) and the adopted EES Regulation (Article 13) – will allow access by private persons. This includes, for example, carriers, such as airlines. These will have access to a specific and limited subset of data through a web-portal, namely for requesting and checking the status of a travel authorisation in the context of ETIAS and for checking the status of a visa in the context of EES.

Where these entities are only supposed to have access to a particular segment of the data, this segment needs to be precisely defined and isolated from the rest of the database in a manner that ensures that other data or data of other persons cannot be accessed. As the EDPS points out, any access to the system should be limited only to authorised staff working for the private entity (for example, the carrier). Moreover, such access should only be possible through a proper authentication scheme which logs the access, and safeguards should extend to data processing after the third party has extracted the data.[172] ETIAS and EES envisage access through an internet interface, which requires particular safeguards.

Regarding cooperation with external service providers, Member States were asked how they ensure that subcontractors respect data subjects' rights. In their responses, Member States referred to Article 43 and Annex X of the Visa Code, which sets out a list of the minimum requirements to be included in contracts. Twelve Member States reported that contracts signed with external service providers include specific provisions on data protection binding subcontractors to ensure respect of data subjects' rights. These include, for example, clauses allowing the national Data Protection Authority to conduct on the spot inspections without prior notice, obligations for the Member States to make available specific information for the visa applicants and a clause obliging the service provider to appoint a Data Protection Officer entrusted with overseeing respect of data subjects' rights.[173]

167 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, paras. 54-55.
168 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 66.
169 Franet, Germany.
170 Franet, Lithuania.
171 eu-LISA (2015a), p. 6.
172 European Data Protection Supervisor (EDPS) (2016), *Opinion 6/2016*, 21 September 2016, paras. 48-53.
173 Franet.

Log files

A user management application stores information about searches and can create log files. These audit trails are used for monitoring lawfulness of access to EU and national databases. Log files are kept at eu-LISA at the central level, and at the national level. Practice varies among the Member States. Austria and Germany, for instance, keep no Eurodac log files separate from those stored by eu-LISA. However, in Germany, log files for the databases A and P (which include the same fingerprints as Eurodac) are kept for 12 months. In Luxembourg, the officer needs to indicate the reason for consulting SIS II when logging in; this information is then stored and the purpose of the search can be monitored.

Practice also varies as to what is included in log files. Hungary, for instance, has a register of all Eurodac data transfer transactions and of the authorities accessing data, including the collection and insertion of fingerprints. The register contains the following information: personal identification data of the person whose fingerprints are collected, inserted and searched for comparison; reference number attached to the transfer; date of the data transfer; and a list of the data transferred. In each case, the result of the search is stored. The list is shared with the Hungarian national data protection authority, which monitors access to verify whether the purpose of the search was genuine. Under GDPR, the national data protection authority (DPA) should have access to the records for oversight purposes,[174] whereas the regular monitoring of compliance with the data protection rules is one of the tasks of the data protection officer[175] (DPO). A DPO must be designated where a public authority or body carries out the processing.[176]

Human factor: improving awareness on risks for unlawful sharing of data

In all the EU Member States covered by the field research, administrative and human factors emerged as crucial when it comes to establishing an efficient system for ensuring access to data in line with purpose limitation. For example, a Spanish provider of legal assistance underlined the need to work on improving the awareness of data protection among public officials.

Awareness of the need to verify rigorously access rights may also be limited, leading to the risk of unauthorised access. Unlawful sharing of data can happen. An expert providing legal advice to asylum applicants in Germany noted, for example:

"I only have to know the name and the date of birth of a given person, maybe the case number, and I can get data which has been recorded in such systems from the police or other authorities, without power of attorney. I do it all the time. I do have power of attorney for that, but nobody asks for it." (Provider of legal assistance, female, Germany)

Reducing instances of indirect access for searches

An authorised authority can have direct access to data through the data system, or indirect access by requesting another authority or branch to carry out the search.

Indirect access remains exceptional. According to FRA research carried out in 2015, indirect requests for accessing Eurodac, SIS II and VIS, are the exception in the EU, but are still allowed in some EU Member States. In exceptional cases, unauthorised bodies may request for SIS II data to be shared. In these cases, in Sweden, a secrecy examination is carried out according to the Public Access to information and Secrecy Act.[177]

In case of indirect access, the officer who is requested to access the data on behalf of another officer has to examine whether or not to implement the request. They have to verify whether the officer requesting the information is entitled to receive it and, if so, which information they can have.

3.2. Access to EU IT systems for fighting serious crime and terrorism

Access to personal data by law enforcement represents a limitation on the right to respect for private and family life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter). As such, it must comply with the principle of necessity and proportionality. Under Article 52 (1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. With due regard to the principle of proportionality, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union, or the need to protect the rights and freedoms of others.[178]

174 General Data Protection Regulation, Art. 58 (1) (e).
175 General Data Protection Regulation, Art. 39 (1) (b).
176 General Data Protection Regulation, Art. 37 (1) (a).

177 Sweden, Ministry of Justice (*Justitiedepartementet*) Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslag (2009:400)*).
178 See also e.g. CJEU, C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 December 2015, paras. 69 and 80-82.

Table 10: Access to IT systems to fight serious crime and terrorism

Primary purpose				Additional purpose				
SIS II Decision and *police proposal*	**SIS II Regulation and** *borders proposal*	*SIS II return proposal*	*Interop. Proposals (CIR and MID)*	**Eurodac Regulation** *and proposal*	**VIS**	**EES Regulation**	*ETIAS proposal*	*ECRIS –TCN proposal*
yes	yes	*yes*	*yes*	yes	yes	yes	*yes*	*no**

Notes: *Proposed systems and proposed changes in italics.*

* *Rather than holding detailed information on criminal records, ECRIS-TCN will provide information on which Member State(s) hold(s) criminal record information on a specific third-county national. This will allow the competent authorities of the consulting Member State to obtain information on previous convictions through ECRIS itself, i.e. the actual decentralised system for the electronic exchange of information from national criminal registers. The proposal foresees that a single central authority in each Member State can access ECRIS-TCN, but access by Europol and Eurojust is also foreseen.*

Source: FRA, based on existing and proposed legal instruments (2017)

All existing and planned EU IT systems, except ECRIS-TCN, allow for access to national law enforcement authorities and Europol for fighting serious crime and terrorism, as illustrated in Table 10. This is covered by the main purpose of the SIS II Regulation and Decision as well as the SIS II proposals on police and borders,[179] and as an additional purpose in Eurodac,[180] VIS,[181] EES[182] and ETIAS.[183]

Law enforcement authorities' access to Eurodac is recent and the number of queries is therefore limited. In 2016, a total of 326 searches for law enforcement purposes were carried out in Eurodac, in accordance with Article 20 (1) of the Eurodac Regulation. Most of these occurred in Austria and Germany, according to eu-LISA.[184] By the end of September 2015, 11 Member States reported that their law enforcement agencies had performed a total of 9,474 searches in VIS.[185]

3.2.1. Legal safeguards to ensure necessity and proportionality

Authorities interviewed by FRA supported access to IT databases and biometrics data for law enforcement purposes.

"The more information, the better. Moreover, if we are referring to victims and vulnerable groups, whatever improves it [the situation] – if you can use a database… then why not?" (Police, male, Spain)

Possible benefits that this can bring, however, need to be balanced against the potential negative consequences that such access may have for the individual. A person may find themselves among the list of suspects for a crime, for example, as a result of similarities in name with another person, data entry mistakes or other reasons. They would have to prove their innocence.

Even if specific individuals whose data are included in the EU IT systems may be connected to organised crime or even terrorism, these persons represent a small segment in the overall amount of data available. There is no prior evidence when including an individual in the database that the risk is higher than in the general population of the Member States. Having the possibility to undertake checks against certain groups of people – for example asylum applicants or visa applicants – but not against others whose personal data are not stored in a database is likely to result in an artificial increase of crime detection rate, hence stigmatising these groups as potentially more criminal than others. For this reason, Article 40 (4) of the Eurodac Regulation envisages that the overall evaluation of Eurodac also examines whether law enforcement access to Eurodac has led to indirect discrimination against persons covered by the regulation.

The lack of even an indirect or remote connection between communication data retained and the purpose of their retention – serious crime – was among the arguments that the CJEU used in the *Digital Rights Ireland* case to conclude that the Data Retention Directive was not in line with the Charter.[186] Furthermore, the ruling required that a differentiated retention (storage) period is established on the basis of the possible usefulness of the data for the purposes of the law enforcement objective.

179 SIS II Regulation, Art. 1; SIS II Decision, Art. 1; SIS II police proposal, Art. 1; SIS II borders proposal, Art. 1.
180 Eurodac Regulation, Art. 1(2); Eurodac proposal, Art. 1 (c).
181 Council Decision 2008/633/JHA, Art. 1.
182 EES Regulation, Art. 6 (2).
183 ETIAS proposal, Art. 1 (2).
184 eu-LISA (2017a), table 9.1., p. 14.
185 eu-LISA (2016), p. 24 for information on the Czech Republic, Estonia, Finland, Germany, Greece, Hungary, the Netherlands, Poland, Slovenia, Spain and Switzerland.
186 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, paras. 57-60.

Usefulness of a measure is not in itself sufficient to justify law enforcement access. According to the CJEU, even where a measure pursues an objective of general interest, including a fundamental one such as the fight against organised crime and terrorism, it does not mean that the measure would be considered necessary for the purpose.[187]

The fundamental rights experts who were consulted showed serious concerns about the lack of proper controls. Some representatives of asylum authorities expressed concerns related to the particular sensitivity of the asylum applicants' data, the human factor and the possibility of committing mistakes. An officer working with victims of trafficking in human beings firmly rejected expanding access, considering that the information contained in these databases is very sensitive and therefore should have very limited access.

The national data protection authority in Italy, raised concerns regarding the control of purpose limitation in the context of access by law enforcement.

"Our problem, as DPA, is that these databases (Eurodac and VIS), even though they have been created to manage the asylum and the visa policies, have become additional police databases, this is the real problem. Consequently, it is crucial to limit the access to the information only to the cases which are really necessary in order to avoid abuses."
(National Data Protection Authority, female, Italy)

The security challenges in recent years have led to an increase in police accessing national databases. Although this report does not analyse national systems, the following example from Belgium illustrates the broader context. According to a Belgian official, because of suspicion that there could be IS fighters among asylum seekers, copies of fingerprints of specific nationalities are handed over to the anti-terrorism police. Furthermore, since the Paris attacks in November 2015, the full list of the names of asylum applicants is handed over daily, which is then screened by police.

The specific safeguards in place to ensure that law enforcement authorities' access to IT systems is limited to situations when it is necessary and proportionate vary depending on the system, as described in the following paragraphs.

Reasonable suspicion

The legal instruments establishing the IT systems only permit law enforcement authorities to access these if the comparison is necessary to prevent, detect or investigate terrorist offences or other serious criminal offences, if it is necessary in a specific case and if there are reasonable grounds to consider that the comparison will substantially contribute to this purpose.[188] The Eurodac Regulation has a higher threshold. It requires 'a substantiated suspicion' that the fingerprints of a suspect, perpetrator or victim of a terrorist offence or other serious criminal offence can be found in Eurodac.[189]

Substantial contribution to fighting serious crime and terrorism

Eurodac,[190] EES[191] and VIS[192] require the presumption that their consultation will substantially contribute to the prevention, detection or investigation of terrorism or other serious crime. According to Article 45 (1) (c) of the proposed ETIAS Regulation, if there are reasonable grounds to suggest a substantial contribution 'may' rather than 'will' occur (as is the case for Eurodac, EES and VIS), this is considered a sufficient reason to search the system. This shift of the threshold implies a reduced responsibility of the law enforcement authorities to conduct their own proportionality assessment of the relevance of the data to the intended law enforcement objective.

Limiting searching possibilities

Searches to establish if there is a 'hit' are in the case of Eurodac limited to fingerprints and according to the proposal searches can in addition be carried out with facial image.[193] Alphanumeric data, in addition to biometric data can be used for searches in VIS and EES if the purpose is to establish the travel history. In the case of VIS, such data can include the purpose of travel, arrival and departure date, and residence,[194] and in the case of EES, date and place for entry and exit.[195] As ETIAS holds only alphanumeric data, searches can, according to the proposal, only be done with such type of data, which includes address, email address and IP address.[196] The wide search categories means that the searches are not individualised and instead, a group of people will be included in the 'hit'.

187 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 51.

188 ETIAS proposal, Art. 45 (1); EES Regulation, Art. 32 (1); Eurodac Regulation, Art. 20 (1); Eurodac proposal, Article 21 (1); VIS Regulation, Art. 3 (1).
189 Eurodac Regulation, Art. 20 (1).
190 Eurodac Regulation, Art. 20 (1) (c).
191 EES Regulation, Art. 32 (1) (c).
192 VIS Regulation, Art. 3 (1).
193 Eurodac Regulation, Art. 19 (1); Eurodac proposal Art. 20 (1).
194 Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2008 L 218/129, Art. 5 (2).
195 EES Regulation, Art. 32 (5).
196 ETIAS Proposal, Art. 45 (2).

Eurodac and VIS do not limit access to data, but provide full access to the data stored. Access to data beyond name and date of birth could be particularly harmful for the person, as the searches concern persons who have no connection to crime. ETIAS includes a safeguard for access to data on an individual's current occupation, criminal convictions or whether they have ever been subject to return to the country of origin by a Member State, as the request needs to justify why the consultation is necessary.

Cascading system

Eurodac, EES and ETIAS contain an additional safeguard to prevent access when it is not necessary or proportionate, known as a 'cascading system'. Under this approach, authorities must first consult other databases. If these databases do not yield any results, only then can police search the Eurodac, EES and ETIAS systems. Access to Eurodac for law enforcement purposes is only lawful if the data subject's identity could not be established from national fingerprint databases, databases of other Member States available via the Prüm system,[197] and VIS.[198] If Prüm has not been implemented, access for law enforcement can principally not be granted.[199] By the end of 2016, the Prüm mechanism for fingerprint exchange was operational in 21 of 27 EU Member States (Denmark does not allow law enforcement access to Eurodac). Croatia, Greece, Italy, Ireland, Portugal and the United Kingdom had not implemented the mechanism.[200]

The cascading requirements for access to ETIAS and the EES are less stringent. Access to ETIAS is allowed if the required information has not previously been obtained after consulting "all relevant national databases and the Europol data".[201] According to the EES Regulation, searches for identification are allowed, if a prior search in national databases or fingerprint databases of other Member States available via the Prüm system has not been fully carried out within two days of being launched. However, in certain cases, a prior search is not necessary or a VIS consultation might be possible in parallel, rather than prior to the EES search.[202]

The cascading system is based on a recognition of the principles of proportionality and purpose limitation. Its introduction, along with the possibility for law enforcement access to Eurodac, reflected the special sensitivity of the data contained in the system. The Eurodac Regulation states that "the proportionality principle requires that Eurodac be queried for such purposes only if there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record, [...] [and] that the threshold for authorities responsible for internal security to query Eurodac must therefore always be significantly higher than the threshold for querying criminal databases."[203]

As stated in the 2016 FRA opinion on the revision of Eurodac,[204] this approach reflects the fact that notwithstanding the gradual expansion of the system to cover other categories of persons, a large share of persons included in the Eurodac database are applicants for international protection. Given that their data are collected for a different purpose and without any connection to a criminal activity or another security risk, safeguards accompanying the access of law enforcement to this data should be particularly robust, even more so than in case of other groups of persons. The foreseen expansion of Eurodac to collect additional data, including fingerprints of very young children, needs to be seen as an argument for retaining, if not further reinforcing, the current set of safeguards.

Similarly, neither EES nor ETIAS collects data of persons directly or even indirectly connected to criminal activities or investigations. There is no link between the data and the law enforcement objective similar to that established by the CJEU regarding communication data in the *Digital Rights Ireland* case. The obligation to first consult databases more directly linked to criminal investigations, such as national fingerprint databases, is therefore a core element of the mechanism, which seeks to make law enforcement access to data collected in such a blanket (non-targeted) manner capable of meeting the proportionality requirement.

Although interoperable, the systems are expected to retain their specific purposes and legal frameworks, and the reasons for originally introducing different access mechanisms remain valid.[205]

197 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/1 was integrated in EU, and the implementing Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/12 transposed into EU legal framework the basic elements of a 2005 international agreement between several EU Member States. The Prüm mechanism allows the automated comparison of fingerprints, DNA (in both cases on a hit/no-hit basis) and vehicle registration information.
198 Eurodac Regulation, Art. 20 (1).
199 eu-LISA (2017a), p. 13.
200 *Ibid*.
201 ETIAS proposal, Art. 45 (1) (d).
202 EES Regulation, Art. 32 (2).
203 Eurodac Regulation, Recital 10.
204 FRA (2016a), pp. 41–42.
205 Interoperability proposals, Art. 22 (4).

3.2.2. Criminal records of children and impact on their future lives

Article 40 of the UN Convention on the Rights of the Child (CRC) requires special attention to be given to the treatment of children alleged as, accused of, or recognised as, having infringed the penal law to protect them from stigma. If they have offended, opportunities for rehabilitation must be maximised. According to the United Nations (UN) Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules'), which the CRC Preamble recalls, records of juvenile offenders should be kept strictly confidential and closed to third parties, and should not be used in adult proceedings in subsequent cases involving the same offender.[206] In its Recommendation on the Criminal Record and Rehabilitation of Convicted Persons, the Council of Europe's Committee of Ministers advised Member States 'to restrict to the utmost the communication of decisions relating to minors'.[207]

The majority of EU Member States erase records of previous convictions when a child reaches the age of maturity, but some EU Member States retain such data.[208] The age of criminal responsibility varies across Member States. In most EU Member States, it is set at 14 or 15 years, but is set at 12 years in Ireland, the Netherlands and most parts of the United Kingdom (though it is as low as 10 years in Northern Ireland).[209] The ECRIS-TCN proposal does not affect national rules on entering convictions against children into the national criminal record register.[210] In addition, child offenders can be included in SIS II.[211]

In its opinion on ECRIS-TCN, FRA highlighted several elements that may have a disproportionate effect on children. These include the impact on children of convictions related to migration or trafficking in human beings, and the sensitivity of children's criminal records.[212] Some children may have been compelled to commit offences as a consequence of being subject to trafficking in human beings, notably as a result of exploitation. Others may have criminal records relating to migration-related offences when they were moving together with their parents. Children should not suffer disproportionate consequences for decisions made by their parents. Legislation criminalising irregular entry or stay varies among Member States,[213] and the existence of a criminal record may depend on where they have been apprehended.

3.3. Access for immigration control purposes

The immigration status of a third-county national will be available in an increasing number of IT systems. Thus, it will be increasingly attractive for immigration law enforcement officers to consult such IT systems to enhance the efficiency of apprehending and returning migrants in an irregular situation.

Immigration control features as either the main purpose or the added purpose in almost all IT systems, except for the SIS II Decision and the SIS police proposal, as well as ECRIS-TCN.

Table 11: Access to IT systems to detect migrants in an irregular situation

Primary purpose				Additional purpose				
SIS II Decision and *police proposal*	**SIS II Regulation** and *borders proposal*	*SIS II return proposal*	*Interop. proposals*	**Eurodac Regulation** and *proposal*	**VIS**	**EES Regulation**	*ETIAS proposal*	*ECRIS-TCN proposal*
no	yes	*yes*	*yes*	yes	yes	*yes*	*yes*	*no*

Note: *Proposed systems and proposed changes in italics.*

Source: *FRA, based on existing and proposed legal instruments (2017)*

206 UN (1985), *Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules')*, General Assembly resolution 40/33 of 29 November 1985, Rule 21.
207 Council of Europe, Committee of Ministers (1984), Recommendation on the Criminal Record and Rehabilitation of Convicted Persons, No. R(84)10, 21 June 1984, Section I. (5).
208 FRA (2015c), p. 21.
209 European Commission (2014a), p. 6. See also FRA (2017c).
210 ECRIS-TCN proposal, Explanatory Memorandum accompanying the proposal, p. 10.
211 SIS II Decision, Art. 34 and SIS II police proposal, Art. 34.
212 FRA (2015c), pp. 21–22.
213 FRA (2014).

Following the adoption of the EU Action Plan on Return,[214] and in light of the Commission Recommendation on making returns more effective when implementing the Return Directive,[215] the European Union and its Member States are making increased efforts to improve the effectiveness of return policies. This also includes optimising the use of existing and planned IT systems for return purposes. This section describes some of these efforts and the impact they have on fundamental rights.

3.3.1. EU-wide applicability of entry bans

The Return Directive obliges Member States to issue a return decision to third-country nationals staying illegally on their territory.[216] Member States are not obliged to accompany all return decisions with entry bans, but they are under obligation to issue an entry ban if no period for voluntary departure has been granted, or the obligation to return has not been complied with, according to Article 11 of the Return Directive. Entry bans are given an EU-wide effect by prohibiting the entry of the individual concerned into the territory of all Member States bound by the directive.[217]

One of the purposes of SIS II is to allow authorities in one Member State to know if a person who is stopped or checked has an entry ban issued by another Member State. In 2016, SIS II had 830,002 alerts on persons and more than half – 484,036 alerts – concerned entry bans.[218]

According to the SIS II Regulation, Member States are not obliged to enter all entry bans accompanying a return decision into SIS II.[219] The European Commission has encouraged a 'systematic' registration of such entry bans in SIS II to ensure their EU-wide effect.[220] In future, the SIS II proposals on borders and return will require all entry bans and return decisions issued in accordance with the Return Directive to be entered into SIS II.[221]

SIS II only includes information of the existence of an alert, the reason it exists (for example, an entry ban), a reference to the decision behind it and the action to be taken.[222] No further details are recorded. Therefore, if a person is stopped in a Member State other than that which issued the alert, officers may, in case of doubts, need to consult that Member State to further clarify the course of action.

When the person is held, delays in the consultation procedure may lead to extended and arbitrary deprivation of liberty.

3.3.2. EU-wide enforcement of return decisions

Return decisions issued by one EU Member State can be directly enforced in another, according to EU law, which makes possible the mutual recognition of return decisions.[223] However, the Return Directive itself does not set out an obligation of mutual recognition of return decisions.[224] Therefore, Member States have the choice either to recognise the original return decision issued by another Member State (in accordance with Directive 2001/40/EC) or to issue a new one in application of Article 6 (1) of the Return Directive. The SIS II proposal on returns aims to strengthen the cooperation between EU Member States in this regard. In future, when a Member State apprehends a person holding a return decision by another EU Member State, the authorities of the apprehending state should communicate to the authorities of the state who issued the return decision whether the person has left voluntarily or if the return was enforced.[225]

In case of recognising a return decision, according to Directive 2001/40/EC, the Member State executing the return decision is responsible for ensuring that the removal does not violate fundamental rights and in particular the principle of non-*refoulement*.[226] Given the absolute nature of the prohibition of *refoulement*, authorities must refrain from implementing a return decision if there are legal bars to returning an individual, and also in cases where the person concerned has not explicitly referred to such bars (for example, by applying for asylum). The authorities of the removing Member State need to examine and document that there are

214 European Commission (2017a).
215 European Commission (2017), *Commission Recommendation of 7.3.2017 on making returns more effective when implementing the Directive 2008/115/EC of the European Parliament and of the Council*, C(2017) 1600 final, Brussels, 7 March 2017.
216 Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ 2008 L 348/98 (*Return Directive*), Art. 6 (1).
217 Return Directive, Recital 14. See also: Commission Recommendation (EU) 2017/2338 of 16 November 2017 establishing a common 'Return Handbook' to be used by Member States' competent authorities when carrying out return-related tasks, OJ 2017 L 339/83, Annex (Return Handbook), sub-section 11.1.
218 See: eu-LISA (2017d), p. 9.
219 See Art. 24 (3) of the SIS II Regulation, which is a 'may clause'.
220 Return Handbook, sub-section 11.2, p. 49.
221 SIS II return proposal, Art. 3 (1); SIS II borders proposal, Art. 24 (3).
222 SIS II Regulation, Art. 20 (2).
223 Council Directive 2001/40/EC of 28 May 2001 on the mutual recognition of decisions on the expulsion of third-country nationals, OJ 2001 L 149/34, Art. 1; and Council Decision 2004/191/EC of 23 February 2004 setting out the criteria and practical arrangements for the compensation of the financial imbalances resulting from the application of Directive 2001/40/EC on the mutual recognition of decisions on the expulsion of third-country nationals, OJ 2004 L 60/55.
224 Return Directive, Art. 6. See also Return Handbook, sub-section 5.2, pp. 22–23.
225 SIS II Return Proposal, Art. 6.
226 See also Return Handbook, sub-section 5.2, p. 23.

no fundamental rights bars against the removal. This raises difficult practical challenges, as the returning Member State, which recognised the original return decision, needs to trust that the Member State which issued the decision respected the principle of non-*refoulement*. The SIS II proposal on return envisages the storage of a number of data related to the return decision, including the information on its suspension and the postponement of its enforcement.[227] In this way, in future, the returning Member State can to some extent verify, at least indirectly, if the authorities issuing the return decision have examined possible bars to removal. Member States would need to systematically issue certificates of non-removability as required by Article 14 (2) of the Return Directive to enable the returnee to explain why they have not been able to comply with the voluntary period of departure. However, the situation in the country of origin may also have changed giving rise to new fundamental rights risks representing bars to removal.

3.3.3. Disproportionate impact on fundamental rights of certain immigration law enforcement measures

Almost all IT systems have the purpose of contributing to detecting and returning migrants in an irregular situation, either as a primary or added purpose. As immigration law enforcement would become more effective if IT systems were interoperable, migrants in an irregular situation would avoid situations where they would risk apprehension. As FRA demonstrated in its research on rights of migrants in an irregular situation, certain enforcement measures have a disproportionate impact on human dignity and the ability to enjoy basic rights protected by the Charter.[228] FRA research has shown that if migrants in an irregular situation know that they risk being apprehended or reported to the authorities, they will be discouraged from approaching providers of basic services – such as medical facilities or NGOs that offer legal advice – or from sending their children to school. This is because they are afraid that information about them will be further shared with other authorities and result in their apprehension.[229]

The fear of being apprehended may also reduce the willingness of migrants in an irregular situation to report a crime. As emerged from FRA research on severe labour exploitation, victims or witnesses of crimes are reluctant to approach the police in fear that this would lead to their removal. This puts them at risk of further victimisation and allows perpetrators to remain unpunished. This also deprives law enforcement authorities of the opportunity to combat crime effectively.[230] According to Recital 10 of the Victims' Rights Directive, the right of victims to be acknowledged as victims and to have access to justice should not be made conditional on their residence status.

FRA guidelines on apprehending migrants in an irregular situation suggest that social service providers should not share information with immigration authorities. The guidelines also suggest that possibilities could be considered for victims and witnesses to report crimes without fear of being apprehended.

3.4. Access for identification of missing persons and victims of crime

Field research showed that IT systems are important to help identify missing persons and victims of crime. SIS II allows for registering alerts for missing persons,[231] which could include victims of crime. In all six EU Member States covered in the field research, interviewees stated that SIS II has been relevant for identifying missing persons, including victims of crime. Several officers stated that they have been able to identify victims of crime, including victims of trafficking in human beings, through fingerprint checks against Eurodac and national databases. A Polish officer underlined that thanks to a SIS II alert, they were able to identify that a woman who was suspected of having committed document fraud was actually a victim of trafficking for sexual exploitation. Another officer from Germany mentioned that persons frequently registered in VIS as visa sponsors are checked against criminal registers to rule out that they are linked to organised crime, such as trafficking in human beings for sexual or labour exploitation. Several Member State officers as well as experts were more sceptical and pointed out that as of yet, there are not many cases demonstrating that databases would have contributed to identifying victims of crime. At the same time, police officers in Poland pointed out that, in general, the focus is on crime investigation, and not primarily on finding victims.

SIS II includes alerts on known victims, but in order to profile potential victims of trafficking in human beings there is a need for human judgment.

According to Recital (25) of the EU Anti-Trafficking Directive, training should be provided to officials that come across victims or potential victims of trafficking in

227 SIS II return proposal, Art. 4.
228 FRA (2011).
229 *Ibid.*

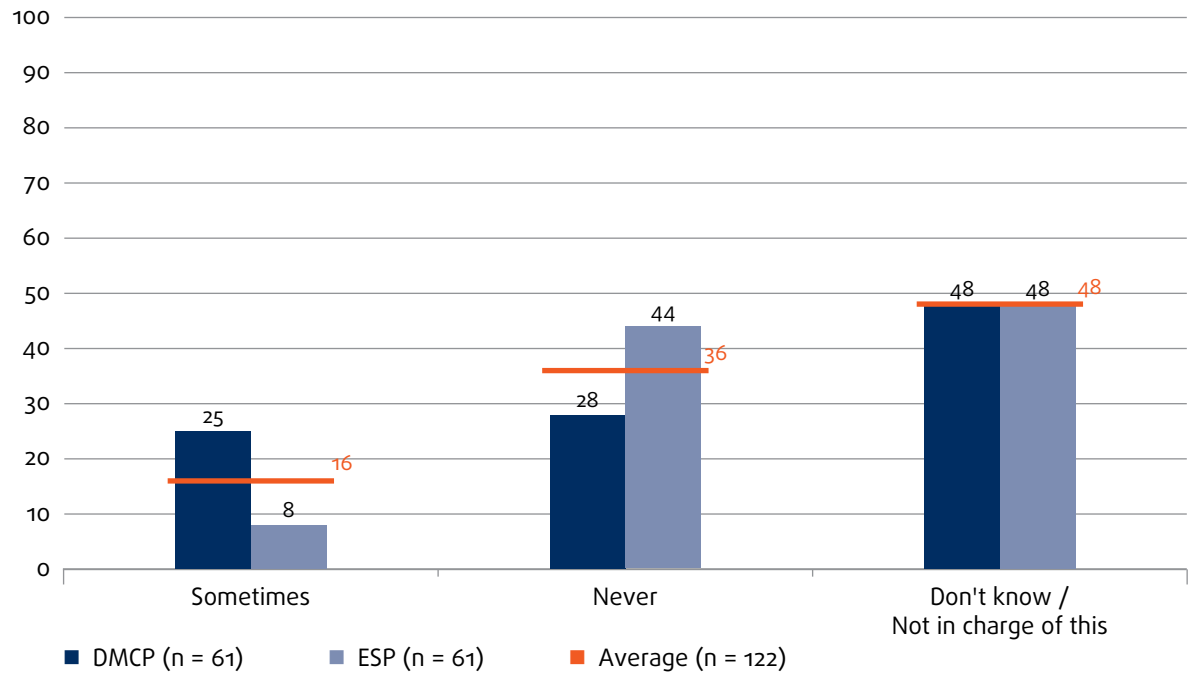
230 FRA (2015d), p. 19.
231 SIS II Decision, Art. 32 (2) (a) (i); SIS II police proposal, Art. 32 (2) (a) (i).

human beings, such as consular staff, on how to identify and handle such cases.[232] The European Commission[233] and the Council of the Baltic Sea States[234] have produced guidelines on identifying victims for consular services and border guards, and Member States have organised training seminars for consular staff.[235] Such measures could improve awareness on how to conduct visa interviews with suspected victims of trafficking in human beings, refer victims to providers of medical or psychological support and issue replacement travel documents, in case the trafficker confiscated the original one.[236]

In the small-scale survey carried out at DMCPs and their service providers, staff were asked if special measures were taken for suspected victims of trafficking in human beings. Figure 9 shows that one quarter (25 %) of the officers at DMCPs took such measures, but only 8 % of the staff at service providers. For other victims of crime shown in Figure 10, the percentage of staff who said that they take special measures is significantly lower: 13 % of DMCP officers and only 3 % of service providers' staff. This could reflect the absence of measures, but also the possibility that staff did not often come across suspected victims of human trafficking or victims of crime.

Generally, experts interviewed in the research underscored the potential of IT systems for improving victims' protection. However, there were also concerns raised about the protection of personal data and how to sufficiently control the use of data. Others noted the risk for stigmatisation.

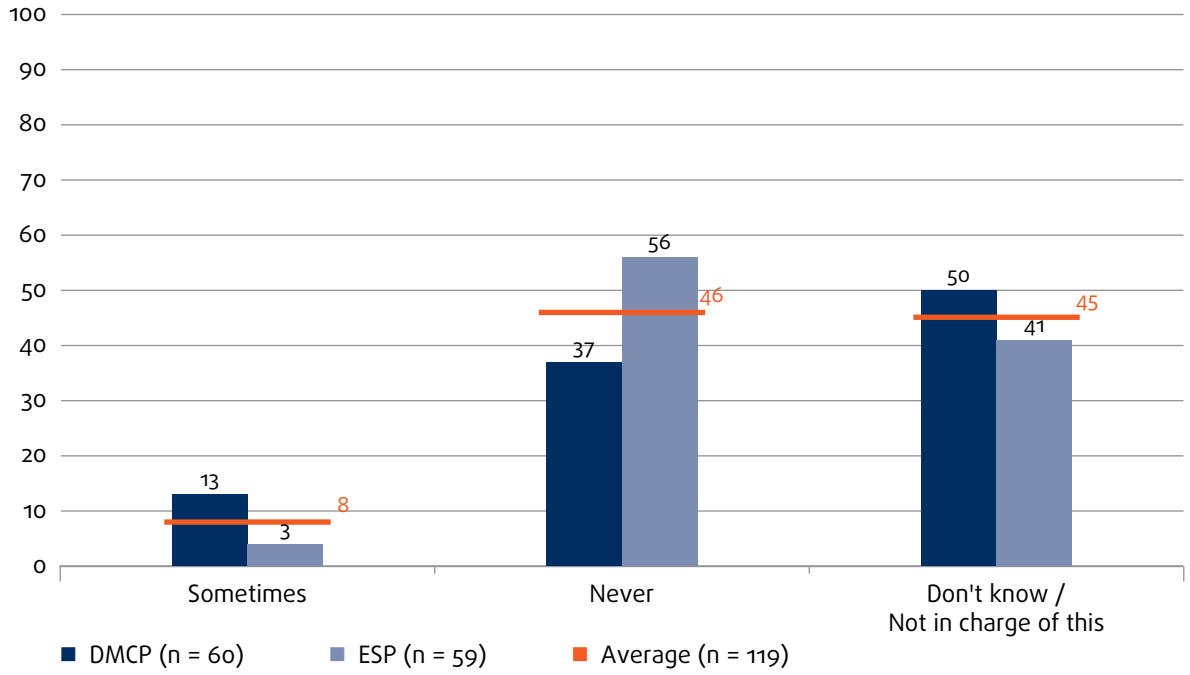
Figure 9: Special measures for suspected victims of trafficking in human beings during the visa application procedure (%)



Note: *The results are based on the survey question "And for the following groups, are specific measures taken and how often?"*
Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

232 Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA, OJ 2011 L 101/1 (*Anti-Trafficking Directive*).
233 European Commission (2013a).
234 Council of the Baltic Sea States (2011). The Council is composed of Denmark, Estonia, Latvia, Lithuania, Finland, Germany, Iceland, Norway, Poland, Sweden, Russia and an EU representative.
235 See, for instance, the programme for the Training Seminar on Human Trafficking for Diplomatic and Consular Personnel.
236 See Council of the Baltic Sea States (2011).

Figure 10: Taking of special measures for other victims of crimes during the visa application procedure (%)



Note: *The results are based on the survey question "And for the following groups, are specific measures taken and how often?"*
Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016.*

The SIS II police proposal will strengthen possibilities to identify victims of crime through alerts on missing persons that include biometrics. Dactylographic data (fingerprints and palms prints) or facial image shall be used primarily. If these are not suitable for identification then DNA can be used.[237] At external borders, border guards currently have access to fingerprint searches to verify the identity of the visa holder.[238] Field research revealed that border guards do not always systematically fingerprint all visa holders to check against the biometrics stored in VIS, as mentioned in Section 2.2. For example, during the non-participatory observation in Barajas airport, in Spain, researchers found that fingerprints are only taken when the system requires it. After checking the visa, the system may prompt the fingerprint, either in case of doubts of the passenger's identity (for example, the photo looks different), or in the case of suspected jihadism.

Conclusions

The principle of purpose limitation, as mirrored in the Charter and in secondary EU law, requires personal data to be processed only for specified and explicitly defined purposes. EU institutions and Member States need to reflect the principle of purpose limitation when regulating lawful access to IT systems. Safeguards to prevent unlawful access will contribute to ensuring compliance with purpose limitation rules. Such safeguards include log files that record audit trails, along with spatial (physical) as well as electronic access control. Ensuring safeguards may be particularly challenging when private actors can access limited sub-sets of data stored in the systems, as envisaged in ETIAS and the EES. Ensuring purpose limitation if IT systems are made interoperable involves particular challenges. Data protection by design and by default continue to be relevant in the development of technical solutions for IT systems.

The EU IT systems are vulnerable to 'function creep', meaning that data may be used for purposes which were not initially envisaged. Further purposes are included, which are additional to the original purpose. Access by law enforcement for fighting serious crime and terrorism and enforcing immigration law are typical examples. There is no prior evidence of involvement in crime for persons included in the IT systems, with the exception of ECRIS-TCN and some categories in SIS II. Therefore, EU law allows law enforcement authorities to access stored data only under certain conditions: there must be reasonable grounds to consider that information can be found in the database and access must substantially contribute to fighting serious crime and terrorism. Additional safeguards limit the data that can be searched and employ the cascading system,

237 SIS II police proposal, Art. 20, Art. 22 (1) (b).
238 By using the number of the visa sticker in combination with verification of fingerprints of the visa holder. VIS Regulation, Art. 18 (1).

which requires other databases to be checked first before consulting Eurodac, EES and ETIAS.

Access by law enforcement may have a disproportionate effect on children, particularly if ECRIS-TCN becomes interoperable with other IT systems. This includes the impact on children with convictions related to migration or trafficking in human beings, and the sensitivity of children's criminal records. Data on children may be retained for considerable time and may be used for migration management purposes. The Convention on the Rights of the Child and the Charter require special attention to be given to the treatment of children alleged as, accused of, or recognised as having infringed the penal law. Children should not suffer disproportionate consequences for decisions made by their parents – for example, to enter the EU as irregular migrants.

IT systems have the potential to help identify missing persons, in particular unaccompanied children, as well as victims of crime. Interviewees pointed out that the focus remains, however, on perpetrators, and that a more victim-centred approach is needed. For example, the small-scale survey at DMCPs showed that it is rare for special measures to be taken for suspected victims of trafficking in human beings, which could reflect the absence of measures, but also the possibility that staff did not often come across suspected victims of trafficking in human beings or victims of crime.

Aside from their specific purpose, most IT systems are also intended to contribute to enforcing immigration law. The immigration status of a third-county national will be available in an increasing number of IT systems. This objective can be achieved more effectively if the IT systems are made interoperable. Thus, consulting IT systems will be increasingly attractive for immigration control purposes to enhance the efficiency of apprehending and returning migrants in an irregular situation. Depending on how this is done, there is a risk that fundamental rights of migrants in an irregular situation are disproportionately affected. It may lead to migrants not approaching healthcare providers because they fear that their personal data will be handed over to other authorities for apprehension purposes, or not reporting crimes to the police, which also leads to impunity on the part of perpetrators of crime. The necessity and proportionality of enhancing the effectiveness of the immigration control objective through interoperability needs to be carefully considered in light of the possible impact on the rights of migrants in an irregular situation. Applying FRA's guidelines on the rights-compliant apprehension of migrants in an irregular situation (2014) could limit the negative impact.

FRA opinion 8 suggests measures to enhance the use of IT systems to protect children. FRA opinion 9 makes suggestions on how to make the industry pay more attention to fundamental rights and FRA opinion 10 relates to preventing unlawful access to the data. FRA opinions 14–15 concern the fundamental rights impact of access by law enforcement and FRA opinion 16 concerns the use of large-scale IT systems for apprehending migrants in an irregular situation.

4 Persons in need of international protection

Charter of Fundamental Rights of the European Union

Article 18 – Right to asylum

The right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention of 28 July 1951 and the Protocol of 31 January 1967 relating to the status of refugees and in accordance with the Treaty on European Union and the Treaty on the Functioning of the European Union [...].

Article 19 – Protection in the event of removal, expulsion or extradition

1. Collective expulsions are prohibited.

2. No one may be removed, expelled or extradited to a State where there is a serious risk that he or she would be subjected to the death penalty, torture or other inhuman or degrading treatment or punishment.

Article 18 of the Charter protects the right to asylum. Effective access to international protection also forms the basis for the protection from *refoulement*, which is reflected in Article 19 of the Charter, as well as in Article 78 of the Treaty on the Functioning of the European Union (TFEU).

IT systems affect asylum applicants and beneficiaries of international protection in different ways. All asylum applicants in the EU are required to enrol their fingerprints into Eurodac, which serves to determine the Member State responsible for examining their claim. The fingerprints of persons claiming asylum are increasingly checked against VIS. This is to see if they have previously applied for a Schengen visa. With the increased attention given to internal security, many asylum applicants are checked via SIS II, particularly at points of first arrival.

This chapter looks at how the quality of fingerprints and mistakes in the alphanumerical data accompanying them can serve to influence the overall sense of trustworthiness and credibility that is assigned to an applicant for international protection. It also looks at the risk of data stored in IT systems relating to persons in need of protection being unlawfully shared with third countries. It examines the consequences of illegal access to data on possibilities for a person to seek protection. It also explores possible positive fundamental rights implications. This entails an information system supporting a person who arrived in a Member State without a passport – by being able to identify them through other means, and if such systems can be optimised to limit the risk of *refoulement*.

4.1. Application of the Dublin rules

The Dublin Regulation serves to determine which of the 28 EU Member States and four Schengen Associated Countries (Iceland, Liechtenstein, Norway and Switzerland) is responsible for examining an application for international protection. For this purpose, the Regulation lays down a hierarchy of criteria in Chapter III (Articles 7–15). The criteria give priority to unaccompanied children. If an unaccompanied child makes an application for international protection, the Member State responsible is "where a family member

or a sibling" of the child is present.[239] The Regulation also guarantees family unity by ensuring that family members of beneficiaries or applicants of international protection can make their asylum application in the same Member State.[240] Other criteria that must be examined include whether the applicant has a valid residence permit or visa issued by another Member State (Article 12), or whether the applicant entered the territory of a Member State that has waived the visa requirement (Article 14).

For the majority of applicants none of these criteria apply. In these cases, the responsibility to examine the application lies with the Member State through which the applicant irregularly entered into Union territory. To establish the Member State where the applicant entered first, their fingerprints are checked in Eurodac (Article 13). In case of a hit, the applicant will be sent back to the first Member State following a 'take charge' request.[241]

The transfer to the Member State of first entry is not automatic. Following case law by the ECtHR and the CJEU,[242] a Member State must refrain from a transfer in certain cases. For example, if the responsible authorities are aware that systemic deficiencies in the asylum procedure and in the reception conditions of asylum seekers in the Member State of intended destination "amount to substantial grounds for believing that the asylum seeker would face a real risk of being subjected to inhuman or degrading treatment within the meaning of that provision." In practice, authorities may take a very strict approach, as the following example illustrates. A Syrian family with five children appealed the decision of the German Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge* – BAMF) to transfer them back to Italy, which was responsible for processing the case, according to the Dublin rules as established by a hit in Eurodac. The local administrative court in Germany ruled that the mother and children should not be deported, due to shortcomings in the Italian system, but the father should. The father appealed and the Federal Constitutional Court was of the opinion that the family was to follow him to Italy. An interim injunction from the ECtHR stopped the transfer.[243]

To ensure a correct application of the Dublin Regulation, high quality fingerprints in Eurodac is of paramount importance. As described in Chapter 1, false matches are rare due to the strict quality controls for Eurodac. Responsibility for processing a claim is determined based upon matches with Eurodac as well as VIS. Although rare, instances of false matches resulting in wrong Dublin transfers were mentioned by officers interviewed during the field-research. Although most instances have been clarified, they cannot be aware of those that remain unclarified.

A provider of legal assistance in Sweden explained a case whereby an asylum seeker was transferred to another Member State, in accordance with the Dublin procedures. However, the transfer was based upon a false biometric match. In the other Member State, the fingerprints were taken again and there was no match, which proved that the asylum seeker was indeed right in objecting to his transfer. Nonetheless, the asylum seeker continued to be met with distrust. The processing of the case was delayed by 6 months to 1 year. He was detained in Belgium and had no access to legal representation, even after the mistake was discovered. As a consequence, the applicant suffered mental health issues. The provider of legal assistance representing the asylum seeker in Sweden could not legally challenge the claims and statements made by the Swedish Migration Agency. The provider of legal assistance has no opportunity to undertake a biometric test to prove that the client was right. Although conducting such a test should be possible in theory, it would be difficult in practice. Furthermore, the legal assistance did not have access to all relevant information and documents regarding the events that had taken place in Belgium. Regardless of the arguments or evidence the legal assistance presented, the authorities appeared to have already decided on the case. Later on, the provider of legal assistance had troubles getting in contact with the client. The provider of legal assistance found it close to impossible to understand who was responsible for the mistake and if there were any legal possibilities to claim compensation. In any case, such a claim would have had to be pursued pro bono.

239 Dublin III Regulation, Art. 8 (1); Article 2 (g) defines family members as the family already existing in the country of origin, including the "spouse of the applicant or [their] unmarried partner in a stable relationship, where the law or practice of the Member State concerned treats unmarried couples in a way comparable to married couples under its law relating to third-country nationals; the minor children of couples referred to in the first indent or of the applicant, on condition that they are unmarried and regardless of whether they were born in or out of wedlock or adopted as defined under national law, when the applicant is a minor and unmarried, the father, mother or another adult responsible for the applicant, whether by law or by the practice of the Member State where the adult is present, when the beneficiary of international protection is a minor and unmarried, the father, mother or another adult responsible for [them], whether by law or by the practice of the Member State where the beneficiary is present. "

240 Dublin III Regulation, Art. 9 and 10.

241 Dublin III Regulation, Art. 21.

242 ECtHR, *M.S.S. v. Belgium and Greece*, No. 30696/09, 21 January 2011. CJEU, Joint cases, C-411/10 and C-493/10, *N. S. v. Secretary of State for the Home Department and M. E. and Others v. Refugee Applications Commissioner and Minister for Justice, Equality and Law Reform*, 21 December 2011.

243 ECtHR, *E.A. v. Germany*, No. 64208/11, 10 July 2012.

VIS matches also impact Dublin responsibilities. In the context of the VIS evaluation, national authorities have reported cases where there was no match in the VIS, despite the asylum applicant having applied for a visa. This means that the Dublin rules could not be implemented as foreseen.[244]

The overall trustworthiness and credibility of the applicants may be affected. If the texture of the skin results in low fingerprint quality, or even makes it impossible to enrol fingerprints, there is a tendency to assume that the applicant is trying to avoid fingerprinting.

Similarly, inaccurate data in databases result in suspicion that the applicant has intentionally used false documents or given incorrect data. There are many reasons for inaccurate alphanumeric data in national databases, such as mistakes in names and surnames. For example, wrong transcriptions can cause errors, but some asylum applicants intentionally use false documents or give incorrect data. The common perception among public officers is that using false identity is a criminal act and should be treated as such. However, some migrants may be physically unable to obtain the documents necessary to travel (such as a passport or a visa) when escaping persecution or conflict.[245] Some seek to hide their identity when fleeing their country of origin in order to protect themselves.[246]

4.2. Data sharing with third countries

Sharing data with third countries infringes on the privacy of the person concerned. In the case of persons in need of international protection, it may endanger their safety or the safety of their family members. Interoperability will make access to data easier and therefore increase the risk that data are unlawfully shared with third countries.

IT systems include large amounts of data on third-country nationals that are attractive to organised crime groups, as well as hackers linked to foreign governments seeking to prevent political opponents from leaving those states. If IT systems are not immunised against unlawful access by countries of origin, asylum applicants or their family members who remain in the country of origin may be exposed to acts of retaliation to force dissidents to return, hence undermining the right to asylum.[247]

The new EU data protection framework as well as the individual legal instruments establishing the various EU databases strictly regulate the transmission of data to third countries. Chapter V of the GDPR obliges both the data controller and processor to ensure that data processed after transfer to a third country or an international organisation complies with data protection rules. The controller and processor will also be responsible for onward transfers, for example, from one third country to another.[248]

Due to the different types of data stored in the individual IT systems, data sharing with third countries and international organisations is regulated differently in each of the existing or proposed information systems, as illustrated in Table 12. The proposed ETIAS Regulation (Article 55) contains an explicit prohibition to share the information contained therein with third countries and international organisations, with the exception of Interpol. Other systems allow for sharing personal data with third countries to identify a third-country national for the purpose of return, albeit with some exceptions.[249] To facilitate police cooperation, under certain conditions a Member State may also share SIS II data with third countries through mechanisms used by Europol (Article 41), Eurojust (Article 42) and Interpol (Article 55), according to the SIS II Decision 2007/533/JHA. The ECRIS-TCN proposal does not allow for sharing with countries, but states' requests on previous convictions contained in ECRIS-TCN must be addressed to Eurojust, which will contact the Member State holding information on the conviction (Article 14 (1)).

Typically, information is shared to obtain the assistance of the country of origin for purposes of identifying a third-country national in view of a future removal. This also concerns rejected asylum applicants.

Sharing personal data with third countries can lead to particular risks in the case of persons in need of international protection, where they or their families may be subject to retaliation measures ranging from criminal sanctions upon return, to persecution of family members. In general, there is a prohibition to share information that a person applied for international protection in the EU with third countries,[250] although

244 European Commission (2016a), p. 44.
245 In relation to the non-penalisation of the use of fraudulent documentation and the applicable UNHCR standards, see, for example, FRA Opinion on the exchange of information on third-country nationals under a possible system to complement the European Criminal Records Information System), p. 11.
246 See in this regard also the opinion of Advocate General Sharpston in CJEU, C-554/13, *Z. Zh. and O. v. Staatssecretaris van Veiligheid en Justitie*, delivered on 12 February 2015, para 63.
247 See FRA (2016a), pp. 31–33; and FRA (2016b), pp. 54–55.
248 General Data Protection Regulation, Art. 44.
249 See EES Regulation, Art. 41 (2); SIS II return proposal, Art. 10; VIS Regulation, Art. 31 and Eurodac proposal, Art. 38.
250 This is expressed in Article 48 of Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast), OJ 2013 L 180/60 (*Asylum Procedures Directive*), as well as in Article 35 of the present Eurodac Regulation.

Table 12: Purposes allowing sharing data with third countries in existing and planned EU IT systems

Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS II Regulation and** *borders proposal*	*SIS II return proposal*	**EES Regulation**	*ETIAS proposal*	**ECRIS-TCN**	*Interop. proposals (CIR and MID)*
For return purposes	For return purposes	No, only by Europol and Eurojust with the consent of the Member State who issued the alert, and by Interpol for checking against Interpol databases (SLTD), under certain conditions.	No, only by Europol with the consent of the Member State who issued the alert	*For return purposes*	*For return purposes*	*No, only for checking against Interpol databases (SLTD and TDAWN)*	*No, only by addressing Eurojust who will contact the Member State holding information*	*No*

Note: *Proposed systems and proposed changes in italics.*
Source: *FRA, based on existing and planned legislative instruments (2017)*

safeguards are not always systematically followed, as FRA research showed. Civil society organisations reported, for example, that Bulgaria shared all fingerprints of asylum seekers claiming to be Syrians with the Consular Section of the Syrian Embassy and that this has put the safety of the concerned persons at risk.[251] Providers of legal assistance interviewed also mentioned Polish cases when the status of Vietnamese persons as asylum seekers were not correctly registered in the IT systems and they were treated as migrants in an irregular situation subject to return and not in need of protection. The fear that the information will be shared with third counties is present among asylum seekers and migrants. For example, one asylum seeker (2016) in Melilla explained that he feared his fingerprints could be shared with his country of origin as he did not know the purpose and destination of the fingerprinting.

To prevent such risks, in the case of asylum applicants, information is normally only shared with the third country at the end of the asylum procedure. However, in specific circumstances, this may also be done before the procedure is completed, for example following a rejection of the application by the administration but where an appeal to the court is still pending. Such an approach can put people at risk.

Some third countries punish their own nationals for applying for asylum abroad. This was, for example, reportedly the case in Eritrea.[252] It is, therefore, important to pay attention to what information is shared with whom. The ECtHR noted that communication between the authorities of the host country and the consular services of the country of origin for the purpose of return, without explicitly informing that the person has applied for international protection, may give the country of origin sufficient information from which it can be inferred that the person is a rejected asylum seeker.[253]

Given the steady increase in data collected in individual databases, interoperability can further exacerbate the risk that the data communicated to third countries may be sufficient to identify a person as an asylum seeker or give indications – for example based on the length of stay – of conduct. This may lead some countries of origin to threaten or harm the person or their family members.

To mitigate the risk of serious harm for asylum applicants or their families, the proposed changes to the Eurodac Regulation clearly forbids sharing information regarding the fact that the individual has applied for asylum (Article 38 (2)). The existing safeguard which bans the transfer of personal data to third countries if there is a real risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of their fundamental rights, also continues to apply. The scope of this safeguard is, however, limited to data which are exchanged between Member States

251 European Council of Refugees and Exiles (ECRE) (2013), 'Bulgaria accused of putting asylum seekers at risk by providing information on Syrians to Syrian embassy', Brussels, 31 October 2013.

252 Amnesty International (2013), p. 30. For a general finding on migrants returned to Eritrea see: Human Rights Council (2015), para 444.

253 ECtHR, *F.N. and Others v. Sweden*, No. 28774/09, 18 December 2012, paras 74-76.

following a match in Eurodac. In its 2016 legal opinion on the proposed Regulation, FRA suggested that this safeguard should also apply to personal data stored in the system and not only to data exchanged after obtaining a match.[254]

Sharing data often occurs in the framework of EU or bilateral readmission, or law enforcement agreements. Data are then shared with third countries along principles similar to those used in the Prüm cooperation, namely through comparison against each other's biometric databases on a hit/no-hit basis. This provides the possibility for a very precise identification of an individual in the third country, which may, in certain situations, expose the person and their family members to serious harm.

According to a report by the European Data Protection Supervisor, the majority of interviewed Member States (15 out of 22) said that as a rule, VIS data are not shared with other national or international authorities. However, four EU Member States added that in theory such data could be shared in exceptional cases, which is permitted according to Article 31 (2) of the VIS Regulation. Three Member States permitted national law enforcement authorities to share data with other authorities if necessary, to comply with obligations under national law.[255]

4.3. Potential benefits of large-scale IT systems

Many persons arrive in the EU without travel documents. This makes it difficult to establish their identity and may lead to negative consequences for them, ranging from delays in the asylum procedure to undermining their actual chances to obtain international protection. If these persons have previously travelled to the EU, their fingerprints can be compared with those contained in other databases such as VIS or the EES, thus confirming their claimed identity and avoiding negative consequences of the inability to produce valid travel documents.

The use of IT systems can also prevent asylum applicants from being illegally returned in violation of the principle of non-*refoulement*. Police officers can consult Eurodac and national databases that include information on the protection status of the person when apprehending a migrant. They are able to see if a person is registered as an asylum applicant. A Polish provider of legal assistance interviewed during the field research explained that because an asylum application had not been entered in a database, the asylum applicant was unlawfully sent to a detention centre for irregular migrants. The person spent some time in the centre, was subsequently freed and provided a compensation for their unlawful detainment.

Not consulting IT systems may result in risks of violating the principle of non-*refoulement*. For example, in Slovakia, police officers did not consult an IT system for checking the protection status of the returnees. As a result, persons who had applied for asylum in other Member States were returned.[256] Finally, technical problems may make it impossible to access an information system, resulting in the unlawful expulsion of the person.[257]

4.4. The right to leave any country, including your own

The existence of a past entry ban and an entry into Interpol databases may prevent third-country nationals from seeking safety in the EU. The right to leave any country, including your own, is protected by international human rights law.[258]

Persons in need of international protection, however holding an entry-ban issued by an EU Member State who and have returned to their country of origin will be prevented from reaching the EU through legal channels. If, as a result of changes in the country of origin, the person has a well-founded fear of persecution, or has fled to another country from where he or she has been identified for resettlement in the EU, the existence of a past entry ban will raise additional complications.

"[A]ccess to protection is something that could be severely impeded if there are strong ways of preventing a person from entering the territory… This could lead to situations where people are unlawfully refused entry and refused access to protection systems." (Fundamental rights expert, male)

A visa applicant who has an entry ban can still be issued a visa with limited territorial validity. Such a visa is only valid in the Member State that issued the visa.[259] More than half of EU Member States refuse a visa application without further investigation, if the person has an entry ban (Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Finland, Germany, Greece, Hungary, Lithuania, Luxembourg, Poland, Portugal and

254 FRA (2016a), p. 31.
255 VIS Supervision Coordination Group (VIS SCG) (2016), p. 6.
256 Slovakia, The Slovak Humanitarian Council.
257 Łysienia, M. (2014), pp. 50–51.
258 UN (1966), International Covenant on Civil and Political Rights, 16 December 1966, Art. 12 (2); Council of Europe (1963), Protocol No. 4 to the European Convention on Human Rights, 16 September 1963, Art. 2 (2).
259 Visa Code, Art. 25.

Spain). In other Member States, for instance in France, Latvia and the Netherlands, the consular or diplomatic representation often consult the Ministry for Foreign Affairs for advice when the person is registered in SIS II, before rejecting their visa.[260]

EU Member States frequently rely on data stored in Interpol databases to detect false documents. One example would be the Interpol Stolen and Lost Travel Documents Database (SLTD). Third countries may report travel documents as stolen or lost for these to be included in SLTD. This could be misused to prevent persons in need of protection, such as political opponents, from leaving the countries. Over-reliance on data stored in the Interpol database could prevent EU Member States from issuing visas to persons in need of international protection.

Conclusions

Under EU law, Article 18 of the Charter protects the right to asylum. Effective access to international protection also forms the basis for the protection from *refoulement*, which is reflected in Article 19 of the Charter as well as Article 78 of the Treaty on the Functioning of the European Union. Asylum applicants and beneficiaries of international protection can be affected by the use of data in IT systems in different ways. First, all asylum applicants in the EU have to enrol their fingerprints into Eurodac, which serves to determine the Member State responsible to examine their claim. Second, the fingerprints of persons claiming asylum are increasingly checked against VIS. This is to see if they have applied for a Schengen visa in the past. Finally, with the increased attention given to internal security, many asylum applicants are checked in SIS II, particularly at points of first arrival.

The high quality of fingerprints in Eurodac is of paramount importance to ensure the correct application of the Dublin Regulation. If the texture of the skin makes it impossible to enrol fingerprints, or results in low fingerprint quality, there is a tendency to assume that the applicant is attempting to avoid fingerprinting and does not want to co-operate with authorities. This may impact the overall sense of trustworthiness and credibility of the applicant in question – according to findings of the FRA field research. Similarly, inaccurate data in databases results in the suspicion that the applicant has intentionally used false documents or given incorrect data.

IT systems including data on asylum applicants may be particularly attractive for hacking by oppressive regimes or persecuting agents. Strong data security safeguards must limit such risks.

Sharing data stored in IT systems with third countries may endanger the safety of applicants for international protection or the safety of their family members. The new EU data protection framework, as well as the individual legal instruments establishing the various EU databases, strictly regulate the transmitting of data to third countries. Typically, information is shared to obtain the assistance of the country of origin for purposes of identifying a third-country national in view of a future removal. This also concerns rejected asylum applicants. Generally, it is prohibited to share information with third countries about whether a person has applied for international protection in the EU. However, safeguards are not always systematically followed, as FRA research has shown.

Data stored in IT systems can also be used to benefit fundamental rights. If applicants for international protection have previously travelled to the EU, their fingerprints can be compared to those contained in other databases such as VIS or the EES, thus confirming their identity and avoiding negative consequences resulting from the inability to produce valid travel documents. The use of IT systems can also prevent asylum applicants from being illegally returned in violation of the principle of non-*refoulement*. As police officers can consult Eurodac and national databases that include information on the protection status of the person when apprehending a migrant, they are able to see if a person is registered as an asylum applicant.

The right to leave any country, including your own, is protected by international human rights law. The existence of a past entry ban, or an entry in an Interpol databases SLTD (Stolen and Lost Travel Documents) and TDAWN (Interpol Travel Documents Associated with Notices database) may prevent third-country nationals from seeking safety in the EU. According to FRA research, more than half of EU Member States systematically refuse a visa application without further investigation as to whether the person has an entry ban. This has a considerable impact on applicants' opportunities to seek safety.

FRA opinions 11–13 point to ways to increase respect for the right to seek asylum.

260 Franet.

5 How data quality affects fundamental rights

Charter of Fundamental Rights of the European Union

Article 8 – Protection of personal data

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

This chapter deals with the quality of data stored in existing IT systems. There is generally a high trust in the reliability of a biometric match, meaning when the biometrics are taken for comparison with those stored in an IT system. The person concerned will generally have difficulties to rebut a wrong assumption based on a false biometric match or no match. As described in Section 4.1 the person concerned has no possibility to undertake a biometric test to prove that the Member State was wrong. The power of biometrics lies in that it connects a person to alphanumerical data stored in an IT system, which is the basis for decisions affecting the future of that person: their right to asylum, right to private and family life, or if they are at risk of detention.

This chapter describes data quality problems and how these may affect the rights of people concerned. It deals with data entry mistakes, flawed decisions that constitute the basis for an entry in a database (for example, an entry ban), non-deletion of data when the retention time expires, as well as with measures to address these failings. It illustrates how weak a person's position is, in relation to the authorities and the seeming 'objectivity' and hence 'reliability' of data. Authorities often suspect identity fraud when cases of data quality are the real reason for concern.

5.1. Principle of data accuracy

Under the principle of data accuracy – reflected in Article 5 (1) (d) of the General Data Protection Regulation, as well as Article 4 (1) (d) of the Police Directive – the controller should not use information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. The controller must take every reasonable step to ensure that inaccurate personal data are erased or rectified without delay.

The principle of data accuracy is also reflected in national data protection law and in all legal instruments regulating EU IT systems.[261] The proposal for the new eu-LISA Regulation includes ensuring an adequately

261 See, for instance, Belgium, Act on the protection of private life regarding the processing of personal data (*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel/Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens*), 8 December 1992, Art. 4 (1) (4); Spain, Organic Law 15/1999, of 13 December 1999, on *Protection of Personal Data* (*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*), 14 December 1999, Art. 4 (5). See also, VIS Regulation, Art. 29 (1) (c); Eurodac Regulation, Art. 23 (1) (c); Eurodac proposal, Art. 24 (1) (c); SIS II Regulation, Art. 34 (1); SIS II Decision, Art. 49 (1); SIS II police proposal, Art. 56 (1); SIS II borders proposal, Art. 39 (1); SIS II return proposal, Art. 13; EES Regulation, Art. 39 (1) (c); ETIAS proposal, Art 7 (2) (a) and 8 (2) (a); ECRIS-TCN, Art. 13 (1) (d).

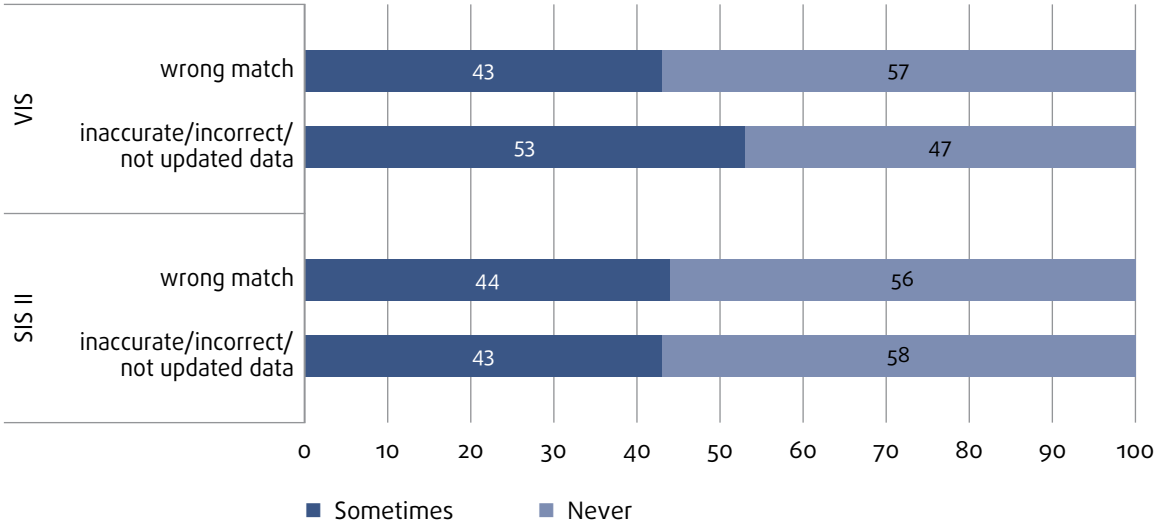
high quality of service for users of large-scale IT systems among the objectives listed in Article 2.[262]

Data contained in IT systems are generally perceived as accurate and trustworthy. The public officials and experts interviewed in the project consider biometrics (especially fingerprints) as a very effective identifier to reduce identification errors.

National courts have also upheld the reliability of a biometric match. As an illustration, in the United Kingdom, three asylum applicants disputed their Dublin transfer, saying that they had not had an opportunity to contest the fingerprint evidence. The England and Wales High Court (Administrative Court) stated that a Eurodac match normally discharges the burden of proof on the Secretary of State and does not need to be corroborated. This puts the onus on the asylum applicants to produce evidence to disprove the match.[263]

FRA's small-scale surveys at border crossing points and DMCPs confirmed that alphanumerical data in EU IT systems are not always accurate. The reasons are manifold as Section 5.2 shows, and may originate from, for example, administrative mistakes and technical deficiencies to inaccurate data fed into the system. Staff at BCPs and DMCPs were asked how often they or their colleagues find that some of the personal data – such as name, sex, nationality or age – inserted in VIS or SIS II are inaccurate, incorrect or not updated. For SIS II, more than 40 % of DMCP staff and for VIS slightly more than 50 % indicated that incidents of wrong matches or inaccurate data sometimes occur in these databases, as FRA reported in its publication on interoperability. It should also be noted that SIS II searches can be made for both exact and non-exact matches. Problems with data accuracy in SIS II[264] and VIS[265] have been underlined in evaluations by the European Commission, the European Data Protection Supervisor (EDPS), the Council Working Party on Information Exchange and Data Protection (DAPIX) and the High Level Expert Group on information systems and interoperability.[266]

Figure 11: Experiences with wrong matches and inaccurate data in VIS and SIS II at DMCPs (%)



Note: *The number of respondents varies for the replies, ranging from 39 to 53 persons, depending on the DMCP. The results are based on the following two survey questions: "Have you or one of your colleagues ever experienced that some of the personal data – such as name, sex, nationality or age – inserted in VIS or SIS II was inaccurate/incorrect/not updated?" and "Have you or one of your colleagues ever experienced that some of the personal data - such as name, sex, nationality or age - inserted in VIS or SIS II matched with the wrong identity?"*

Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

262 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011*, COM(2017) 352 final, 29 June 2017.

263 United Kingdom, England and Wales High Court (Administrative Court), *R (on the application of YZ, MY and YM) v. Secretary of State for the Home Department*, [2011] EWHC 205 (Admin), 10 February 2011.

264 European Commission (2016e); and European Commission (2016), SWD(2016) 450 final, Brussels, 21 December 2016.

265 European Commission (2016d); and European Commission (2016a).

266 European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, OJ 2008 C 200/1, p. 2; Council of the European Union (2016); High Level Expert group on Information Systems and Interoperability, Register of Commission Expert Groups.

Border guards participating in the small-scale survey also said that persons who should be included in VIS because of having applied for a visa frequently could not be found in the system. More than 60 % of respondents indicate that this happened at least once in the past 12 months. More than a quarter of respondents experienced this more than 10 times in the past year and a few experience this over 100 times. More than half of the border guards surveyed indicate that they at least sometimes experienced inaccurate, incorrect or not updated personal data in VIS or SIS II. Eurodac includes only very limited alphanumerical data: the EU Member State where the data were collected, gender, reference number, ID of authority, and dates (Article 11). While fewer respondents provide information on such experiences with Eurodac, almost half of those providing information still experienced some instances such inaccuracies.

There are different reasons for the presence of such a significant amount of inaccurate data in EU level IT systems. Authorities are aware that mistakes can happen and a number of efforts are in place to ensure quality. The trustworthiness of the data management system is in principle defined by the quality of the data it holds, as FRA found.

"[The main issue is] [w]hether the data management system is high quality and can be trusted by those who may be involved." (Fundamental rights expert, female)

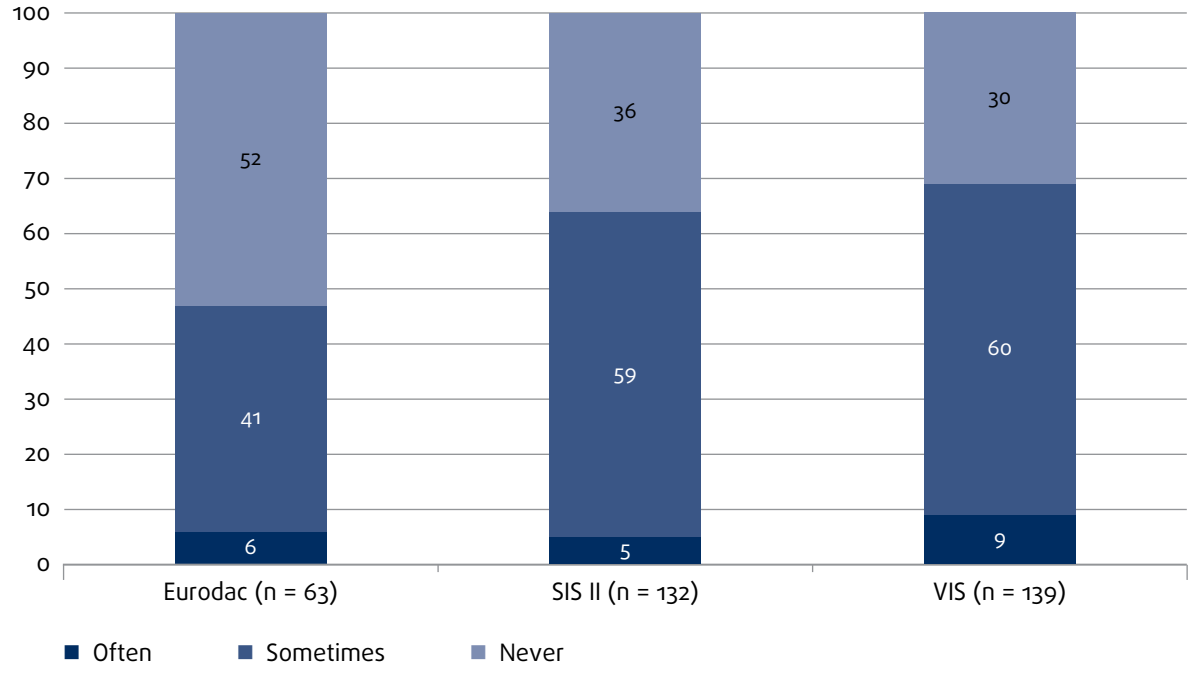
Section 5.2 illustrates the most common causes as well as quality measures in place to prevent or address mistakes when they are discovered.

5.2. Data entry mistakes and corrective measures

All IT systems except Eurodac contain a significant amount of alphanumerical data, such as the name and surname, place date of birth, nationalities, and sex of the data subject.[267] The ETIAS proposal also suggests the collection of additional data, such as the applicant's email address, phone number, education and current occupation.[268]

In its current version, Eurodac only stores the user ID of the staff member authorised to access Eurodac,

Figure 12: Experiences with inaccurate, incorrect or not updated personal data in Eurodac, SIS II and VIS at BCPs (%)



Note: *The results are based on the survey question: "Have you or one of your colleagues ever experienced that some of the personal data – such as name, sex, nationality or age – inserted in VIS, SIS II or Eurodac was inaccurate/incorrect/not updated?"*

Source: *FRA Biometrics project, BCP survey, 2016*

267 See: Eurodac proposal, Art. 12–14; VIS Regulation, Art. 9; SIS II Regulation, Art. 20; SIS II borders and police proposals, Art. 20; SIS II return proposal, Art. 4; EES Regulation, Art. 16 and 17; ETIAS proposal, Art. 15 (2).

268 ETIAS proposal, Art. 15 (2).

information on sex, and dates for the collection and transmission of data, although significantly more data will be stored in future. Registration numbers in Eurodac cannot be altered. In case of mistakes, the registration must be repeated. Unless the first registration is deleted, future queries against Eurodac will result in two hits with different registration numbers and dates.

Many factors affect the reliability of the alphanumerical data in a system, such as:

- spelling errors;
- wrong sex or nationality registered;
- lack of documents provided by a person;
- incorrect or incomplete information provided by the data subject;
- lack of interpretation in case of language difficulties leading to data entry errors;
- technical deficiencies;
- incorrect transcription of names into the Latin alphabet;
- cultural norms determining the usage of first and second names;
- recording of birth dates when the precise date is unknown;
- lack of skills and training;
- the common format for data transmissions is not followed;
- increased workload and strain on the staff recording and dealing with data.

The last point was particularly evident following the large number of arrivals in 2015. The fingerprint registration in Eurodac connects an asylum seeker to the name and date of birth stored in national databases. There were many instances when the name and/or date of birth presented in Sweden was different to the previous registration made.

A Swedish provider of legal assistance said that the majority of the clients claimed that when they transited other Member States they did not have access to an interpreter when stating their name and date of birth, despite being unable to use or understand Latin letters. In fact, the majority said that officers never asked them to state their date of birth. If asked, most of the Afghans stated their age or year of birth according the Persian/Afghan calendar. Almost everyone said that they did not know what name or day of birth the other country registered and had not been able to confirm the registered information. They also had no access to legal representation. Children claimed that they were not appointed any guardian during the registration. In Sweden, the asylum seekers were met with mistrust because of the differences in the registered names and dates of birth. They were suspected of concealing their correct identity, which affected the credibility of their asylum claims. The registration in the other Member State was typically seen as the 'correct' registration, without possibilities to make changes. This meant that children seeking asylum were considered as adults, which impacted on the application of the Dublin regulation, as these asylum seekers were more likely to be transferred to the EU Member State where they had first been registered. If then consequently granted asylum in the wrong name, for example, due to spelling errors or the wrong date of birth, these mistakes were carried over to the refugee travel document issued by Sweden, and possibly to further documents on issued citizenship. The mistakes severely affected possibilities to prove family links and apply for family reunification. A Swedish provider of legal assistance explained that when clients no longer fear that their residence permit will be questioned, they then try to change the data.

Awareness among officers about the negative consequences that mistakes in databases may have is limited. As providers of legal assistance interviewed in Italy noted, even when mistakes are pointed out during the audition in front of the Territorial Commission for the Right of Asylum, inaccuracies in writing names and surnames in national databases are not always corrected.

The required follow-up action may not be taken when a SIS II alert has been deleted for whatever reason. The judge may forget to communicate the deletion of SIS alerts, in which case the third-country national will not get a visa or be stopped at the border.

Member States are taking different measures to prevent mistakes and to correct these when they are discovered, particularly in SIS II. The main quality control measures for alphanumeric data are as follows.

Cross-checking and verifying data upon entry

Particularly for SIS II, EU law gives particular attention to ensuring data accuracy before they are entered into the system.[269] SIS II alerts on persons are entered on the basis of a judicial or administrative national decision issued in

269 SIS II Regulation, Art. 34 (1); SIS II Decision, Art. 49 (1); SIS II police proposal, Art. 56 (1); SIS II borders proposal, Art 39 (1); SIS II return proposal, Art. 13. As regulated in for instance Bulgaria, Ordinance No. 81213-465 of 26 August 2014 on the organisation and functioning of the National Schengen Information System of the Republic of Bulgaria (*Наредба № 81213-465 от 26 август 2014 г. за организацията и функционирането на Националната Шенгенска информационна система на Република България*), 5 September 2014, Article 10 (1).

respect of a specific person. In such cases, a reference to the personal data is included in the national decision. In addition, other sources of information may be used (for example, checks on multiple identities or aliases are carried out in national, European or international databases). The officer is required to verify and process individually the data of each person before including them in the system. To avoid future problems in case the data to be entered are similar to an already existing registration in SIS II, the SIRENE Manual gives guidance on how to verify the information.[270]

In practice, some EU Member States reported to FRA that they carefully verify the information to be included in SIS II. For example, within the Danish Police a legal advisor verifies the data before they are entered into the IT system. For alerts on persons to be arrested or checked or who are missing, this includes confirming that the name and date of birth is consistent with the name and date of birth on genuine travel documents or, alternatively, with the name and date of birth in the underlying judgment or administrative decision. The legal adviser controls why the alien has been convicted, the sentence, the relevant provision of the expulsion decision and the length of an entry ban, as well as other elements.

In contrast, insufficient verification procedures before entering data into VIS were perceived as problematic by some persons who FRA interviewed.

"This is the problem of that VIS database, that it takes a lot of incomplete, loose data. There is no filter in that central database which would verify if the data are real, [w]hether someone could make a mistake inserting such and such data. There is no verification. So, you need to solve these situations individually." (Asylum and Immigration Agency, female, Poland)

The risk of mistakes is reduced if the person is actively involved in verifying the data inserted, or they have the possibility to clarify contradictions when mistakes are discovered. To avoid mistakes, in Poland, migrants are asked to fill in a special questionnaire, which is the basis for transliteration. The International Civil Aviation Organization (ICAO) has developed standardised rules in relation to Latin, Cyrillic and Arabic characters.[271] In Germany, when the police finds evident spelling errors the persons are presented with these errors to clarify them. In some EU Member States, the person has to read and verify the information being inserted. In Finland, in accordance with the Finnish 'asylum guidelines' the applicant signs the U3A form, which includes the personal data.[272] This is one way to have the individual concerned cross-check the personal data, which can help in spotting mistakes before the data are entered into the system. However, the individual concerned may deliberately provide incorrect information to avoid the consequences of a SIS II alert.

Correcting mistakes when noted

The authorities that first entered the data in the EU IT system are exclusively responsible for the lawfulness and accuracy of the data, including modifications, up-dates, corrections and deletions.[273] When authorities of other Member States become aware that such data are incorrect, they have a duty to alert the responsible Member States.[274] When they become aware of inaccurate data in EES they can correct such data themselves.[275]

For **SIS II**, a well-developed system has been set up to correct data if another Member State has initiated the alert. The SIRENE Bureaux have a formal role as data quality coordinators. The SIRENE Bureau of the Member State that notices an inaccurate alert must at the earliest opportunity, and no later than 10 days,[276] inform the SIRENE Bureau in the Schengen Member States responsible for the alert. The Member State that issued the alert must check the communication and, if necessary, correct or delete the item in question without delay, in accordance with its national procedures.[277] If no agreement is reached within two months, the SIRENE Bureau of the Member State that discovered the incorrect data must advise its national data protection authority to refer the matter to the European Data Protection Supervisor who must act as a mediator between the Member States. In practice, not all cases of inaccuracies are referred. For example, spelling mistakes may not necessarily lead to contacting the SIRENE office in the other Member State. However, if the person concerned puts forward plausible arguments that the alert may not be in force or in case of a misused identity, the procedure as laid down in the SIRENE

270 Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Commission Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (SIRENE Manual), OJ 2017 L 231/6, point 2.2.3, pp. 24–25.
271 International Civil Aviation Organization (ICAO) (2015), p. 30.
272 Finland, Asylum guidelines (*Turvapaikkaohje*), MIGDno/2013/700.
273 VIS Regulation, Art. 29 (1) (c); Eurodac Regulation, Art. 23 (1) (c); Eurodac proposal, Art. 24 (1) (c); SIS II Regulation, Art. 34 (1); SIS II Decision, Art. 49 (1); SIS II police proposal, Art. 56 (1); SIS II borders proposal, Art. 39 (1); SIS II return proposal, Art. 13; EES Regulation, Art. 39 (1) (c), ETIAS proposal, Art. 8 (2) (a).
274 VIS Regulation, Art. 24 (2); Eurodac Regulation, Art. 27 (4); Eurodac proposal, Art. 28 (4); SIS II Regulation, Art. 34 (3); SIS II Decision, Art. 49 (3); SIS II police proposal, Art. 56 (3); SIS II borders proposal, Art. 39 (3); SIS II return proposal, Art. 13; ETIAS proposal, Art. 48 (4); ECRIS-TCN proposal, Art. 9 (4).
275 EES Regulation, Art. 35 (3).
276 SIRENE Manual, OJ 2017 L 231/6, Point 2.8, p. 30.
277 *Ibid.*

Manual is generally followed.[278] Many Member States have implemented data quality control mechanisms, which may be preventive or corrective. The role of the SIRENE Bureaux, as data quality coordinators, will be enhanced according to the SIS II proposals, as they should delete alerts that have achieved their purpose.[279]

If authorities notice that its Member State is responsible for a **mistake in VIS**, they typically contact the central visa authority, which is located in the Ministry for Foreign Affairs or Interior, who will involve the embassy or consulate in question, if necessary. In some Member States, such as Belgium, the Czech Republic and Sweden, an authority that has access to VIS, such as those in charge of border controls, should make the correction. If another Member State is responsible for the inaccurate VIS entry, its central authority must inform this Member State.

As regards information to the person concerned, Member States' practices vary. Some Member States (for example Latvia, Lithuania, Malta, the Netherlands and Slovakia) inform the person about any corrections to their SIS II data if they are resident in the Member State in question. In other Member States, the person concerned is not informed (this is the case for example, in Bulgaria, the Czech Republic, Luxembourg and Slovenia) or is only informed if following an individual assessment, there is a particular need to inform them (such as in Sweden, for example). Concerning corrections of data in VIS, in some Member States, the individual concerned is notified when the authorities become aware of a mistake (for instance in the Czech Republic, Lithuania, Poland, Slovenia and Sweden). This is not the case in Latvia and Luxembourg if the verifications are manually resolved within 48 hours.

Cross-checks with information stored in other IT systems and expanded role of eu-LISA

A person can appear with divergent data in different EU or national IT systems. In case the person appears under different identities, interoperability could help connect the different identities to the same person and, therefore, help spot mistakes.[280] However, there may also be a risk that the person will be suspected of deliberately stating false information to be registered under different identities. National registers frequently form the basis for the information to be included in SIS II. In most Member States, national alerts are automatically transferred to SIS II without requiring a separate alert to be created. This also applies to the update and deletion procedures. Provided the information is correct in the national system, interoperability between the national register and SIS II reduces the risk for errors. This in turn means that the officers in charge of entering data in the national systems are responsible for their accuracy.

At present, eu-LISA does not check the quality of alphanumerical data in the same way that it checks biometric data in Eurodac, by way of an automated process. An exception is SIS II – on a monthly basis, the central system generates automated data quality reports on alphanumerical data for the Member States, containing information about alerts with possible data quality issues. Each Member State is responsible for correcting or completing incorrect data in alerts for which it is responsible. Preventive measures are put in place to avoid reoccurring data quality problems. This procedure is expected to be formalised in the new SIS proposals through the adoption of implementing measures.[281] Moreover, an action plan for the improvement of data quality has been prepared within DAPIX Renewed Information Management Strategy.[282]

A data quality control mechanism will be introduced in Article 8 of the proposal for a new eu-LISA regulation.[283] The central systems would automatically identify apparently incorrect or inconsistent data submissions – both alphanumerical as well as biometric – so that the originating Member State can verify the data and carry out any necessary remedial actions. Moreover, a central data repository, which is referred to as a 'data warehouse' in the Explanatory Note would produce statistical and data quality reports. The interoperability proposals now refer to this system as the central repository for reporting and statistics (CRRS).[284] It would contain anonymised data extracted from all the systems.[285] A central repository adds additional responsibilities to eu-LISA as well as to EDPS as the supervisory authority. EDPS questioned the repository and instead suggested a solution which would allow statistics to be extracted automatically.[286]

278 Franet, according to most EU Member State responding to the FRA questionnaire.
279 SIS II police proposal Art. 51 (5); SIS II borders proposal Art. 34 (4); SIS II return proposal, Art. 13.
280 High Level Expert Group on information systems and interoperability (HLEG) (2017), pp. 32–33.
281 SIS II proposal police co-operation, Art. 15; SIS II proposal border checks, Art. 15, SIS II proposal return, Art. 13.
282 Council of the European Union, Working Party on Information Exchange and Data Protection (DAPIX) (2016), p. 9.
283 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011*, COM(2017) 352 final, 29 June 2017.
284 Interoperability proposals, Art. 39.
285 Interoperability proposals, Art. 39 (3).
286 European Data Protection Supervisor (EDPS), *EDPS Opinion on the proposal for a Regulation on the eu-LISA*, Opinion 9/2017, Brussels, 9 October 2017, p. 9.

Interoperable IT systems would make access to data easier for the end-user, ensure the correct identification of persons and harmonise quality requirements.[287]

Mistaken or confused identity

Two persons may have the same identity details (typically, same name, date and place of birth) in the IT system.

Mistaken identity can have particularly severe consequences for the person concerned. For example, a person is mistakenly arrested or stopped when crossing the border. Border guards interviewed in the field research told about victims of mistaken identity who learnt that they had been issued an entry ban by a state they never visited. The issues can usually be solved through follow-up questions.

According to information FRA collected from Member States relating to SIS II, between 2012 and 2014, Austria, Estonia, Lithuania, Malta and the Netherlands recorded between zero and 50 instances of mistaken identities, whereas Germany reported 100 to 200 instances. Other Member States did not provide the requested information.

The burden to demonstrate that the person stopped or apprehended is not the person who was issued the alert lies on the person concerned, in addition to them being inconvenienced and losing time during border checks. Typically, at border crossing points, the person who gets a hit in SIS II, but is not the subject of the alert is taken aside for further questioning.

If it becomes clear that the person stopped is not the person wanted by an alert, supplementary information can be added to the SIS II alert, provided the person concerned consents to including also his or her – preferably biometric – personal data, preferably biometric data. The stored data shall only be there for establishing the identity of the person and shall not be used for any other purpose.

Sources: Franet questionnaires to the Member States; SIS II Regulation, Art. 34 (5); SIS II Decision, Article 49 (5); SIRENE Manual, point 2.12.1, p. 32, Franet research.

5.3. Flawed administrative decision

Mistakes can also occur earlier, during the administrative or judicial process. Data entered in an information system could be based on an administrative decision that an EU Member State has taken without respecting the procedural and substantial safeguards included in EU or national law. This issue emerges particularly in the context of SIS II, as it includes issued alerts that are based on administrative or judicial decisions taken by Member States.

Member States have to ensure that an entry is not based upon a flawed administrative decision. In practice, the officer typically checks and confirms that the legally prescribed conditions justifying the entry in SIS II are fulfilled. The validity of decisions or criminal sentences that form the basis for entering data in SIS II should also checked. In the case of any doubts, an inquiry should be conducted. Each case is processed individually.[288] The SIRENE Manual gives guidance on how to verify information when the data to be entered are similar to an already existing registration.

A critical type of decisions are entry bans issued according to Article 11 of the Return Directive (2008/115/EC).[289] When exercising their discretionary powers, for example, to determine the length of an entry ban, Member States must respect the principle of proportionality.[290] In particular, an entry ban decision must be balanced against the right of the foreigner to enjoy their family life. Past interventions by the Greek Ombudsman illustrate that a proportionality assessment does not always take place.[291]

The Member States have the possibility to refuse taking action based on an alert if it is incompatible with its national law, its international obligations or essential national interests. This could include, for example, situations in which the Member State considers the individual's fundamental rights to be disproportionately affected. As a DMCP staff of Germany explained, in such an instance, it would still be possible to issue the visa – which would be a visa with limited territorial validity (LTV)[292] – but they would also have to inform the Federal Foreign Office. This is because the police and border guards need to be aware of exceptions to allow individuals to enter the country.

287 Interoperability Proposals, Art. 2.

288 As regulated in for instance Bulgaria, Ordinance No. 81213-465 of 26 August 2014 on the organisation and functioning of the National Schengen Information System of the Republic of Bulgaria (*Наредба № 81213-465 от 26 август 2014 г. за организацията и функционирането на Националната Шенгенска информационна система на Република България*), 5 September 2014, Art. 10 (1).

289 Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, OJ 2008 L 348/98 (*Return Directive*).

290 Additionally, see in this context, Annex to the Commission Recommendation establishing a common "Return Handbook" to be used by Member States' competent authorities when carrying out return related tasks, C(2017) 6505, 27 September 2017, pp. 22 and 49.

291 Greek Ombudsperson, Human Rights Section, Intervention case no 1709/08/5, 29 November 2010, decision available in Greek; Greek Ombudsperson, Human Rights Section, Intervention case no. 15767/451312012, 20 December 2012.

292 Visa Code, Art. 25.

5.4. Reliability of biometric matches

Biometric matching is based on probability. A match may, with high probability, be a correct match. However, accuracy can only be established following a manual verification of all 10 fingerprints. The capturing and matching involves some risks –even if minimal – of false matches, these being either 'false accepts' or 'false rejects'. Accurate and transparent tools to quantify the level of uncertainty of a match prevents any unjustified and unfair decisions from occurring.[293] According to public officials FRA interviewed, the use of electronic readers to minimise manual entries, as well as automatic verification against other data entries, when applicable, could contribute to reducing the risk of mistakes.

Public officials interviewed noted that problems with the quality of biometric data are not frequent, but do occur. Given the large amount of data stored, even a low percentage of mistakes may affect a significant number of people.

"[A false match] is very rare, but on a data set of 40 million fingerprints, 0.003 % is still a significant percentage. You need to be vigilant and report it." (National visa authority, female, Belgium)

There are different factors that may affect the reliability of a biometric match, as described in the following pages together with existing or possible corrective measures.

Respect for quality standards when capturing fingerprints and facial image

The quality of the fingerprint enrolled in the database is decisive for the reliability of a future match. The stored fingerprints must respect set quality standards.[294] Although there is no standard way of measuring the print quality, NFIQ and NFIQ-II (American National Institute for Standards and Technology (NIST) Fingerprint Image Quality) have become de facto standards due to their proven high performance and availability.[295] Eu-LISA uses quality algorithms, which are very similar to the methods that NFIQ uses. The fingerprint image is converted to a template that is used for automated matching purposes.

Member States have an obligation to ensure the accuracy and quality of biometric identifiers,[296] whereas eu-LISA monitors whether the quality standards are followed. The quality standards are transformed into algorithms that vendors build into their products. eu-LISA has an automatic mechanism in place to check the quality of fingerprints that will be stored in Eurodac. Fingerprints that do not respect the quality standards for Eurodac are returned to the Member State, which means that the fingerprints can continue to be stored at national level, but not by eu-LISA. Until 2015, Member States used KIT-4 equipment to capture fingerprints for VIS to ensure that prints met the standards of the central VIS system, which is managed by eu-LISA. If it was not possible to enrol any of the 10 fingerprints according to set quality standards, the visa application was submitted without any fingerprints. In 2015, the 'zero failure to enrol' policy was introduced.[297] According to this policy, it is the individual Member State's responsibility to ensure that prints meet the quality standard, and no fingerprint can be rejected because its quality is too low. eu-LISA is working together with Member States to introduce a new feature that would provide warning messages if the quality check is not passed.[298]

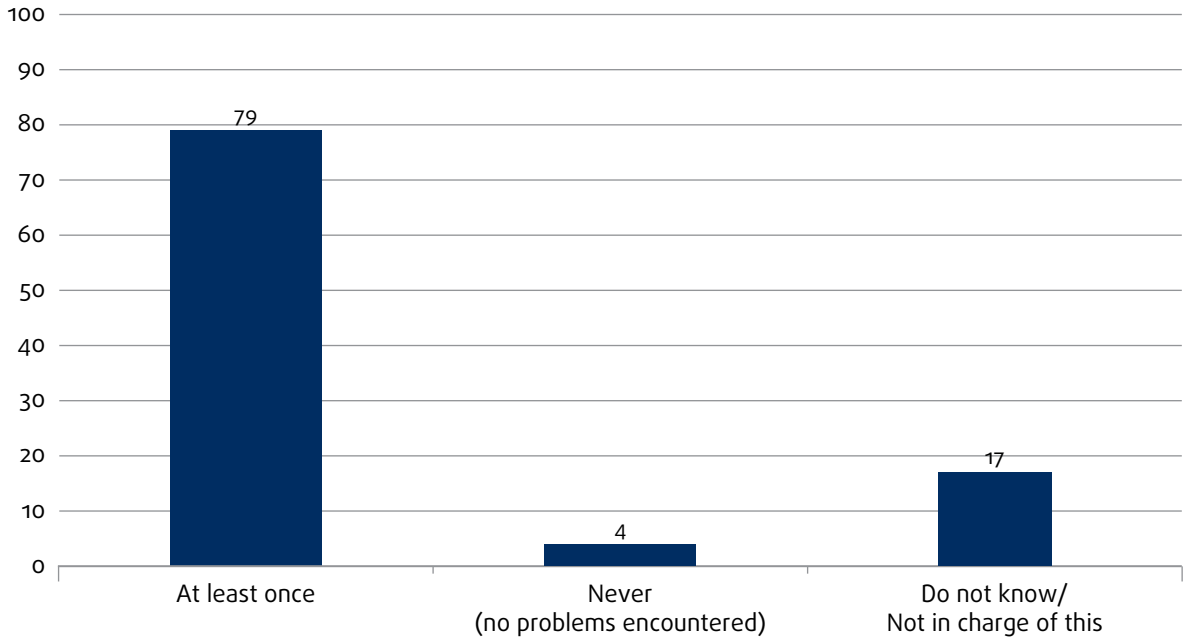
In 2016, the Eurodac central system rejected some 54,300 fingerprint datasets due to insufficient quality.[299] This may happen due to the low quality of the fingerprint image or because of a sequence check error, meaning that the fingers were recorded in the wrong order.

Staff at DMCPs and their service providers who participated in the small-scale survey frequently find that they are unable to enrol fingerprints according to the expected quality standards. Only 4 % of the staff members at both DMCPs and their service providers reported to have never had any problems with enrolling or reading fingerprints in accordance with expected standards (Figure 13).

As illustrated in Figure 14, consular staff and service providers have reported technical problems with the equipment as one of the three most frequent reasons that cause difficulties in enrolling fingerprints. The two main reasons, however, relate to physical problems, such as injured fingertips, which was experienced by 70 % of respondents who had problems with enrolling or reading fingerprints.

293 eu-LISA (2015a), p. 40.
294 Commission Implementing Decision (EU) 2016/1345 of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II), OJ 2016 L 213/15.
295 European Commission (2016f), p. 4 .
296 VIS Regulation, Art. 29 (1) (c); Eurodac Regulation, Art. 23 (1) (c); Eurodac proposal, Art. 24 (1) (c); SIS II Regulation, Art. 34 (1); SIS II borders proposal, Art. 39 (1); SIS II police proposal, Art. 56 (1); EES Regulation, Art. 39 (1) (c).
297 eu-LISA (2015a), p. 35; eu-LISA (2016), p. 10.
298 eu-LISA (2016), p. 10, ft. 41.
299 eu-LISA (2017a), p. 13.

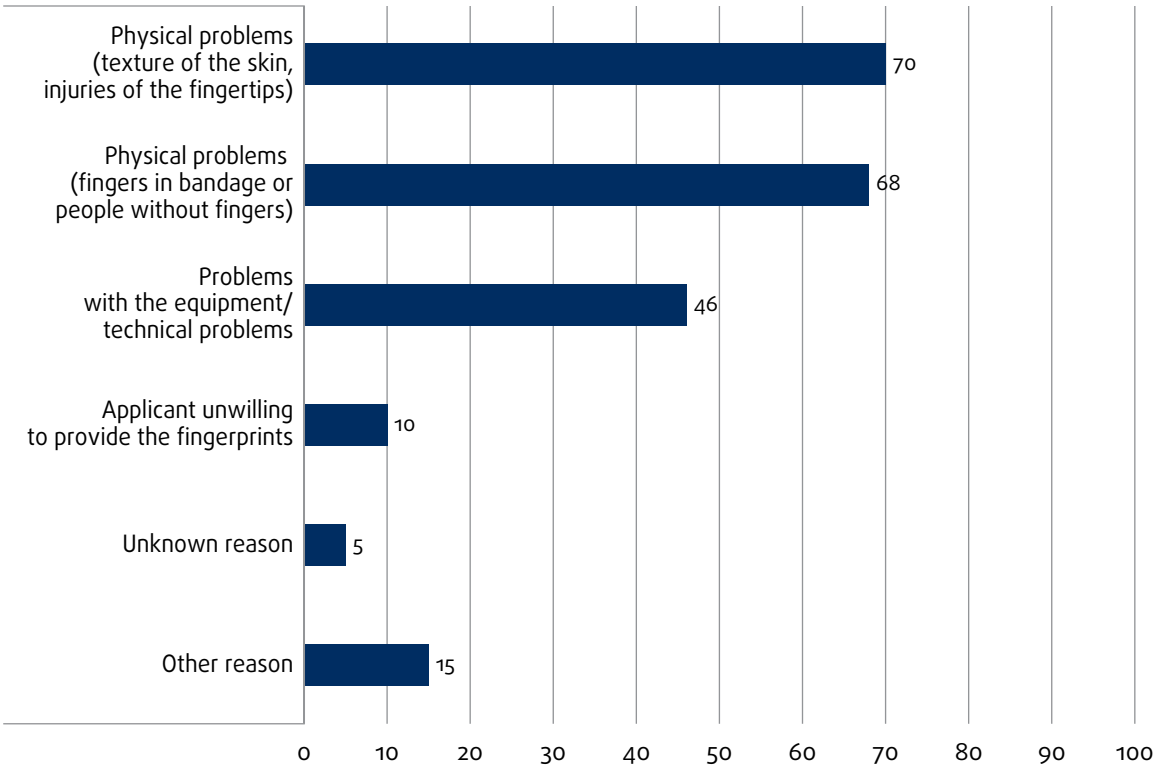
Figure 13: Experiences of quality problems in enrolling or reading fingerprints at DMCPs, past 12 months (%)



Note: *The results are based on the survey question "How often does it happen that you are not able to enrol or read fingerprints in accordance with expected quality standards? Please provide an estimated number of times in the past 12 months." (n = 126).*

Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

Figure 14: Reasons for problems encountered in the past 12 months during enrolment or reading of fingerprints (%)



Note: *The results are based on the survey question "What are the reasons for problems with enrolling or reading fingerprints that you have encountered in the past 12 months? Please select all that apply." (n = 110).*

Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

Fingerprints can be collected using a **scanning device or on paper with ink**. If fingerprints are collected on paper with ink, they have to be subsequently scanned and transferred to the IT system. Although it is hard to reach the same quality with paper and ink as with scanning, there are practical advantages, such as that there is no confusing sequencing in repeat attempts. This process is used, for instance, in the airport asylum procedure in Poland.

Light Emitting Sensor (LES) Technology can be packaged into thin devices, such a mobile devices, and will improve the quality of the scan.

Conditions to acquire biometrics, such as the physical environment (for example, temperature and humidity) and the characteristics of the person concerned – in particular, age – affect the quality of fingerprints and may possibly lead to a mismatch.

An additional problem in Eurodac and VIS is that the **personal data of another person has been attached to the fingerprints**, according to interviewees in all Member States. In Eurodac, sometimes the fingerprints in the system are attached to the wrong file number. According to the VIS Regulation, visa applications should be linked to previous applications of the same person in VIS,[300] but sometimes applications are wrongly linked. In VIS, the fingerprints may have been attached to the previous applicant by mistake. For example, Polish consulates attached the fingerprints of a mother to her child's visa application. A similar situation was noted in a Belgian DMCP, where the biometrics of two applications were switched accidentally.

"The staff were doing two applications at the same time and there is only one biometrics [reader], and so they switched around (attached the biometrics to the wrong application). It happened in our embassy... so I imagine in small embassies in the world it can happen that people might not be well trained or they have so many applications that things get messed up." (DMCP, female, Belgium)

The availability of a considerable amount of alphanumerical data providing information makes it easier to detect such mistakes, which is the case in VIS. In the future, this will also be the case of Eurodac, since according to the proposal it will collect alphanumerical data.

For **facial images**, ICAO has drawn up quality standards.[301] When eu-LISA piloted facial image recognition in 2015, in more than 90 % of cases the capture was successful.[302] All planned IT systems foresee the possibility to undertake biometric searches with facial images, as soon as it is technically possible to guarantee a reliable match. The facial images stored in VIS are not yet used for facial recognition purposes, but this could be the case in the future.[303] The availability of a photograph helps to confirm the identity of a person who has been identified on the basis of a fingerprint search.

Facial images captured by surveillance cameras are not planned to be used for these purposes. They could principally also be used for matching purposes. The British police is developing and testing a pilot system that utilises surveillance footage for facial recognition.[304] In such scenarios, there is a risk for a number of probable matches and consequently a higher risk for mistakes in the matching.

The quality of facial images depends on factors, such as background and object occlusion, illumination and light reflection, ergonomics (position of the person in relation to the camera), time elapsed since the acquisition of the image, age, gender (women wearing make-up), phenotypical origin (light bounces off very white skin, not enough illumination for very dark skin) and skin conditions.[305] Facial recognition techniques have improved during the last years, but cases of lookalikes and twins may still lead to wrong matches. Furthermore, the time that passes between taking and comparing the picture affects a correct matching. Changes in the facial shape of a child also have an impact on the reliability of a match, for example, when the image of a six-year-old child is compared five years later.[306]

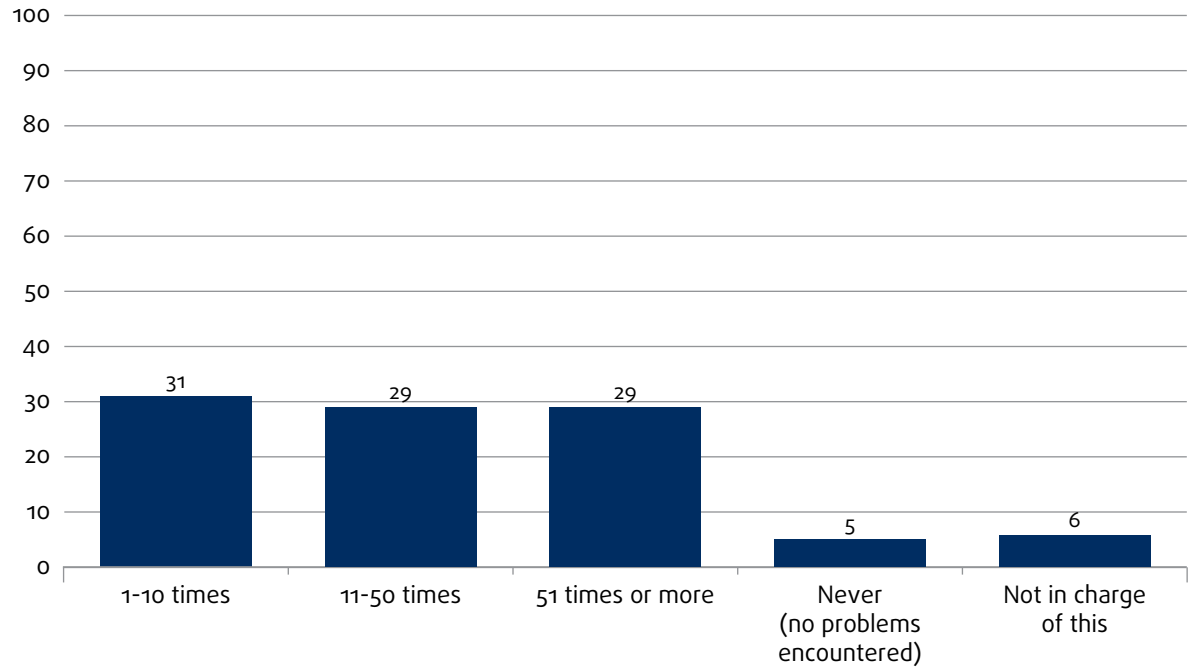
Respect for quality standards when fingerprints are matched

The question is whether the fingerprints can be accurately matched when the algorithm and the relevant matching points have changed, for example. This could be an important consideration in the context of long retention periods. This can entail particular consequences for children, as explained in Chapter 7.

Among the border guards that took part in the small-scale survey, only 5 % had never encountered problems when trying to check fingerprints against VIS in the past 12 months. As illustrated in Figure 15, more than half (60 %) were not able to check fingerprints up to 50 times in the past year and almost one out of three (29 %) were not able to perform the check 51 times.

300 VIS Regulation, Art. 8 (3).
301 ISO/IEC 19794-5.
302 eu-LISA (2015b), p. 43.
303 European Commission (2016d), p. 13.
304 eu-LISA (2015a), p. 21.
305 Sanchez del Rio, J., Conde, C., et.al., (2015).
306 Chaudhary, A., Sahni, S. and Saxena, S. (2014), pp. 82–88; Ramanathan, N., Chellappa, R., Biswas, S. (2009), pp. 131–144.

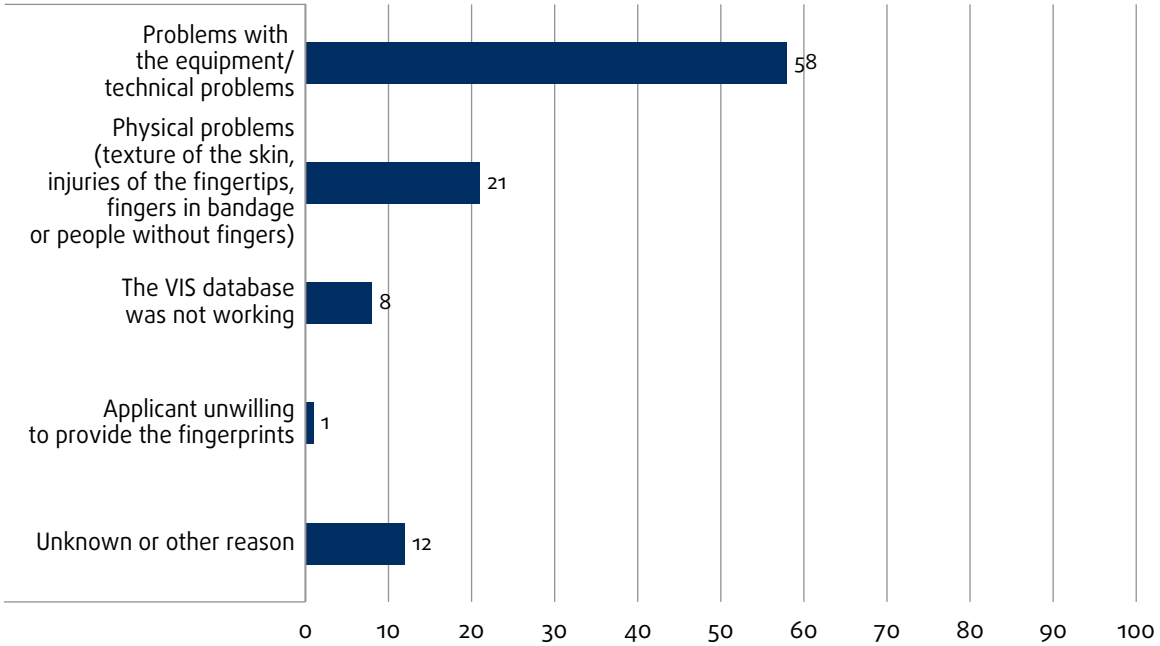
Figure 15: Estimated number of times border guards could not check fingerprints against VIS, past 12 months (%)



Note: *The results are based on the survey question "How often does it happen that it is not possible to check fingerprints against VIS? Please provide an estimated number of times when checking fingerprints against VIS was not possible in the past 12 months." (n = 148).*
Source: *FRA Biometrics project, BCP survey, 2016*

For a majority of border guards, this was most commonly due to problems with the equipment or other technical difficulties (58 %). However, a considerable number of border guards said that they were not able to check fingerprints against VIS because the system was not working (41 %) or due to the applicant's physical features, such as texture of the skin or injuries to the fingertips (42 %) (Figure 16). During the non-participant observations which took place at the same border crossing points where the survey took place, it was noted that fingerprint checks against VIS are not always systematically carried out, as also mentioned in Section 2.2 .

Figure 16: Most common reasons why border guards could not check fingerprints against VIS, past 12 months (%)



Note: *The results are based on the survey question "Which among the reasons you just mentioned for the impossibility to check fingerprints in Q8 (previous question), was the most common reason for the impossibility to check fingerprints against VIS? (TICK ONLY ONE ANSWER)" (n = 129).*
Source: *FRA Biometrics project, BCP survey, 2016*

Fingerprints change or degrade with time. Experts interviewed for the project raised in particular the case of children, as further explained in Section 7.2, and older people. The US-VISIT programme waives fingerprinting for persons over 79 years old. Injuries on fingertips also affect the quality.

An important quality assurance measure is the manual check of fingerprint matches by a **dactyloscopic expert**. In Eurodac, a dactyscolopic expert of the Member State to which the asylum applicant will be transferred verifies the correctness of the automated comparison.[307]

Human examiners generally use extended features – dots, spurs, incipient ridges, pore structures, etc. – to match fingerprints. At present, automated solutions, such as AFIS, do not equally support these features. With the increasing adoption of 1000dpi fingerprint scanners, however, it would be feasible to incorporate such features into AFIS.[308] The fingerprinting devices are equipped with a software which ensures the quality for acquiring and matching fingerprints. Devices equipped with multi-spectral imaging technology (MSI) have the capacity to read damaged and low quality fingerprints. This technology is not widely used, but Sweden, for instance, uses it when the quality of fingerprints is too low.

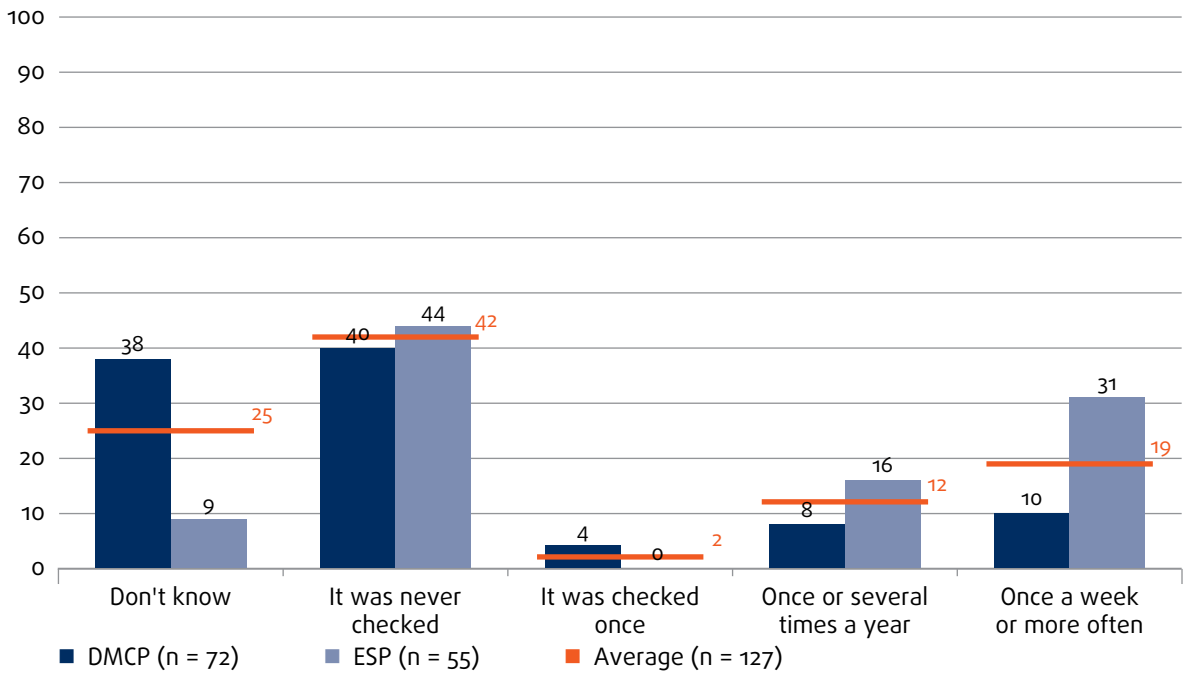
eu-LISA is informed when a dactyloscopic expert identifies a false match after comparing fingerprints.[309] A hit that falsely linked two records will be unlinked.[310] According to eu-LISA, in 2016, the Member States reported 72 false hits, representing a slight increase compared with the previous reporting period (26 false hits for the period 20 July to 31 December 2015). The majority of false hits were reported by Germany (33 %) and Italy (25 %).[311]

Insufficient guidance and supervision

Producers of devices issue instructions on how to take good quality fingerprints that national authorities often refer to in their national instructions on fingerprinting. The Finnish guidelines for asylum authorities, for example, include what to do if the device generates fingerprints of an insufficient quality.[312]

Training contributes to reducing mistakes. The industry and forensic experts provide training to staff of national authorities, who also receive on-the-spot training.

Figure 17: Frequency of checking that the fingerprinting process is carried out according to instructions (%)



Note: *The results are based on the survey question "How often is it checked that the fingerprinting process is carried out according to instructions?"*

Source: *FRA Biometrics project, DMCP officers and external service providers (ESP) survey, 2016*

307 Eurodac Regulation, Art. 25 (4); Eurodac proposal, Art. 26 (4).
308 eu-LISA (2015a), p. 13.
309 Eurodac Regulation, Art. 25 (5); Eurodac proposal, Art. 26 (6).
310 eu-LISA (2017a), p. 15.
311 *Ibid.*
312 Finland, Asylum guidelines (*Turvapaikkaohje*), MIGDno/2013/700.

Problems occur when staff frequently rotate. Some officers interviewed during the field research said that training could focus more on the interaction between the staff and the person being fingerprinted, and the role of databases.

Clear guidance on what to do if the fingerprints do not match quality standards is not systematically provided. According to FRA's small-scale survey among DMCP staff and their service providers, 79 % of the service providers have been informed about what to do if fingerprints do not meet quality standards, whereas 66 % of the DMCPs had received such training or guidance.

The small-scale survey of DMCPs and their service providers suggests that service providers are more carefully supervised regarding the fingerprinting process than staff at DMCPs. A third of the staff of the service provider said that at least once a week there was a check to see if the fingerprinting process is carried out according to instructions, whereas the same was true for only 10 % of the DMCP staff. Many respondents at DMCPs mentioned that they do not know if they are checked.

5.5. Data not deleted in time

According to the principle of storage limitation, as is expressed in Article 5 (1) (e) of the GDPR and Article 4 (1) (e) of the Police Directive, data which identify a data subject must not be retained for longer than is necessary for the purposes for which the data are processed. The data must be erased when the purpose has been served and there is no longer a justifiable reason to store them. The principle is also found in Article 5 (e) of Convention 108 and Article 5 (2) (e) of the draft modernised Convention 108. Therefore, data must be erased when the purpose has been served and there is no longer a justifiable reason to store them.

The period of data retention varies between one and 10 years depending on the purpose of the IT system, as Table 13 illustrates. Upon the expiration of the retention period, data must be automatically deleted.

In *Digital Rights Ireland*, the CJEU examined the validity of the Data Retention Directive[313] and declared it invalid due to its incompatibility with fundamental rights. One of the reasons the CJEU gave for this decision was the data retention period. It observed that the Data Retention Directive required data to be retained for a period of at least six months, without distinguishing between the different categories of data to be collected and stored under the directive. Moreover, the period was set between six and 24 months, but the directive did not require the determination of the retention period to be based on objective criteria to ensure that it is limited to what is strictly necessary.[314] Finally, the

Table 13: Data retention periods in existing and planned EU IT systems

Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS II Regulation and** *borders and return proposals*	**EES Regulation**	*ETIAS proposal*	*Interop. proposals (BMS, CIR, MID)*
Applicants for international protection: 10 years, *10 years;* apprehended persons: 18 months, *5 years*	5 years	Alerts for 3 years and then review the need to keep the alert; *max 5 years*	Alerts for 3 years and then review the need to keep the alert; *max 5 years*	Short-term travellers 3 and 5 years for those who overstay	Visa free travellers 5 years	*Data stored in BMS and CIR as long as stored in corresponding IT system. Data stored in MID as long as linked data are stored in two or more corresponding IT systems.*

Note: *Proposed systems and proposed changes in italics.*

Source: *FRA, Fundamental rights and interoperability of information systems (2017)*

313 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105/54 (*Data Retention Directive*).

314 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, paras. 63-64.

directive did not "ensure the irreversible destruction of the data at the end of the data retention period", and therefore it did not ensure a sufficiently high level of protection and security.[315]

Solely setting a time limit for the erasure of the data may not be sufficient to comply with the principle of storage limitation. A periodical examination of whether the purpose of retaining the data no longer exists may be required. In *Tele2*, the CJEU declared that EU law precludes the general and indiscriminate retention of traffic and location data, as very precise conclusions can be drawn about the private lives of the persons whose data are retained. Such a big interference with the right to privacy can be justified for the purposes of fighting serious crime, if it is strictly necessary.[316]

The majority of legal instruments regulating the functioning of the IT systems do not provide for such requirements. There are, however, some exceptions. For instance, the proposed SIS II Regulations on borders (Article 34) and on police (Article 51) have set requirements for periodical examinations of the necessity of retaining the data. Accordingly, the proposals require that Member States who issued an alert to review the need to retain it within five years of its entry into SIS, or to delete it.[317] Member States may decide to set shorter review periods under national law.[318]

Eurodac data should be deleted in advance of the expiry of the foreseen retention time in case the person acquires EU citizenship.[319] In Poland, the National Data Protection Authority intervened to ensure respect for this requirement. To prevent mistakes regarding retention times, changes were made to the functionalities of IT systems to run the list of persons who have acquired citizenship against those listed in Eurodac.[320]

Due to different rules of data retention between the national level and the EU system, the same data that has been deleted from EU IT systems may continue to exist in national level systems. Such data could be exchanged with other Member States through information exchange mechanisms, such as Prüm. Likewise, the dactyloscopic cards can also continue to exist after the entry into the database has been deleted.

It may also happen that an entry ban stored in SIS II, which should have been deleted, has not been done. In Spain, at least 12 such cases happened within one and a half years. A Mexican citizen interviewed by FRA said that he had been issued a 10-year entry ban in 2006, and in 2013, he received a residence permit in Sweden because he was married to a Swedish citizen. He said that he every time he goes through a border check he is questioned for 10–20 minutes because an entry-ban issued by Italy has not been deleted. The cooperation between Sweden and Italy to have the entry ban deleted appears not to have worked well in this case.

5.6. Multiple identities and identity fraud

All legal instruments that regulate EU IT systems directly or indirectly address identity fraud. The VIS and EES Regulations explicitly include the fight against identity fraud among the listed purposes.[321] The existing and planned instruments that regulate SIS II do not include identity fraud among the objectives but clarify how to distinguish between persons with similar characteristics and on how to tackle misused identities.[322] The Eurodac Regulation does not address identity fraud but Recital 12 of the proposed revision indicates that data processing is essential because some people may use "deceptive means to avoid their identification".

The SIRENE Manual distinguishes between not confirmed identity, when there is not sufficient proof of the identity, misused identity, when the identity of another real person is used, and aliases, when an assumed identity used by a person is known under other identities.[323]

The use of biometric identifiers is a valuable method in the fight against document fraud and multiple identities. The biometric data stored in the database links the person to the alphanumeric data entries or, if stored in a chip, to a travel document.

315 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 8 April 2014, para. 68.
316 CJEU, Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016.
317 SIS II borders proposal, Art. 34 (2); SIS II police proposal, Art. 51 (2), SIS II return proposal, Art. 13.
318 SIS II borders proposal, Art. 34 (3);SIS II police proposal, Art. 51 (4), SIS II return proposal, Art. 13.
319 Eurodac Regulation, Art. 13 (1) and Eurodac proposal, Art. 18 (1).
320 Franet, Poland.
321 VIS Regulation, Art. 2 (c); EES Regulation, Art. 6 (1) (i).
322 SIS II Decision, Art. 50-51; SIS II Regulation, Art. 35-36; SIS II police proposal, Art. 58–59; SIS II borders proposal, Art. 41–42, SIS II return proposal, Art. 13.
323 Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Commission Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (SIRENE Manual), OJ 2017 L 231/6.

Table 14: Combating identity fraud in the legal instruments of the IT systems

Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS II Regulation and** *borders proposal*	*SIS II return proposal*	**EES Regulation**	*ETIAS proposal*	*ECRIS-TCN proposal*	*Interop. proposals*
Recital (12)	Objectives (Art. 2 (c))	SIS II Dec, Art. 50–51; *SIS II proposal, Art. 58–59*	SIS II Reg., Art. 35-36; *SIS II borders proposal, Art. 41–42*	*Art. 13*	Objectives (Art. 6 (1)(i))	*no*	*n/a*	Objectives (Art. 2 (2) (b))

Note: *Proposed systems and proposed changes in italics.*
n/a = not applicable.
Source: *FRA, based on existing and proposed legal instruments (2017)*

Biometric identifiers can be subject to fraud. Methods used to create fraudulent biometric identifiers include:

1) **Injuring fingerprints**, as documented in the context of asylum, which is discussed in Chapter 2.

2) '**Spoofing'**, which is to forge a fingertip from materials such as plastic. While this rarely happens, Swedish border guards, for example, have been aware of such cases.

3) Providing a different name and other biodata when registered a second time, resulting in the **same biometric identifier being attached to multiple identities** in the IT system(s). In Sweden, false matches resulting in multiple identities in VIS are relatively frequent. A Swedish DMCP staff estimated to have come across about 20 cases last year.

4) Using **non-genuine supporting documents**. The officers enrolling biometrics have to trust the documents and papers that are used in conjunction with the biometrics, for example, when someone is applying for a visa. Such supporting documents might easily be forged or changed.

The prevailing perception, particularly in the context of SIS II, is that a false match is not a mistaken or confused identity, but a case of identity fraud. Any documents that the individual concerned can present can be helpful to rebut a wrong assumption. Polish border guards interviewed in the field research confirmed that they give more weight to an individual's documents than to data stored in the database. Interoperability can also help an individual rebut a wrong presumption if data stored about them in another database can corroborate their statement, but such mistakes may also lead to the individual being suspected of deceiving the authorities.

Sometimes, however, the use of multiple identities and various names have other reasons. The use of different names may simply be a personal choice without any secondary intention. Weak systems for civil registry in many developing countries enables the use of multiple identities.

At border crossing points, suspected cases of identity fraud are usually sent to a second line check to determine whether the traveller is allowed to enter or not. The explanations provided are checked against multiple databases. If the suspicions are confirmed, criminal procedures are initiated, which could result in an entry ban in SIS II.

If the identity fraud involves the **misuse of another person's identity**, this person is often unaware or only becomes aware when it affects them personally, for example when trying to cross a border. It is, therefore, important for the data subject to receive information about the identity fraud. For example, in Germany, Finland and France, the SIRENE office notifies individuals who have been a victim of identity theft, at least if they are a national resident of the country concerned. One way to address the problem of misused identity in SIS II is to attach the personal data of the person who is a victim of an identity mistake to the alert.[324] This is the procedure used in practice in cases of mistaken identity, as explained in Section 5.2. The SIRENE Manual outlines that the issuing Member State should add further identification particulars to the alert,[325] either on its own initiative or at the request of another Member State.[326] If the victim of identity fraud agrees, information such as names, aliases, physical characteristics, place and date of births, sex, photographs, fingerprints, nationalities and numbers of identity papers and date of issue can be added to the alert. Storing the misidentified victim's fingerprints is considered a safe way to avoid identity mistakes. Information about travel plans could also be

324 SIS II Regulation, Art. 36 and SIS II Decision, Art. 51; SIS II police proposal, Art. 59; SIS II borders proposal, Art. 42; SIS II return proposal, Art. 13.
325 By using the L form, referred to in point 2.12.3 in the 2017 SIRENE Manual.
326 By using the Q form, referred to in point 2.12.1. in the 2017 SIRENE Manual.

added, as the Czech Republic reported to FRA.[327] The data of the person whose identity has been misused must only be available for the purpose of establishing the identity of the person being checked and must in no way be used for any other purpose.

Two European Commission proposals on interoperability to detect multiple identities

On 12 December 2017, the European Commission launched two legislative proposals on interoperability between EU IT systems in the areas of police and judicial cooperation, asylum and migration (COM(2017) 794 final), and borders and visas (COM(2017) 793 final). The proposed provisions are in principle identical. The key objective of these proposals is to ensure the correct identification of persons included in the IT systems, which have been made interoperable.

The proposals include a multiple-identity detector (MID) as a central component of the interoperability solution. The high level working group did not discuss such a component, as the explanatory memorandum also recognises. The other three components of the Commission proposals are a common identity repository (CIR), a shared biometric matching service (BMS) and the European search portal (ESP). CIR and MID are essentially databases, BMS corresponds to AFIS in a national context and ESP is the message broker enabling simultaneous queries in multiple systems.

Functionalities of the different components

Common identity repository (CIR) creates individual files containing data relevant for the identification of a person based on personal data stored in Eurodac, ETIAS, EES, ECRIS-TCN and VIS. Personal data stored in these IT systems include fingerprints, facial image, name, nationality, place of birth, sex and travel documents (travel documents are not included in ECRIS-TCN). SIS II is not included in CIR because of its complex technical architecture, but it is directly included in the interoperability set-up. CIR replaces the central systems concerning the personal data it stores, but keeps the separation of the data according to each IT system (Articles 17 and 18). Article 20 provides for the possibility to access CIR for any national security measure provided by law, which aims to maintain public policy and public security. The legal clarity and foreseeability of such a provision may not be obvious.

The **shared biometric matching service (BMS)** stores biometric templates that it obtains from the individual IT systems and keeps a reference to the systems in question (Article 13).

The **multiple-identify detector (MID)** creates and stores links between data stored to establish multiple identities (Articles 20 and 30–33). MID will store an identity confirmation file, including the links, a reference to the IT systems where the linked identity data originates, and a single identification number allowing the data to be retrieved from the linked files in the respective IT systems (Article 34). The authority that created the data in the respective EU IT system should manually verify the links in MID (Articles 21 and 26). For this verification, the authority will have access to the identity confirmation file stored in MID and the related individual files in CIR and SIS. Recital 42 foresees involving the third-country national in the verification of multiple identities, where possible. The multiple-identity detection and the manual verification allows authorities to access data beyond what is foreseen in the specific legal instruments, such as, for instance, the launch of a multiple-identity detection in CIR and SIS when an entry is created in Eurodac, according to Article 25.

The **European search portal (ESP)** allows authorities to simultaneously conduct searches in Eurodac, EES, ECRIS TCN and VIS, the Europol data and Interpol databases (SLTD and TDAWN), as well as in CIR and MID. This is done by using the templates in BMS for matching purposes, or with alphanumeric data, according to access rights laid down in EU and national law (Articles 6 and 7). Searches in ESP shall take place based upon biometric data, and in case of a hit, access to the individual file is given.

Conclusions

FRA researched confirmed reports of the existence of significant amounts of inaccurate data in SIS II and VIS. The reasons for this are manifold, such as data entry mistakes, technical problems or administrative mistakes. Flawed judicial or administrative decisions may also be the origin. For example, if the authorities have not considered the right to private and family life in the decision for issuing an entry.

Currently, Eurodac only stores the applicant's fingerprint data and no biographic data, other than sex. Mistakes can occur if, for example, the fingerprints are attached to the wrong person or if there are double registrations of the same person. Similar situations have led to mistakes in VIS.

The quality of the enrolled fingerprint is decisive for the reliability of a future match. Long retention periods may affect future matches. Problems with the equipment and the texture of the fingers also affect a future match.

Mistakes in relation to alphanumerical data can have various reasons. Understanding different cultural norms is important to record personal data more accurately. This means understanding naming cultures, dates of birth according to different calendars and different ways of reporting age. It is also important to address transliteration problems.

327 Franet, Czech Republic.

The principle of data accuracy requires the controller to take steps to ensure with reasonable certainty that personal data processed in large-scale IT systems are accurate and up to date. Inaccurate data must be erased or rectified without delay. For SIS II, for example, eu-LISA has a central data quality monitoring tool already in place and other significant measures are underway to support the Member States in ensuring that data are accurate. Nevertheless, increased attention is needed to avoid entering mistakes in the systems, which can negatively affect an individual's fundamental rights.

There is generally a high trust in the reliability of a biometric match. The power of biometrics lies in that it connects a person to alphanumerical data stored in an IT system, which is the basis for decisions affecting the future of that person. However, an individual may have difficulties rebutting a wrong assumption based on a false biometric match or no match. Presently, data quality standards for collecting fingerprints in Eurodac, which mainly holds personal data on asylum applicants, is higher than standards for collecting biometric data in VIS, for which a 'zero failure to enrol initiative' is applied. However, fingerprints are also checked against VIS to see if the person has previously applied for a visa, which may affect the application of the Dublin rules. If IT systems become interoperable, fingerprints collected according to the quality standards of the particular IT system will through a positive match connect the person to alphanumerical data across all IT systems. In developing quality standards, age, disabilities – for instance, a missing hand or finger – and phenotypical characteristics – such as, reflection of light on the skin in the context of facial recognition – need to be considered.

FRA research indicates that the quality of data could be strengthened if the authorities increasingly involved the person concerned in the verification procedures, and if they were open to plausible arguments that the person concerned presents. FRA opinions 17–19 suggest measures to address the serious data quality issues that this research identifies, and the second part of FRA opinion 5 addresses ways to reduce the negative consequences for children in case of a wrong match.

6 The right of access, correction and deletion of own data stored

Charter of Fundamental Rights of the European Union

Article 8 – Protection of personal data

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

The high level of trust in a biometric identifier, combined with the risk of quality issues, highlights the importance of looking into possibilities for the persons concerned to exercise their right to access, and to correction and deletion of data. This chapter analyses the obstacles migrants and asylum seekers face when trying to exercise these rights.

In addition to Article 8 (2) of the EU Charter of Fundamental Rights, the rights of access, correction and deletion of one's own stored data are also included in Articles 15-17 of the GDPR and Articles 16 and 17 of the Police Directive, as well as in Article 8 of the Council of Europe Convention No. 108. The right of access, as guaranteed under Article 15 of the General Data Protection Regulation (GDPR) and Article 15 of the Police Directive, may be restricted, provided the measure is necessary and proportionate for specific reasons. For example, such a reason may entail the need to protect national security or prevent criminal offences.

The right of access, rectification and erasure of data is reflected in all existing and proposed EU IT systems,[328] but it is limited regarding SIS II.[329] The authorities can deny access to SIS II if this is indispensable for the performance of a lawful task in connection with an alert or for the protection of rights and freedoms of third parties.[330]

According to providers of legal counselling and data protection officers interviewed during the field research, complaints concerning the incorrect or unlawful use of data are rare. Data entries are rarely challenged for these reasons.

Procedure for exercising the right of access, correction and deletion

The possibility to exercise the right of access is part of the right to an effective remedy, as protected under Article 13 of the ECHR and Article 47 of the Charter. The CJEU stated that the characteristics of a remedy must be determined in a manner that is consistent with the principle of effective judicial protection.[331] The European Court of Human Rights (ECtHR) stated that a person needs to be able to challenge the data storage or to

328 See: Eurodac Regulation, Art. 29 (4) and (5); Eurodac proposal, Art. 31; EES Regulation, Art. 52; ETIAS proposal, Art. 54; ECRIS-TCN proposal, Art. 23; VIS Regulation, Art. 38; Interoperability proposals, Art. 47.

329 SIS II Regulation, Art. 41; SIS II Decision, Art. 58; SIS II police proposal, Art. 65; SIS II borders proposal, Art. 47; SIS II return proposal, Art. 13.

330 SIS II Regulation, Art. 41 (4); SIS II Decision, Art. 58 (4).

331 CJEU, C-432/05, *Unibet (London) Ltd, Unibet (International) Ltd v. Justitiekanslern*, 13 March 2007, para. 37; C-93/12, *ET Agrokonsulting-04-Velko Stoyanov v. Izpalnitelen direktor na Darzhaven fond 'Zemedelie'–Razplashtatelna agentsia*, 27 June 2013, para. 59; C-562/13, *Centre public d'action sociale d'Ottignies-Louvain-la-Neuve v. Moussa Abdida*, 18 December 2014, para. 45.

refute the truth of the information, including when it is stored for security purposes.[332]

EU law has fostered the use of non-judicial remedies through the right to lodge a complaint with national data protection authorities. Such authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period, including cooperation with a data protection authority in another Member State, if the case involved another state.[333] The person concerned should also have the right to mandate a not-for-profit body, organisation or association to lodge a complaint with a supervisory authority on their behalf.[334] In most EU Member States, a person who wishes to exercise the rights of access, correction and deletion in SIS II should turn to the data controller. This is referred to as direct access. Some EU Member States have a system of indirect access. In this case, the person concerned turns to the national data protection authorities. This is the case in Belgium, Luxemburg and Portugal, among others.[335] Some EU Member States, for example, France and Germany, have a system of both direct as well as indirect access for SIS II.[336]

According to information on 18 EU Member States provided by the VIS Supervisory Coordination Group,[337] 10 EU Member States have a system of direct exercise for exercising the right of access to VIS. Six Member states operate a combination of direct and indirect exercise and two have opted for indirect exercise of data subjects' rights.

As a rule, the persons concerned are informed about the rights of access, correction and deletion at the moment the data are included in the IT systems, although in practice this may not always be effective (See Chapter 1).

Information on how to exercise such rights may also be available on the websites of the controller and the national data protection authority. The Belgian data protection authority, for instance, has leafletws for exercising the right of access to SIS II available in English, French and Dutch. However, in Spain, such information is only available on the website of the national data protection authority, and only in Spanish. In the context of SIS II, Member States provide a summary of the alert, as well as other information, such as who issued the decision, which is the legal basis for entry of the alert.

To support the data subjects, the SIS II Supervision Coordination Group has issued a guide for exercising the right of access, which includes information on formal requirements and addressees of such requests for access.[338] It also includes model letters for how to request access to data and its deletion and correction.

The Schengen visa application form informs the data subjects of their right to obtain access to personal data stored in VIS and to request that inaccurate data relating to them be corrected and that unlawfully processed data be deleted.[339] The Member States complete the information on remedies according to their national law. Information is also available on web pages, in fact sheets at the DMCPS and their service providers, or it is provided orally.

There are no comparable statistics on the exercise of the right of access to data stored in the three existing IT systems.[340] Table 15 shows available data. They illustrate that requests are very few, particularly taking into account that in 2016, some 5 million fingerprints were stored in Eurodac [341]and some 800,000 alerts in SIS II.[342] The VIS rollout only recently finished in 2015.[343] This can explain the low number of requests for VIS.

Similarly, the number of requests for deletion or correction are also very limited (see Table 16)

In spite of formal procedures, persons concerned often lack awareness and understanding of how to exercise the right of access, correction or deletion of data stored in Eurodac, SIS II and VIS. The Supervisory Groups for SIS II and VIS confirm this lack of awareness.

Table 15: Requests for right of access

	Eurodac	SIS II	VIS
2010-2011		6072 (SIS II SCG)	
2014			160 (VIS SCG)[344]
2015	89 (eu-Lisa)		
2016	156 (eu-Lisa)		

Sources: SIS II SCG (2014), p. 5 ; VIS SCG (2016), p. 10 ; eu-LISA (2017a), p. 18

332 ECtHR, *Rotaru v. Romania*, No. 28341/95, 4 May 2000, para. 72.
333 General Data Protection Regulation, Recital 141 and Art. 77.
334 General Data Protection Regulation, Recital 142.
335 SIS II Supervision Coordination Group (SIS II SCG) (2014), p. 6.
336 *Ibid.*
337 VIS Supervision Coordination Group (VIS SCG) (2016), p. 8.
338 European Data Protection Supervisor (EDPS) (2015).
339 Visa Code, Annex I.
340 VIS Supervision Coordination Group (VIS SCG) (2016), p. 10.
341 eu-LISA (2017a), p. 10.
342 eu-LISA (2017d), p. 9.
343 European Commission (2015d).
344 Supervisory Coordination Group, also includes national visas for one Member State.

Table 16: Requests for deletion or correction

	Eurodac	SIS II	VIS
2010-2011		372 (SIS II SCG)	
2014	1987 (Franet)	1538 (Franet)	1 (VIS SCG)

Sources: Questionnaires distributed to Member States via Franet 2015, SIS II SCG (2014), p. 5; VIS SCG (2016), p. 10. Some statistics are also available in the Report by the European Commission on the evaluation of SIS II

The cumbersome nature of the processes also discourage affected people from pursuing them. This is reflected in the relatively low number of persons who actually exercise such rights.

Administrative hurdles and language barriers

Administrative hurdles may prevent the person from exercising the right of access, correction and deletion. In the Czech Republic, for example, a person can exercise their right of access to their own data stored in SIS II only once every six months. Therefore, if the applicant needs any follow-up information, the procedures may become lengthy and involve additional lawyer's fees.

Almost all the competent authorities accept requests in another language than that of the Member State, with only one exception, Poland. In most cases replies are provided in English, accompanied in some cases by a reply in the national language, but Poland and Italy reply in their national languages only, although Italy is considering introducing the possibility to also answer in English, according to the SIS II Controller.

According to a data controller interviewed in Germany, a correction is usually not complicated if evidence, such as a reliable birth certificate or passport is presented. However, some persons may have difficulties in presenting such proof due to the persecution or conflict in the country of origin. An asylum seeker interviewed in Sweden said that she was not in a position to present a Syrian passport, the proof she had been requested to present in order to carry out the correction.

In some cases, another Member State may bear responsibility for the data entry. This Member State is then also responsible for corrections or deletions. This further complicates the exercise of these rights. The situation where another Member State should be approached is more common for SIS II, but may also arise when a person wishes to exercise their rights in relation to Eurodac or VIS. The SIS II Best Practice Catalogue recommends that the person concerned should be able to submit an access request in any Member State, via Member States' consulates and SIRENE Bureaux.[345] According to Article 38 (3) of the VIS Regulation, the authorities must contact the authorities in the Member State responsible within 14 days and they must get back within one month. Such time lines for dealing with requests are absent in Eurodac and in SIS II.

Understanding the procedures

Chapter 2 describes the challenges in providing information. Even if information on the right of access, correction and deletion is provided, the person concerned often has a limited understanding of how to exercise such rights in practice. There is also a certain confusion between possibilities to appeal the underlying decision for the data entry and to exercise the right of access.

Asylum applicants and persons apprehended at the external border, whose data are inserted in **Eurodac** may not be able to absorb data protection related information, due to more serious concerns about their situation. At that point in time, they may not pay attention to the information because of more urgent priorities to consider, related to their need for protection.

In all the countries covered in the field research, a lack of awareness about where to address a request for access, correction or deletion in **SIS II** was acknowledged as a widespread problem among the persons concerned, providers of legal assistance and even authorities. Examples of incomplete requests, where contact data and signature are missing emerged during the research. In the words of the Spanish SIS II controller:

"For a common person, who also is not Spanish and is not fluent in Spanish... it's difficult for them. Even more, if they don't know they are in SIS." (Data controller, male, Spain)

In Spain, public authorities and providers of legal assistance concur that it may often be necessary for the person concerned to engage a lawyer to comply with the procedures for exercising the right of access, deletion and correction. Furthermore, all the required

345 European Commission (2015), *Commission Recommendation of 16.12.2015 establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS II*, C(2015) 9169 final, Brussels, 16 December 2015.

documentation has to be provided by the complainant. However, providers of legal assistance also found it challenging to understand the rules of the system. They often had limited practical knowledge on how to exercise the right of access, correction and deletion.

A frequent reason for refusing a visa is the existence of an entry ban in SIS II. However, as laid down in Annex VI of the Visa Code,[346] the standard form for notifying a negative decision only indicates the Member State that issued the entry ban. It does not mention that the person can exercise their right of access, correction or deletion, and how this could be done. For instance, the VIS controller in Spain often receives information about people challenging their entry bans, although the Ministry of the Interior is responsible.

The interoperability proposals foresee that the right of access, correction and deletion of data can be exercised in relation to the links between data in IT systems stored in MID. This could potentially involve a number of IT systems and Member States within one and the same request.

Few specialised lawyers

Past FRA research has already identified lack of specialised legal professionals and civil society organisations concerned with data protection in many EU Member States. Cases are rare and therefore there is little awareness about this area of law.[347] The same tendencies were also identified in FRA's report on surveillance by intelligence services. The lawyers litigate with pro bono legal support and acknowledge that without pro bono legal support, litigation would not be at all possible.[348]

Similarly, the findings of this research show that not many NGOs and lawyers are specialised in biometrics and laws regulating the use of IT systems and their implications. This is usually not a priority. One provider of legal assistance in Belgium interviewed emphasised the need for civil society organisations to take a more active role regarding access to, correction and deletion of personal data. For each case, the difficulty is estimating whether efforts and gains will be proportionate to the damage done to the person concerned. Challenging a fingerprint match may entail a lot of work and immigration lawyers may be reluctant to take on such cases.

"Going further with a case like that [asylum seeker transferred due to a false positive] would be a pretty big process and take up a lot of time. And clients don't have any way to pay for that. In that case, you do it pro bono and we already do a lot of pro bono work so we have to choose what we do. It could have led to some kind of reprimand or something. But it [a false match] is unusual [...]. So we rather put the time on someone who needs a permit to stay. It would have been extremely interesting, but you choose your fights." (Provider of legal assistance, female, Sweden)

Lawyers may also risk being unsuccessful due to a lack of technical understanding.

"[...] [there are] small chances for us to get it right [prove that point of the client], somehow. To show that it is [a] false match. We are in the hands of the authorities who have the means to control these kinds of things. And it is difficult for us to access the documentation and get our point heard, because we have no one to ask for advice about these things. About the technical things." (Provider of legal assistance, female, Sweden)

At the same time, there are some specialised lawyers. In Ukraine, a provider of legal assistance specialises in assisting migrants who want to ask for information on their personal data in the systems. Usually, these requests concern data registered by Poland in SIS II and individuals want to know whether they have a SIS II entry ban.

Finding out if someone is registered in Eurodac may also be done by exercising the right of access in relation to a national database, if it includes the results of matches against Eurodac. For instance, in Sweden there are frequently requests for accessing data stored in the Central Foreigners' database with the purpose of finding out whether there has been a 'match' or 'no match' against fingerprints stored in Eurodac.

Promising practice

The Swedish Migration Agency foresees to set up a central register care unit that will be responsible for all requests for right of access, correction and deletion in regard to all IT systems of the Migration Agency. Such are the EU IT systems as well as national systems, such as the national system WILMA

Source: FRA interview with Swedish Migration Agency officer, male, Sweden

346 Regulation (EC) No. 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code of Visas (Visa Code), OJ 2009 L 243/1, Annex VI. The Visa Code is currently being revised. See: European Commission (2014), *Proposal for a Regulation of the European Parliament and of the Council on the Union Code on Visas (Visa Code) (recast)*, COM(2014) 164 final, 1 April 2014.
347 FRA (2013), pp. 41–46.
348 FRA (2017a), pp. 118–121.

Restricting the processing of contested data

Pursuant to Article 18 of the GDPR, the data subject can demand that the controller restrict processing contested data for a certain period, allowing the controller to verify the accuracy of the person data. This means that the controller must refrain from using the data pending the verification, including further sharing of the data, in order to ensure that possible false assumption can be rebutted before a decision is made. This is particularly important where the continued use of inaccurate or illegitimately held data could harm the person[349] – for example, by denying entry or imposing detention. Although a derogation from this restriction is possible – for example, for reasons of important public interest – the use of such derogation would need to be assessed in line with the principle of proportionality and strike a fair balance between the rights at stake.

None of existing or proposed legal instruments for the EU IT systems impose the obligation to restrict the processing of personal data when contested, with the exception of the Eurodac proposal. Article 31 (8) provides that the national supervisory authorities of the Member States that transmit or receive the data must notify, upon request, the data subject of their right to request the restriction of processing their data from the controller, in accordance with the GDPR.

6.1. Responding to requests by the data subject

Speedy response

According to EU law, in both criminal and non-criminal proceedings, the reasonableness of the length of proceedings depends on the particular circumstances of the case. Four criteria are used to gauge reasonableness in criminal and non-criminal proceedings: (i) the complexity of the case; (ii) the complainant's conduct; (iii) the conduct of the relevant authorities; (iv) what is at stake for the complainant.[350]

The Eurodac Regulation does not provide any timelines for replying to data subjects' requests for access, correction or deletion of data.[351] Regarding the correction or erasure of data, it states that it "shall be carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures."[352] The existing and the proposed SIS II instruments states that an individual must get an answer "as soon as possible[, but] not later than 60 days from the date on which he applies for access or sooner, if national law so provides".[353] According to the VIS Regulation, a request for exercising the rights of correction and deletion shall be replied to without delay.[354]

Member States have informed the SIS II Supervision Group that requests can take from 10 days to four months to process. Officials interviewed in Germany or Sweden did not consider that there was a risk of delays in processing SIS II requests if only domestic authorities were involved. A more serious reason for delays are lengthy administrate or judicial procedures involved in annulling the decision on the basis of which the entry ban was issued. Providers of legal assistance in Spain noted that the procedure can take up to 1 year in case a court decision is necessary for cancelling the entry ban.

Cooperation with other Member States may result in longer procedures;[355] these could even be stalled. The Swedish national data protection authority has been contacted by individuals who are concerned that alerts in SIS II have not been correctly deleted. This has often concerned information registered in other countries, e.g. in Italy. A provider of legal assistance in Italy also knew of a third-country national who had been granted protection in Italy, but who had an entry ban in SIS II registered by Norway, and still one year after the request for deletion had been forwarded, no answer had been received. Due to the entry ban, the person is stopped at border checks when travelling by air.

Where a system of indirect access is in place, the national data protection authority may have service agreements in place with the relevant data controllers, as for instance in Belgium, to ensure that requests for access to SIS II are dealt within a certain time frame, a maximum of 15 days.

Reason for delays can originate in doubts about the true identity of the person, due to the existence of different aliases or imperfect matches. Clarifying such doubts are necessary in order not to reveal details about the identity of another person.

Delays can also emerge due to heavy case loads. A Swedish lawyer contacted the Greek Council of Refugees for assistance, since the Greek authorities had not responded to requests by the Swedish authorities. These requests were to ascertain whether there were any objections to issuing a residence permit from the Greek side, and if the entry ban could consequently be

349 FRA and ECtHR (2014), pp. 111–112.
350 FRA and ECtHR (2016), pp. 133–148.
351 Eurodac Regulation, Art. 29 (4).
352 Eurodac Regulation, Art. 29 (5).
353 SIS II Regulation, Art. 41 (6) and SIS II Decision, Article 58 (6); SIS II borders proposal, Article 47 (5) and SIS II police proposal, Art. 65 (6), SIS II return proposal, Article 13.
354 VIS Regulation, Art. 38 (4) and (5).
355 SIS II SCG (2014), p. 11.

removed. The delay was caused by the fact that Sweden had requested the deletion of 700 SIS II entries from the system, which took some time to process.[356]

According to the VIS Supervisory report, replying to a request for access, correction or deletion of data can take 30-60 days in practice.[357] As the rollout of VIS has been completed only recently, dealing with the first cases took longer. In Spain, for instance, it took six weeks to deal with the first VIS request, as procedures were not yet in place.

Administrative obstacles

Administrative obstacles may also emerge in dispatching the reply. For example, in Poland, replies are provided in hard copy within 30 days and they can only be dispatched within the country. If the foreigner is outside Poland, there should be an authorised person in Poland who can receive the letter. The controller in Germany noted that acquiring a legal address to send the requested information to can be an obstacle, especially if applicants come from conflict areas.

Communicating the reasoning when the request is denied

In case the requests are denied, the grounds should be communicated to the data subject, according to the SIS II Regulation[358] as well as the VIS Regulation[359]

In case a request for access, information, correction or deletion of data stored in VIS is denied, seven EU Member States reported to FRA that the reasons for refusing the request are not communicated, which may impact possibilities to formulate an appeal.

6.2. Right to an effective remedy

EU data protection law reconfirms that the right to an effective judicial remedy must be provided in relation to decisions by the controller or the processor (Article 79 of the GDPR and Article 54 of the Police Directive) as well as the supervisory authority (Article 78 of the GDPR and Article 53 of the Police Directive). The possibility to lodge an administrative complaint before a supervisory authority (Article 77 of the GDPR and Article 52 of the Police Directive) is not considered an effective remedy under Article 47 of the Charter.

All EU IT systems guarantee the right to bring a complaint before the courts or a competent authority.[360] A right to appeal is also included in the Schengen Borders Code[361] and the Visa Code.[362]

If EU Member States with a system of direct access deny the right of access, correction and deletion, the national data protection authorities function as appeals bodies for rejected SIS II[363] as well as VIS requests.[364] In the context of VIS, in nine EU Member States the appeal should be addressed to the national data protection authority, to the court in one Member State, and in five Member States it could be addressed to either the national data protection authority or the court.[365]

Past FRA research has identified the need to strengthen the independence of data protection authorities. They should have enough resources, such as trained information technology specialists and qualified lawyers.[366] In the field research, an interviewed expert mentions significant limitations in the capacities and abilities of national data protection authorities.

"The data protection authorities are used as a cornerstone of protecting the individual when proposing the measures, but I think they should be supplied with more capacities, and more competences and their role also requires effective cooperation between the national data protection authorities. Furthermore, the supervisory role of data protection authorities is also dependent upon the information that data subjects are provided, and should not replace the right to have access to judicial remedies." (Fundamental rights expert, female)

Access to an effective remedy may not always be available. A legal assistance provider in Poland recalled one case of a person who wanted to request erasure of his personal data stored in a national database, which marked him as an unwanted person on Polish territory. However, there was no applicable procedure

356 Franet.
357 VIS SCG (2016), p. 11.
358 SIS II Regulation, Art. 41 (6); SIS II Decision, Art. 58 (6); SIS II police proposal, Art. 65 (6); SIS II borders proposal, Art. 47 (5); SIS II return, Article 13.
359 VIS Regulation, Art. 38 (5).
360 VIS Regulation, Art. 40 (1); SIS II Regulation, Art. 43 (1); SIS II Decision, Art. 59 (1); SIS II police proposal, Art. 66 (1); SIS II borders proposal, Art. 49 (1); SIS II return proposal, Art. 13; EES Regulation, Art. 54 (1), Eurodac Regulation, Art. 29 (14) and (15).
361 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ 2016 L 77/1, Art. 14 (3).
362 Visa Code, Art. 32 (3).
363 This is the case of the DPAs from Denmark, Estonia, Finland, France (with regard to requests for access under Article 97 and Article 100), Greece, Lithuania, Malta and Slovenia, which have expressly indicated their role of an appeal body, as referred to in SIS II Supervision Coordination Group (SIS II SCG) (2014), p. 7.
364 Nine Member States answered that the data subject could address his or her national DPA for review of the decision of refusal in VIS Supervision Coordination Group (VIS SCG) (2016), p. 12.
365 The remaining Member States did not provide information to the VIS Supervision Group.
366 FRA (2013).

in this specific case, so the organisation decided not to accept taking on judicial representation of the person.

Conclusions

The right of access, correction and deletion of one's own data that is stored is recognised in Article 8 (2) of the Charter as well as EU data protection law. It is also reflected in the specific legal instruments for the IT systems. Efforts to provide information on how to exercise the right of access, correction and deletion of one's own data stored are often insufficient. According to providers of legal counselling and data protection officers interviewed during the field-research, complaints about incorrect or unlawful use of data are rare. Neither are data entries frequently challenged for substantive reasons.

The persons concerned often lack awareness and understanding of how to exercise the right of access, correction or deletion of inaccurate data stored. These difficulties may be exacerbated if IT systems are made interoperable. The cumbersome nature of the processes discourage affected people from initiating procedures. According to FRA research, administrative hurdles and language barriers, difficulties in understanding the procedures and few specialised lawyers are the main reasons behind the low numbers of persons who try to exercise their right of access, correction or deletion of inaccurate data that is stored. The establishment of a 'one-stop-shop procedure' for receiving requests for right of access, correction and deletion of data, like the foreseen central register care unit in Sweden could simplify procedures. In addition, particular programmes focusing the training of lawyers on the right of access, correction and deletion of data stored in EU IT systems could be useful.

A response may be delayed for a number of reasons, due to doubts about the true identity of the person, heavy workloads or administrative obstacles, such as dispatching a written reply if the person lives outside the EU Member State.

7 Best interests of the child – risks and opportunities

Charter of Fundamental Rights of the European Union

Article 24 – The rights of the child

1. Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity.

2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

This chapter analyses how the best interests of the child are affected when children's data, in particular biometric data, are stored in IT systems. It looks at the reliability of biometric matches when data have been collected from young children. It examines challenges in ensuring the right to information and carrying out fingerprinting in a child-friendly manner, and reports on the risk for use of coercive measures against children. Finally, the chapter also explores how IT systems could be optimised for tracking missing or abducted children.

7.1. Best interests of the child in EU law regulating IT systems

Article 24 of the Charter emphasises the best interests of the child as a key principle of all actions that public authorities and private actors take in relation to children. Member States must provide the child with such protection and care as is necessary for the child's well-being and development. The best interests of the child is one of the four core principles of the UN Convention on the Rights of the Child.[367]

The EU data protection acquis provides special protection to children with regard to their personal data.[368] The best interests of the child are also reflected in the Schengen Border Code (SBC), Regulation (EC) No 562/2006. In Article 19 and Annex VII, it requires border guards to pay particular attention to children, whether travelling accompanied or unaccompanied. The Visa Code does not any make references to the best interests of the child. The table below shows that only the Eurodac Regulation and proposal,[369] the EES Regulation[370] and the SIS II police proposal[371] contain a provision explicitly referring to the best interests of the child.

Children are typically included in migration-related databases as a consequence of the decisions of their parents or care takers. As data may be retained in a database for a relatively long time (see Table 17) and used for a number of purposes (see Chapter 3), it may affect decisions that impact on the lives of the children for a long time.

In the case of *S. and Marper*, the ECtHR emphasised that the blanket retention of biometric data by law enforcement authorities of persons not convicted of

367 UN, Convention on the Rights of the Child, 20 November 1989, Art. 3.

368 See the General Data Protection Regulation, particularly Recitals 38 and 58.

369 Eurodac Regulation, Recital 35; Eurodac proposal, Recital 26.

370 EES Regulation, Art. 10 (2).

371 SIS II police proposal, Art. 33 (1) and Recital 23.

Table 17: References to the best interests of the child in EU IT systems instruments.

Eurodac and *Eurodac proposal*	**VIS**	**SIS II**	*SIS II police proposal*	*SIS II return proposal*	*SIS II borders proposal*	**EES Regulation**	*ETIAS proposal*	*ECRIS-TCN proposal*	*Interop. proposals*
yes	no	no	*yes*	*no*	*no*	yes	*no*	*no*	*no*

Note: *Proposed systems and proposed changes in italics.*
Source: *FRA, based on existing and proposed legal instruments (2017)*

a crime may be especially harmful for children, given their special situation and the importance of their development and integration in society.[372]

Unaccompanied children are in a particularly vulnerable situation. In 2016, 63,300 asylum seekers applying for international protection in the Member States were unaccompanied children, according to Eurostat.[373] The majority of these were boys (89 %) and two-thirds were 16 to 17 years old (68 %, or about 43,300 persons), while those aged 14 to 15 years accounted for 21 % (around 13,500 persons) and those aged less than 14 years for 10 % (almost 6,300 persons). More than a third (38 %) of asylum applicants considered to be unaccompanied children in the EU in 2016, were Afghans and about a fifth (19 %) were Syrians.[374]

The impact of data stored in IT systems on the best interests of the child may also be positive as a way to protect both the right of the child to preserve their identity,[375] as well as their right to protection of personal data.[376] In line with the CRC, where a child is deprived of some or all of the elements of their identity, the signatories shall provide appropriate assistance and protection, with a view to quickly re-establishing the identity of the child.[377] In the absence of travel documents, fingerprinting is one of the very few options to identify a person.

A better and more accurate identification is all the more important in the case of children. Where children arrive separate from their families, fingerprints and facial images will allow Member States to follow up a line of inquiry when a fingerprint match indicates that they were present in another Member State. For example, IT systems may help trace missing and abducted children, including child victims of crime. Public officials interviewed during the field research were aware of the duty to protect children, but said that practical guidelines on the use of data on children stored in databases are missing.

372 ECtHR, *S. and Marper v. the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 124-125.
373 Eurostat, 'Asylum applicants considered to be unaccompanied minors', 11 May 2017.
374 *Ibid.*
375 UN, Convention on the Rights of the Child, Art. 8.
376 Charter of Fundamental Rights of the European Union, Art. 8.
377 UN, Convention on the Rights of the Child, Art. 8 (2).

UNHCR experts interviewed for the project were of the opinion that it would be better to focus on creating incentives for children not to travel further as an effort to reduce the number of missing children.

Promising practice

The Irish child protection authorities deal with unaccompanied and separated children before immigration agencies conduct their checks and verifications. This gives them an important role in the protection of children within the immigration processes.

"All unaccompanied or separated children in Ireland come to the child protection authorities first, before they have to deal with the immigration staff... And I know that that's quite unique in Europe, because usually it's the asylum piece first and then we deal with the child protection stuff".

Source: Staff of the Tusla, Child and Family Agency of Ireland

7.2. Collecting and storing biometric data of children

The EU IT systems do not have a harmonised approach regarding the age that biometric identifiers are collected. Fingerprints of children who are at least 14 years old are collected in Eurodac,[378] and according to the proposal for the recast of the Eurodac Regulation,[379] fingerprints and facial images are collected from children when they are at least six years old. In VIS and EES, the minimum age for collecting fingerprints is 12 years,[380] and facial images are collected of all children. There is no age limit for storing fingerprints and facial images in SIS II, which includes missing and abducted children as well as children who have been issued an entry ban. When issuing residence permits, Member States are obliged to collect fingerprints of all children who are at least six years.[381] When issuing passports, Member States

378 Eurodac Regulation, Art. 9 (1).
379 Eurodac Proposal, Art. 2 (2), 10 (1), 13 (1) and 14 (1).
380 Visa Code, Art. 13 (7) (a); EES Regulation, Art. 17 (3).
381 Council Regulation (EC) No. 380/2008/EC of 18 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, OJ 2008 L 115/1, Art. 1 (5).

Table 18: Minimum age for the collection of biometrics from children

Eurodac Regulation and *proposal*	**VIS**	**SIS II Decision and** *police proposal*	**SIS Regulation and** *borders proposal*	*SIS II return proposal*	**EES Regulation**	*ETIAS proposal*	*ECRIS –TCN proposal*	*Interop. proposals (BMS)*
14 years old; *6 years old*	12 years old	*No age limit*	*No age limit*	*No age limit*	12 years old	*n/a*	*n/a*	*As in corresponding IT systems*

Note: *Proposed changes and legislation in Italics.*

Source: *FRA, based on existing and proposed legal instruments (2017)*

must collect fingerprints of those who are at least 12 years old.[382]

At the national level, the age limit for the processing of fingerprints also varies significantly. For example, Belgium and Spain collect fingerprints of unaccompanied children without a lower age limit. Some Belgian officials interviewed in the field research questioned the benefits of this, as fingerprints can change at an early stage. Denmark collects fingerprints of unaccompanied children who are at least six years old. Finland and the United Kingdom also collect fingerprints of children as of six years of age who apply for asylum.[383] The United Kingdom has issued guidance on the respect for the best interests of the child when processing fingerprints of children for asylum purposes.[384] France continued its practice to collect fingerprints of children who were at least six years old for storage in the national database, VISABIO, and the minimum age for collecting fingerprints in VIS was raised from six to twelve years of age.[385] The French Data Protection Authority insisted on the deletion of unlawfully collected data.[386]

Reliability of biometric data

Taking biometrics of young children impacts on the quality and reliability of a future match. Experts interviewed expressed concerns about the reliability of a match when a long period has passed since the fingerprint was captured. Present technologies for fingerprinting and facial recognition guarantee a reliable match when then child was at least six years old when the biometrics were taken and the match happened within a time frame of five years.[387] Scientific research does not allow for conclusions on the reliability of a match when more than five years have passed. In the context of Eurodac, given that the fingerprints and facial image of children applying for international protection may remain in the database up to ten years, the margin of error when comparing children's fingerprints may be higher than for adults.

To improve accuracy, the industry is developing fingerprinting equipment with so-called juvenile features. Such equipment uses zooming techniques to take into account the physical development of a child, by making it possible to align a fingerprint of a child that was enrolled when the child was six years of age, to the fingerprint taken for matching purposes when the child was 12 years of age.

Regular retaking of fingerprints would ensure reliability, but may represent a disproportionate interference with the privacy of the child. In addition, the physical conditions in which fingerprints are captured and matched may affect the quality of children's biometrics differently to adults. As observed, for example, at Frankfurt airport, children may have difficulties in reaching the regular border control desks, which are elevated, and therefore be in an uncomfortable position, which can affect the matching quality.

Reliability of alphanumerical data

The EU IT systems will store an increasing amount of alphanumeric data, also about children.[388] This is in particular the case for Eurodac, which is expected to

382 Regulation (EC) No. 444/2009 of the European parliament and of the Council of 28 May 2008 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ 2009 L 142/1, Art. 1 (1).

383 Franet.

384 United Kingdom, UK Visas and Immigration Department (2013), *Asylum Instruction: Fingerprinting,* para. 1.2 and para. 2.2; United Kingdom, Borders Citizenship and Immigration Act 2009, section 55.

385 France, Code de l' entrée et du séjour des étrangers et du droit d'asile (*Code on the entry and stay of aliens and on the right of asylum*), Article R611-9 ; Décret n° 2010-645 du 10 juin 2010 relatif au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa (*Decree No 2010-645 of 10 June 2010 on the automated processing of personal data relating to aliens applying for the issuance of a visa*), Art. 3.

386 France, CNIL (*La Commission nationale de l'informatique et des libertés*), Délibération No. 2012-293 of 13 September 2012.

387 Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen (2013); FRA (2016), *The impact of the proposal for a revised Eurodac Regulation on fundamental rights. Opinion of the European Union Agency for Fundamental Rights,* FRA Opinion - 6/2016 [Eurodac], Vienna, 22 December 2016, p. 26.; Chaudhary, A., Sahni, S. and Saxena, S. (2014), pp. 82–88; Ramanathan, N., Chellappa, R., Biswas, S. (2009), pp. 131–144.

388 SIS II police proposal added additional categorises, such as address of the victim, victim's father and mother name, see Art. 59.

include name, nationality, place and date of birth, and travel document details in the future.[389] The reliability of alphanumeric data is a concern if the authorities make mistakes when including the children's information, or if the children provide incomplete or wrong information, which may be a particular risk in the case of unaccompanied children of a young age.

Age determination

The age of asylum seekers and beneficiaries of international protection is a decisive factor in determining which procedural safeguards apply. For example, according to Article 14 of the Eurodac Regulation, fingerprints are collected from children who are at least 14 years old and from children who are at least six years old according to Article 13 of the Eurodac proposal. Whether a child's data are included in Eurodac is of crucial importance to the application of the Dublin rules. However, some asylum-seeking children either do not know their own age, do not have documents to prove it or deliberately conceal their correct age. This behaviour is usually a way to either be considered younger in order to obtain particular protection for children or to be considered an adult to be placed in open accommodation with less supervision, as observed with Nigerian girls arriving in Sicily.

In the context of Eurodac, in case the authorities doubt the correctness of the claimed age, they can assess the age of the applicant. Age assessment procedures are not standardised across the European Union.[390] Various criteria are used, ranging from a visual estimation to medical examinations of wrists, teeth and/or genitals, possibly involving x-rays.[391] Some of these methods have been heavily criticised from a fundamental rights perspective as not reliable methods for making precise estimates.[392] Article 17 (5) of the Asylum Procedures Directive defines minimum safeguards for a medical examination of unaccompanied children. However, the grounds, timing and methods vary in practice among the Member States.[393]

Reference materials: Promoting common approaches for age assessment

In 2018, the European Asylum Support Office issued guidelines highlighting the key points which need to be taken into account when assessing the age of an asylum applicant. This follows a first publication mapping age assessment practices in Member States, which has been available since 2013.

The 2018 guide is a tool that provides concrete recommendations to address practical challenges. For example, the guide addresses the need for a best interests assessment in the context of age, to determine whether an age assessment is necessary or not, and if so, what methods would be the most convenient for that specific child. It also includes a checklist for best interests assessments, an overview of practices in Member States and an overview of national legal instruments and jurisprudence.

In line with EU law and international standards, the guide recommends the use of least intrusive methods, the need for the child's or guardian's informed consent, and the benefit of the doubt in cases where Member States still have doubts after the age assessment has been conducted.

Sources: For the forthcoming 2018 EASO guidelines, see the EASO Practical Tools webpage. See also, EASO (2013), Age assessment practice in Europe, Luxembourg, Publications Office.

Sometimes the authorities doubt the reliability of identification documents.

"Even if they have an identification document on them, and this is the interesting part, actually from Afghanistan they always have a 'tazkiras', an ID card, which is never trusted. So they are systematically subjected to these tests." (Provider of legal assistance, female, Belgium)

Age assessment is often considered a time consuming and complicated process. Therefore, according to officers interviewed in Germany, the stated age is usually accepted, except in obvious cases. A medical assessment is done if the person looks older than 18 years, but declares to be a minor. Practices appear to differ – a police officer interviewed said that if based on the 'four eyes principle' it can be estimated that the applicant is older than 14 years. A note of this is made and then the child is fingerprinted.

Providers of legal assistance in Sweden expressed concern that the Swedish Migration Agency has the tendency to pressurise a child to voluntarily provide fingerprints even if the child claims to be less than 14 years old, with the threat that the agency will in any case consider the child to be 14 years of age.

389 Eurodac proposal, Art. 12, 13 (2), and 14 (2).
390 FRA (2010c), p. 53.
391 For a recent overview of existing practices, see European Asylum Support Office (EASO) (2013).
392 Benon, J. and Williams, J. (2008) p. 821.
393 European Commission (2017b), p. 38.

"It is very clear that there is a strong force at the Migration Agency that the person who claims to be thirteen should take fingerprints. Children are pressurised into having their fingerprints taken, or else the Agency threatens to assess the age of the applicant as 14. I have been involved in several cases where there is a very unclear practice […]. The Migration Agency should make an objective evaluation; 'do we want to assess the person as 14, and then take fingerprints? But it seems like they do the opposite. If you say that you are 13, they assume it is because you don't want to leave your fingerprints. Then they threaten to assess you as older if you don't agree to leave the fingerprints."
(Provider of legal assistance, female, Sweden)

Other stakeholders in Sweden said the authorities relied on the age registered by another country, without listening to the arguments of the child why their age was registered differently in the other Member State. Information about the age of a child stored in IT systems may also be wrong, as an example from Finland illustrates. A boy, who was clearly a child, according to his lawyer, was denied an age assessment because a consultation in VIS showed that he had previously applied for a visa with false documentation of a man aged 30.[394]

7.3. Informing children in an understandable language

The right to information is a precondition for the child to exercise their right to be heard in judicial and administrative proceedings that affect them, which is protected by Article 12 of the CRC and Article 24 (1) of the Charter on Fundamental Rights. According to Article 12 of the GDPR, the controller must take appropriate measures to provide information on the data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. FRA underlined that it is essential to provide adequate, easy to understand, child-friendly information to separated, asylum-seeking children.[395]

Table 19 shows that a requirement to provide age-appropriate information is only included in the Eurodac Regulation and Eurodac proposal.[396] The Eurodac proposal mentions the importance of providing age-appropriate information during the fingerprinting and facial image procedure.[397]

Any special ways for providing information to children were not observed during the non-participant observations at the DMCPs.

The proposal for a revision of the Dublin Regulation foresees the adoption of a specific leaflet for unaccompanied children.[398] The Dublin criteria for deciding which Member State will be responsible for the asylum application includes a fingerprint match against those in Eurodac.

In practice, children are not always informed when fingerprinting is carried out. As an illustration, some of the unaccompanied children interviewed in Italy and Spain during the field research said that they had not been properly informed. Unaccompanied children having arrived in Sicily said that at the moment of arrival, the police officers did not provide any information about the fingerprinting process, or its purpose, neither orally nor in writing. They only asked for the name, date and place of birth, and for the children to provide their fingerprints. In other cases, information may not be complete. Concerning the fingerprinting process during apprehension, a Polish police officer indicated that children receive an explanation about the fact that fingerprints are needed for identification purposes in case something happens to them.

Table 19: Provision of information to children in an age-appropriate manner

Eurodac Regulation and *proposal*	**VIS**	**SIS II: Decision** and *police proposal*	**SIS II Regulation** and *borders proposal*	*SIS II return proposal*	**EES Regulation**	*ETIAS proposal*	*ECRIS –TCN proposal*	*Interop. proposals*
yes	no	*no*	*no*	*no*	no	*no*	*no*	*no*

Note: *Proposed changes and legislation in italics.*
Source: *FRA, based on existing and proposed legal instruments (2017)*

394 Finland, Refugee Advice Centre (*Pakolaisneuvonta RY*), Single children with asymlum procedure: Challenges (*Yksintulleet lapset turvapaikkamenettelyssä: Haasteet*).

395 FRA (2010c).
396 Eurodac Regulation, Art. 29 (2); Eurodac proposal, Art. 2 (2) and Art. 30 (2).
397 Eurodac proposal, Art. 2 (2).
398 European Commission (2016), Proposal for a Regulation of The European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless party (recast), COM(2016) 270 final, Brussels, 4 May 2016, Recital 47.

In other situations, the information is provided, but not understood. An unaccompanied child explained that he had just arrived in Spain. He received written information in Arabic, but cannot recall what it said. He did not understand why officers had taken his fingerprints and was not at all aware of what was going on. He feared he was being expelled, when in fact he was being transferred to an institutional care facility.

"I was afraid when they took me to the rooms downstairs to get fingerprinted. I thought that they were going to expel me – and that would be it. I entered, they took photos and fingerprints, and they put me into the car. I thought that I was taken to the airport." (Regular migrant – other, Moroccan male, Spain)

Some countries covered in the field research have made efforts to convey the information about Eurodac in a child friendly manner. In Belgium, there is a specialised unit responsible for relaying information to children in a way adapted to them, through comic books or visual aids. Germany and Sweden[399] have leaflets for asylum-seeking children that also inform about why fingerprints are collected and the process.

If parents accompany a child, the authorities sometimes rely on them to provide information to their child about the need to provide fingerprints. An officer interviewed in Germany explained that a youth worker or child's parents are always requested to be present during the identification of children. When apprehending migrants in an irregular situation in Belgium, the authorities rely on the parents to provide information, as noted during non-participatory observations and interviews with officials. This is also the practice when officials fingerprint children to issue residence permits, according to a public official interviewed in Italy. The same was noted at the Zeebrugge seaport, Terespol land border and Frankfurt and Arlanda airports, where children over 12 years were checked against VIS, or visas were issued at the borders.

7.4. Fingerprinting in a child-friendly manner

According to the Eurodac proposal, fingerprints and facial images should be collected in a child-friendly and child-sensitive manner.[400] Informal child-friendly practices for taking fingerprints are in place, although specific guidelines on fingerprinting children are rare.

Experts repeatedly underlined the need for specific safeguards when taking biometric identifiers of children and for providing information to them in a manner adapted to their needs. People working with the collection and storage of biometrics should be trained in children´s rights, according to an expert interviewed.

Indications of trafficking in human beings or vulnerability can be identified during the fingerprinting process, for example, if an accompanying adult behaves suspiciously and does not allow the child to be fingerprinted, according to UNHCR experts interviewed. They were also of the view that fingerprinting unaccompanied children should be taken in the presence of a guardian.

During the field research, it was observed that police and border guards try to carry out fingerprinting in a child-friendly manner. In Sweden, the officers collecting fingerprints of asylum-seeking children try to dedicate extra time to children and they try to establish trust and create an atmosphere where children can feel safe. If they have reason to suspect that a child may have been mistreated, they report this to the social services. A staff member of a Swedish diplomatic or consular mission said that they explain more to children to help them understand that they need their fingerprints for their files and that it is not dangerous.

At the Fiumicino airport in Rome, the officers try to make the fingerprinting process fun, as noted during the non-participatory observation. A Belgian asylum officer explained that, in general, they pretend it is a game for the children and that most of the time they enjoy "seeing their little hand on the big screen suddenly enlarged 20 times".

Many EU Member States have particular safeguards for fingerprinting unaccompanied children. In Estonia, officials can only fingerprint unaccompanied children under the age of 15 years in the presence of a legal or assigned representative,[401] in Germany sometimes in the presence of a supervisor, and in Spain by a specialised group.[402]

Officials should be trained specifically for fingerprinting children. The child should be accompanied by a responsible adult, guardian or representative. The methods for collecting fingerprints should be age appropriate. This is particularly important for unaccompanied children.

399 Sweden, Migration Agency (*Migrationsverket*), This is how it works to apply: For you who will apply for asylum without a parent or other care taker (*Så fungerar det att söka: till dig som söker asylum utan förälder eller annan vårdnadshavare*), November 2017.

400 Eurodac proposal, Art. 2 (2).

401 Estonia, Visa Registry (*Viisaregistri pidamise põhimäärus*), Government Regulation No. 86 of 17.06.2010, Art. 3.

402 Spain, Database of Unaccompanied Foreign Minors (*Menores Extranjeros No Acompañados*).

7.5. Use of coercive measures

The EURODAC proposal sets out that vulnerable persons and children should not be coerced into giving their fingerprints or facial image, except in duly justified circumstances that are permitted under national law.[403] However, the proposal does not provide a specification of what qualifies as duly justified circumstances. It is hard to image when the use of force against children would be permitted. Children should not be coerced into giving fingerprints, nor should other people who are considered vulnerable.[404] Several United Nations agencies and civil society organisations have underlined that coercive measures in migration related procedures violate children's rights and urged EU institutions to exempt all children, regardless of their age, from all forms of coercive measures when obtaining their fingerprints and facial images for Eurodac.[405]

In Berlin, instances when police detained unaccompanied children for up to six hours for fingerprinting and strip searches have been reported.[406] The FRA field researches came across situations concerning children, which involved some degree of coercive measures or threats of such measures. A German police officer pointed out that if an individual refuses to provide fingerprints, it can lead to longer detention periods, including for children, who are detained until one of the youth offices takes over. In Italy, lawyers and NGOs who collected migrants' experiences, mentioned instances that ended with coercion and threats about the potential negative consequences that could derive from their refusal. This concerned both accompanied and unaccompanied children. In Spain, FRA field researchers interviewed an unaccompanied child, who described the police's attitude as aggressive and violent when they were taking fingerprints. He claimed that he was shouted at and that a police officer held his chin forcefully, while another police officer forcefully held his wrist. The interviewee described this episode as a very unpleasant experience and – throughout the interview – reiterated that he hoped his interview would be useful in preventing this from happening to anyone else in the future. In Belgium, there have been instances when officers did not consider 15- to 17-year-olds to be children, according to providers of legal assistance.

The Fundamental rights experts consulted for this research were aware of incidents where officers detained children with damaged fingerprints. The risk of re-traumatisation for children is particularly apparent if coercive measures are used.

7.6. Missing and abducted children

IT systems could help trace missing children and prevent child abductions. Children may have been reported as missing to the police or may be at risk of being unlawfully removed and therefore abducted. SIS II alerts for missing persons are used to trace missing and abducted children. Out of 97,117 missing persons registered in SIS II in 2016, 65,370 were children.[407] The Italian Ministry of Welfare declared that 62 % of the children that arrived between January and May 2015 went missing.[408] Child abductions are typically carried out by one of the parents or for child trafficking purposes, according to public officials interviewed during the field-research.

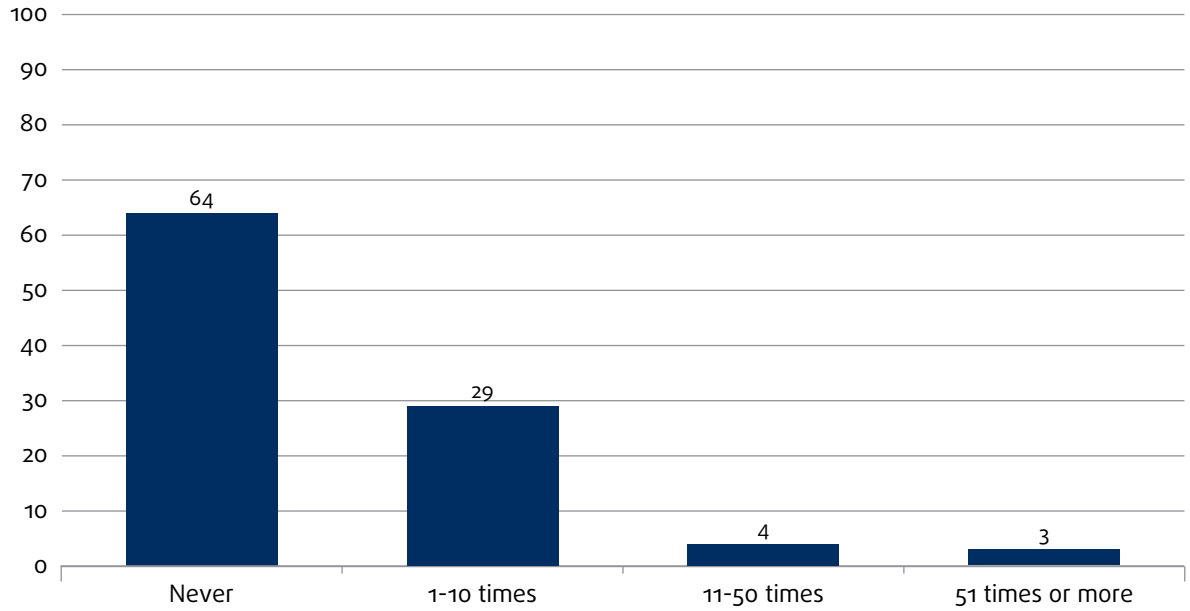
To optimise the use of SIS II for tracing missing and abducted children, the current proposals introduce:

- A new category of missing persons – children at risk of parental abduction;[409]
- The obligation to indicate the type of missing or vulnerable person, such a person could be an unaccompanied child;[410]
- If fingerprints, palm prints, facial image or photographs are not available, DNA profiles can be added to the alert.[411] Direct ascendants, descendants or siblings may consent to include their DNA profiles to the alert to facilitate the search for the missing person.[412]

The reasons that children avoid being registered or run away from reception centres, becoming classified as missing, are multiple. They include, for example, a lack of trust in family reunification under the Dublin regulation, the fear of being prevented from reaching their intended destinations, as well as lengthy processing times for their applications.[413] A German provider of legal assistance who was interviewed expressed a word of caution regarding statistics on missing children. In some cases, children who are identified at the border are counted as missing in the statistics due to the lack of later registration in databases for asylum and residence. They may just have travelled on to the intended destination where they have relatives or family.

403 Eurodac proposal, Recital 30.
404 FRA (2015b), p. 9.
405 UNHCR, UNICEF, OHCHR Regional Office for Europe et al. (2018), Joint statement: Coercion of children to obtain fingerprints and facial images is never acceptable, 28 February 2018.
406 Germany, Berlin State Assembly (*Abgeordnetenhaus Berlin*) (2013).
407 eu-LISA (2017d), p. 10.
408 Missing Children Europe (2016), p. 26.
409 SIS II police proposal, Art. 32 (2) (c) and (4).
410 SIS II police proposal, Art. 20 (3) (r) and 32 (5).
411 SIS II police proposal, Art. 22 (1) (b).
412 SIS II police proposal, Art. 22 (1) (b).
413 UN Children's Fund (UNICEF) (2016).

Figure 18: Estimated number of times border guards come across an SIS II alert of missing persons when dealing with children (%)



Note: *The results are based on the survey question "How often have you come across a child (minor) at this border who had a SIS II alert as a missing person? Please provide an estimated number of times when this has happened in the last 12 months...." (n = 142).*

Source: *FRA Biometrics project, BCP survey, 2016*

FRA's small-scale survey at BCPs shows that children reported as missing are frequently encountered at border crossing points. In this survey, border guards were specifically asked how often they have encountered, during the last 12 months, a case of a child with an alert in SIS II as a missing person. Almost a third of the border guards (29 %) experienced this between 1 and 10 times over the 12-month period. Some respondents even indicated that it happened more than 10 times or even more than 50 times in the past year.

The prevailing opinion among public officials and experts was that the use of biometrics and other data stored in databases could contribute to better tracing of missing and abducted children. According to border and police officers, SIS II alerts on missing persons have been useful in finding missing or abducted children. During the non-participant observations conducted at Arlanda airport, the data of two children matched those of a missing person. On both occasions, the first line officer double-checked the child's identity to make sure that it was not the same person. In one of the instances the child was travelling alone with an older sibling (both under 18) and the first line officer made a phone call to check their reference persons.

Several public officials and experts interviewed would expand access rights to more categories of staff to facilitate the identification of missing or abducted children. A few were of the opinion that present rules on access are enough and access should be kept limited.

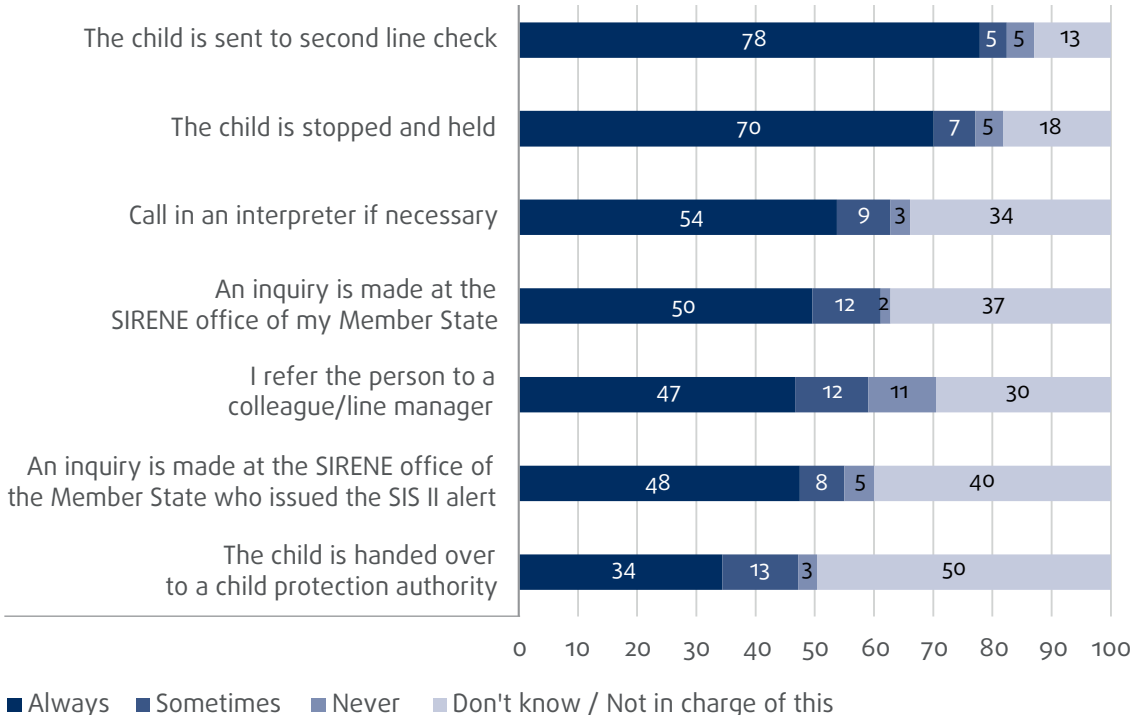
When a child is registered as missing in SIS II, it is always sent to second line check according to 78 % of the border guards surveyed. Over half of border guards said that at least sometimes an inquiry is made at the SIRENE office, either in the border guard's Member State (62 % at least sometimes) or in the Member State that issued the SIS II alert (56 % at least sometimes). About one third (34 %) of the border guards said that the child is always handed over to the child protection authority.[414]

An officer may suspect that a child may be a victim of child abduction even if it has not been issued a SIS II alert. The best interests of the child are a primary consideration in all actions concerning children.[415] In the small-scale survey at DMCPs and their service providers, staff were asked if special measures were taken in suspected cases of child abduction. Only less than one fifth (18 %) of the DMCP officers and 5 % of the staff of service providers said that they sometimes take such measures. As many as one third of DMCP officers and two thirds of the staff of service providers said that such measures are never taken. This could reflect the absence of measures, but also possibly a low occurrence of situations of suspected child abduction.

414 A large percentage of border guards indicate not being in charge of this or not knowing what happens.

415 UN, Convention on the Rights of the Child, Art. 3 (1).

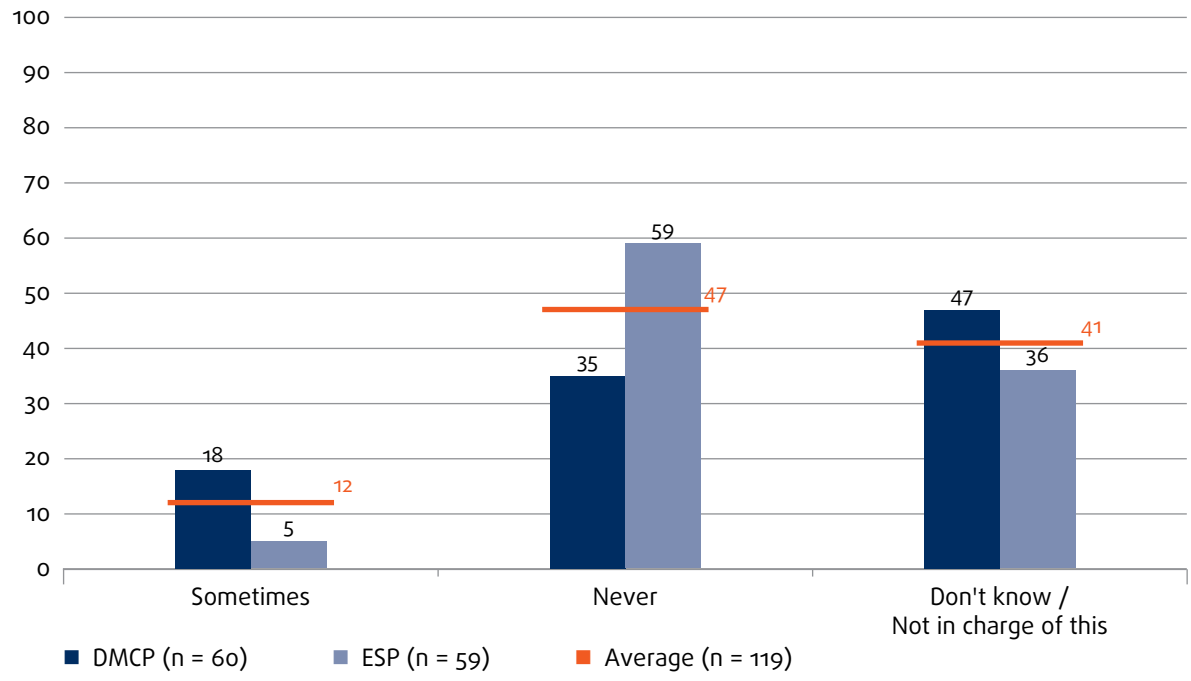
Figure 19: Actions taken if a child has a SIS II alert for missing persons (%)



Note: *The number of respondents varies for the replies, ranging from 105 to 131 persons. The results are based on the survey question "What do you do if a child (minor) has a SIS II alert for missing persons? Please mark the cell that applies for each of the rows in the table below."*

Source: *FRA Biometrics project, BCP survey, 2016*

Figure 20: Taking specific measures if suspecting a possible case of child abduction during the visa application procedure (%)



Note: *The results are based on the survey question "And for the following groups, are specific measures taken and how often: Suspected cases of child abduction?"*

Source: *"FRA Biometrics project, DMCP officers and external service providers (ESP) survey", 2016*

According to desk research undertaken by FRA in 2015, most Member States systematically create SIS II alerts if a child is reported as missing. In some Member States such as Belgium, Denmark, Lithuania, and Spain,[416] the police issue an alert if they have specific information which indicates that the child could be abroad.

However, police authorities can only register children who have been reported to them as missing by the responsible bodies, such as reception centres for asylum seekers. Tracing missing children presupposes keeping track to conclude that a child has disappeared. In practice, this is not regularly done, due to unclear reporting responsibilities at national level, weak guardianship systems and other reasons. In its legal opinion on Eurodac, FRA said that there should be an obligation for Member States to record all children (under the age of 18 years) who have disappeared from reception facilities as missing persons in SIS II.[417] The European Commission has also highlighted the need to raise awareness on the issue of missing children and to establish specific procedures and protocols to systematically report unaccompanied minors going missing.[418]

Spain has a database for unaccompanied foreign minors: MENA – Menores Extranjeros No Acompañados. Spanish providers of legal assistance suggested the establishment of a similar database at the European level,.

Experts interviewed suggested comparing matches of national alerts on missing children with IT system storing biometrics. This could be done through a particular search interface which limits access to police officers investigating cases of missing or abducted children. This means that if a child believed to have been reported as missing is found, interoperability between Eurodac and SIS II could support the identification of the child. The authorities responsible for identifying missing children would conduct a fingerprint search through a single search interface (as a possible interoperability solution) which would provide access to both SIS II and Eurodac (on a hit/no hit basis only).[419]

Regulation 2017/458 introduced the requirement to check all travellers at entry as well as exit against SIS II, both third-country nationals as well as EU citizens.[420]

Checks at exit could contribute to finding missing children. Missing or abducted children are often found when exiting the country, according to a Swedish officer interviewed in the field research. However, typically biometric checks are done if there are doubts concerning the authenticity of the travel document, and abducted children with false documents may not necessarily be detected if biometrics are not checked.

Conclusions

Article 24 of the Charter emphasises that the child's best interests must be a primary consideration in all actions that public authorities and private actors take in relation to children. EU Member States must provide the child such protection and care as is necessary for the child's well-being and development.

The EU IT systems do not have a harmonised approach as to when biometric identifiers are collected. Taking young children's biometrics affects the quality and reliability of a future match. Fingerprints evolve as the child grows, which may be a particular concern if data are retained for long periods. To limit the risks of false matches due to the fact that too long a time has passed since the data were collected, the reliability could be strengthened through further checks and verifications against other available data, and by being open to arguments presented by the child.

As with adults, the reliability of alphanumeric data is a concern if the authorities make mistakes when including information about children. The data are open to error if children themselves provide incomplete or wrong information, which may be a particular risk in the case of unaccompanied children of a young age.

The right to information is a precondition for the child to exercise his or her right to be heard in judicial and administrative proceedings which affect them, protected by the Convention on the Rights of the Child and the Charter. Field research showed that in practice, children are not always informed when fingerprinting is carried out. In other situations, the information is provided, but not understood. Some countries covered in the field-research have made efforts to convey the information about Eurodac in a child friendly manner, through comic books, visual aids or leaflets for asylum seeking children.

It is hard to imagine when the use of force against children or detention would be permitted to coerce them to give fingerprints. An adult person should be able to explain the rationale and reason for collecting fingerprints from a child and should refrain from coercive measures. Adults should aim to build up a relationship of trust with children arriving in the EU so that they start

416 Belgium, Ministerial Directive (Col 9/2002) on missing persons, Point 2.2.4; Franet, Denmark, Ministry of Interior; Lithuania, Order of 16 July 2003 of the Minister of Interior of the Republic of Lithuania; Franet, Spain, Ministry of Interior.
417 FRA (2016a), p. 26.
418 European Commission (2017c).
419 FRA (2016a), pp.24–25; FRA (2017b), pp. 36–39.
420 Regulation (EU) 2017/458 of the European Parliament and of the Council of 15 March 2017 amending Regulation (EU) 2016/399 as regards the reinforcement of checks against relevant databases at external borders, OJ 2017 L 74/1, Art. 1.

relying on official information. This could be achieved by explaining, for example, the rationale as to why fingerprints are collected. During the field research it was observed that police and border guards try to carry out fingerprinting in a child-friendly manner. It means dedicating extra time for children to establish trust and create an atmosphere where children can feel safe. Any suspicion that a child may have been mistreated is reported to the social services. EU Member States should ensure children are fingerprinted in a child-friendly and child and gender-sensitive manner, in line with the best interests of the child.

IT systems could help trace missing children and in prevent child abductions. According to desk research undertaken by FRA in 2015, most Member States systematically create SIS II alerts if a child is reported as missing, but reception centres do not necessarily report this fact to the police. The reasons that children avoid being registered or go missing, are multiple; including, for example, lack of trust in family reunification under the Dublin regulation; fear of being prevented from reaching their intended destinations; and lengthy processing times for their applications. Some of those missing may be subject to abuse and exploitation, including trafficking in human beings. The prevailing opinion among officers and experts interviewed in the field research was that the use of biometrics and other data stored in databases could contribute to better tracing missing and abducted children. According to most border guards surveyed, when it is discovered that a child is registered as missing in SIS II, that child is always sent for a second line check at the border.

Tracing missing children presupposes systematic recording of missing children in SIS II, alongside functioning referral mechanisms and tailor-made training for practitioners who may encounter children in need of protection. In practice, this is not done regularly. Interoperability between EU IT systems may also bring new opportunities to trace missing and abducted children, for instance, by making biometric data available to the officer accessing the system.

FRA opinion 5 recommends fingerprinting children in a child-friendly and child-sensitive manner. For suggestions on how to optimise the use of IT systems to trace missing children, see FRA opinion 6.

Annex I: Research methodology

The EU Agency for Fundamental Rights (FRA) has been analysing the fundamental rights implications of processing biometric data in large-scale EU IT systems since 2015, when the Agency started working on a dedicated biometrics project.[421] The research builds on different research methods and data collection, combining social and legal research.

Mapping of procedures

Legal research included mapping practices and procedures related to the use of databases in all EU Member States. FRA's research network Franet carried out this mapping during the first half of 2015. Researchers reviewed publicly available information on the IT systems and interviewed relevant authorities responsible for the data processing. The authorities received a questionnaire and were asked to provide information on procedures and rules governing the use of databases at national level. In addition, desk research assessed the extent to which civil society is active and aware of the issues in this field.

Field research

The field research collected the views of practitioners and rights holders in six selected EU Member States: Belgium, Germany, Italy, Poland, Spain and Sweden – and at a limited number of diplomatic missions and consular posts (DMCPs) of these Member States in third countries.[422] The countries were selected based on the different migration challenges they face, their types of borders (mainly land and air borders) and their location to ensure a geographical balance. The fieldwork included qualitative interviews, small-scale surveys and non-participant observations. Eticas Research and Consulting, and the Spanish Research Council (CSIC), supported by a network of sub-contracted partners in the six Member States, carried out the fieldwork research on behalf of FRA between January and December 2016. The project coordination was carried out by Dr Gemma G. Clavell and Dr Mariano M. Zamorano on behalf of Eticas and Dr Amparo González and Dr Inmaculada Serrano on behalf of CSIC. The research teams in the EU Member States included:

- In *Belgium*: Dr Paul de Hert, Amy Weatherburn, Jozefien van Caeneghem, Marijke de Pauw, Ines Gallala, Ramon Lathouwers
- In *Germany*: Dr Raphael Bossong, Joanna Bronowicka, Stephanie Horth, Vinzenz Kratzer and Anne Koch.
- In *Italy*: Dr Marco Benvenuti, Francesca Zampagni, Marta Capesciotti, Silvia Morra
- In *Poland*: Monika Szulecka, Karolina Misiewicz, Ignacy Jan Jóźwiak, Kamila Zacharuk
- In *Spain*: Dr Amparo González, Dr Inmaculada Serrano, Ricardo Boscar, José María Zavala Pérez, Lilia Mykolayiv and Leyre Benito Otazu
- In *Sweden*: Dr Anna Bredström, Karin Krifors and Nedzad Mesic

Dr Noleen Gertz, Dr Renata Ávila and Danilo Krivokapic contributed with expertise. Local researchers supported the field research at DMCPs in Algeria, Nigeria, Thailand and Ukraine, for language reasons in particular.

Qualitative interviews

Qualitative interviews were conducted with three different target groups, including practitioners, rights holders, and experts. Practitioners included persons whose work involves using Eurodac, SIS II or VIS. These are data controllers, national data protection authorities, border guards, police, asylum authorities, immigration authorities and staff responsible for processing visa applications at the DMCPs, and their service providers. This group also included providers of legal assistance (mainly lawyers and some NGOs). In addition, qualitative interviews were held with experts on fundamental rights, biometrics and information technology.

Right holders included asylum seekers, visa applicants, migrants in a regular or irregular situation (including both those apprehended at the border as well as inside the territory of a Member State) and others who experienced problems related to the use or corrections of data contained in VIS, Eurodac or SIS II were included in the group 'other'. The interviews with rights holders aimed to collect the views and experiences of third-country nationals whose fundamental rights had been affected in connection to their personal data inserted and/or checked against these IT systems. To collect the views and perspectives of right holders, respondents were selected following quotas on age, gender and nationality by contacting associations dealing with these groups. Fieldwork was conducted between February and September 2016.

421 FRA (2015a).

422 FRA notified DG Justice about the planned research at DMCPs in third countries and got permission to conduct the research, which took place outside the geographical scope of the EU.

Before starting the fieldwork, all interviewers received training at a national level. With the consent of the interviewee, the interviews were recorded; otherwise, the interviewer took notes. FRA developed the interview questions, which were made available in English and in the national languages of the Member States covered. The interviews with rights holders included seven children in Italy, Spain and Sweden aged 16–17 years. National requirements for conducting research were followed, as applicable, including obtaining the parent's or guardian's consent, if required.

A total of 286 semi-structured qualitative interviews were carried out following 11 different interview guidelines:

- 264 with practitioners (public officers, immigration lawyers and NGOs) and rights holders (asylum seekers and migrants) at the national level;
- 22 with other experts in the fields of IT, biometrics and fundamental rights.

Typically, interviews were carried out face-to-face. Only a few interviews were conducted over the phone for practical reasons.

A total of 22 interviews were carried out with experts in biometrics, IT and fundamental rights related fields, out of which 13 were with fundamental rights experts and 9 with experts in IT and biometrics. The following experts participated in these expert interviews: Prof Ajana, Arhus University; Prof Bhabha, Harvard University; Dr Brouwer, Vrije Universiteit Amsterdam; Prof Busch, Norwegian University of Science and Technology; Ms Dimitrova, Leibniz Institute for Information Infrastructure; Mr Dunning, Tusla, The Child and Family Agency, Ireland; Dr Hosein, Privacy International Network; Prof Kindt, KU Leuven; Mr Remillet, OneVisage; Mr Kukharenko, NtechLab, Prof Lodge, Expert Board of the Biometrics Institute; Dr Mittelstadt, University of Oxford; Mr Mouzourakis, European Council of Refugees and Exiles; Dr Niklas, University of Warsaw; Mr Nouak, European Association for Biometrics; Ms Pirlot de Corbion, Privacy International Network; Dr Tomaszewska-Michalak, Panoptykon Foundation; as well as experts of: eu-LISA, Frontex, the Joint Research Centre of the European Commission and UNHCR. One expert preferred not to be named.

Table 20: Overview of qualitative interviews conducted in the six EU Member States

	Target groups	Belgium	Germany	Italy	Poland	Spain	Sweden	Total
Practitioners	Asylum authority	4	3	5	7	3	2	24
	Border guards	3	4	2	5	4	3	21
	Police	2	6	8	7	6	3	32
	Consul/DMCP staff	2	3	2	2	3	3	15
	Immigration authority	1	0	5	2	3	1	12
	National Data Protection Authority	1	2	1	1	0	1	6
	Controllers	3	2	3	2	5	4	19
	Providers of legal assistance	4	4	8	6	5	4	31
Right holders	Asylum applicants	11	11	14	10	11	7	64
	Migrants in an irregular situation/ migrants apprehended at the external border	4	0	4	6	5	11	30
	Other	0	0	0	4	4	2	10
	Total	35	35	52	52	49	41	264

Source: FRA, 2017

Small-scale surveys

Three surveys were carried out to collect information about experiences with obtaining and using biometric and other personal data at the border and for the visa application process. These surveys were conducted with:

(1) border guards (BCP survey);

(2) staff processing visa applications at DMCPs and external service providers (DMCP staff survey);

(3) visa applicants (visa applicants survey).

The questionnaires were available in English and the national languages of the Member State and the third country in question, in the case of DMCPs.

BCP survey

To explore the views and experiences of border guards in charge of reading fingerprints and checking other data against VIS and SIS II at border crossing points, a small-scale survey was conducted at one border crossing point (BCP) in each of the six EU Member States. In order to have a full picture of the challenges at different types of borders, sea, land and air BCPs were included. The BCPs covered are listed in Table 21. The fieldwork was carried out between June and October 2016, covering 160 respondents. The number of respondents per BCP varied ranging from five border guards in Zeebrugge to 33 in Terespol.

The interviewers administered the questionnaires to the border guards. The majority of border guards surveyed were men (72 %, with information on gender missing from 6 % of the respondents). More than 60 % of the border guards surveyed have worked for more than three years as a border guard (27 % worked as border guards for more than 10 years) at the same BCP. Most border guards work as first-line officers (76 %), while 28 % work as second-line officers and 7 % as shift leaders. Twelve percent had another post, including other managers or coordinators, and assistants to the shift leaders.[423]

Table 21: Number of respondents at BCPs

Country	BCP	Type of border	Number of respondents
BE	Zeebrugge	sea	5
DE	Frankfurt	air	27
ES	Barajas	air	32
IT	Fiumicino	air	31
PL	Terespol	land	33
SE	Arlanda	air	32
Total			160

Source: FRA Biometrics project, BCP survey, 2016

423 The numbers do not total 100 % because some respondents work in several positions, such as first and second-line officers.

DMCP staff survey

To capture the views and experiences of staff involved in the visa application procedure, a small-scale survey was carried out at DMCPs and external service providers to DMCPs. As shown in Table 22, the surveys were carried out in Algeria (at DMCPs of Belgium, Poland and Spain in Algiers), in Nigeria (at DMCPs of Belgium, Italy and Sweden in Abuja and Lagos), in Thailand (at the DMCPs of Germany, Italy and Sweden in Bangkok) and Ukraine (at the DMCPs of Germany, Poland and Spain in Kiev and Lviv). The selection of DMCPs was based on several criteria, including the following: staff being experienced with VIS, the overall number of visa applications and the rate of rejections of applications; as well as a balanced geographical coverage. In Belgium, the survey was supposed to be carried out at Zaventem airport, but due to the terrorist attack in 2016 it was moved to Zeebrugge, which is a smaller BCP.

The survey among staff working at DMCPs included 137 persons. The numbers per EU Member State ranged from 12 staff members for Belgium to 35 for Italy. The number of staff members surveyed per host country ranged from 15 persons in Algeria to 53 in Nigeria. Of the 137 respondents, 62 worked for an external service provider.

Regarding the age distribution among respondents, more than half were aged 30 years or younger, and a quarter between 31 and 40 years. At 72 %, most of the respondents were female. Of the respondents who worked at the DMCPs or service providers, 30 % had worked there for less than one year and another 39 % between one and four years.

Table 22: Overview of total number of respondents to the survey for DMCP staff; number of staff at external service providers in brackets

		Country where DMCP is located				
		Algeria	Nigeria	Thailand	Ukraine	Total
MS of DMCP	BE	5 (0)	7 (2)			12 (2)
	DE			13 (0)	15 (6)	28 (6)
	ES	8 (4)			12 (6)	20 (10)
	IT		10 (3)	25 (21)		35 (24)
	PL	2 (0)			20 (9)	22 (9)
	SE		5 (2)	15 (9)		20 (11)
Total		15 (4)	22 (7)	53 (30)	47 (21)	137 (62)

Source: FRA Biometrics project, DMCP staff survey, 2016

Visa applicants survey

This survey collected experiences and views of rights holders in six EU Member States' DMCPs located in four countries outside the EU.[424] Altogether 584 visa applicants participated in the survey. Table 23 shows the number of respondents per DMCP. Some 54 % were women and 43 % men. The remaining respondents did not provide any information on gender or selected the category 'other'. Regarding age, the sample of visa applicants was well balanced, with the majority of respondents (53 %) aged between 31 and 50 years. Fourteen percent of the respondents were 30 years of age or younger, 31% were older than 50 years of age, and the remaining respondents did not provide information on age. Slightly more than half of respondents (57 %) had only applied once for a Schengen visa, with a quarter having applied three times or more. Most respondents applied for a visa to Germany (23 %), Sweden (19 %) or Italy (18 %). Others applied for a visa to Belgium, France, Poland and Spain and very few for other EU Member States. Most respondents were still waiting for the decision on their application (74 %), about 21 % had received a positive decision and few had received a negative decision (4 %). Fingerprints are mostly taken by staff of external service providers (72 %).

424 FRA notified DG Justice about the planned research at DMCPs in third countries and got permission to conduct the research, which took place outside the geographical scope of the EU.

Table 23: Overview of total number of respondents to the survey for visa applicants at DMCPs

EU Member State	Country where DMCP is located	Number of respondents
BE	Algeria	32
BE	Nigeria	49
DE	Thailand	81
DE	Ukraine	50
ES	Algeria	46
ES	Ukraine	45
IT	Nigeria	47
IT	Thailand	53
PL	Algeria	24
PL	Ukraine	50
SE	Nigeria	52
SE	Thailand	53
Other	Ukraine	2
Total		584

Source: FRA Biometrics project, Visa applicants survey, 2016

Non-participant observations

To better contextualise the results of the small-scale surveys, non-participant observations took place at the same locations where the surveys were carried out. Non-participant observations are a qualitative data collection method in which the researcher observes events, activities and interactions to gain a direct understanding of a phenomenon in its context. The researchers adopt a more distant role and do not participate directly in the activities they are observing (in this context, visa application procedures and border checks). The non-participant observations were made during the fieldwork for the small-scale surveys, which were conducted over one to two days. During the observations, researchers completed structured templates describing the activities observed, which were analysed afterwards.

How are the results of the field research presented?

The interviews are referred to in the form of anonymised quotes that are either representative of the research findings or illustrate differences when the answers differ significantly. The analysis refers to experts of Member State authorities as 'officers', whereas it refers to fundamental rights, biometrics or IT experts as 'experts'. The results of the small-scale surveys are represented in figures and described in the text. Where appropriate, reference is made to the findings from the non-participant observations. The conclusions are drawn from different research data and findings.

Annex II: Type of fingerprint images used in existing and planned IT systems

IT system	No. of fingers	Type of fingerprint images	Source
Eurodac	10	plain + rolled	Explanatory memorandum, p. 13; *Article 3 (1) (n) 2016 Eurodac Proposal*
VIS	10	plain	Articles 5 (1) (c), 9 (6) VIS Regulation, Annex Commission Decision 2009/756/EC
SIS II: borders / police, or both	*10*	*plain + rolled (& palm prints) latent*	*Commission Implementing Decision 2016/135*[426] *Explanatory memorandum, SIS II proposals (police) p. 15; (borders) p.16*
EES	*4*	*plain*	*Recital 21, Article 3 (1) (16) EES Regulation*
ECRIS-TCN	*10*	*plain + rolled*	*Article 3 (l)*
Interop. proposals (BMS)	*As in corresponding IT systems*	*As in corresponding IT systems*	*Articles 13, 18, 27 Interoperability proposals*

Note: *Proposed systems and proposed changes in italics*

Source: *FRA, based on existing and proposed legal instruments (2017)*

Fingerprints can be captured either as plain, rolled or latent fingerprints. For rolled fingerprints, a finger is rolled from one side to the other ('nail-to-nail') to capture all of the ridge details. Plain or flat impressions are those in which the finger is pressed down on a flat surface without rolling it. Plain images cover a smaller area than rolled prints; they typically do not have the distortion introduced during rolling.[426]

Latent fingerprints are collected by the police on a criminal site, to be matched against fingerprints of suspected or convicted criminals already stored. Rolled fingerprints are collected from criminals, and are also collected for Eurodac.

425 Commission Implementing Decision (EU) 2016/1345 of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II), OJ 2016 L 213/15.

426 Jain, A. K., Feng, J. (2011).

References

Aida and the Hungarian Helsinki Committee (2016), Country Report: Hungary, 2016.

Amnesty International (2013), 'Eritrea: 20 years of independence, but still no freedom', London, 2013.

Amnesty International (2015), 'Fenced out: Hungary's violations of the rights of refugees and migrants', EUR 27/2614/2015, October 2015.

Amnesty International (2016), 'Hotspot Italy: How EU's flagship approach leads to violations of refugee and migrant rights', EUR/30/5004/2016.

Article 29 Data Protection Working Party (2013), *Opinion 03/2013 on purpose limitation*, WP 203, 2 April 2013.

Article 29 Data Protection Working Party (2017), WP29 Guidelines on transparency under Regulation 2016/679, WP 260.

Benson, J. and Williams, J. (2008), 'Age determination in refugee children', *Australian Family Physician*, Vol. 37, No. 10, October 2008.

Chaudhary, A., Sahni, S. and Saxena, S. (2014), 'Survey: Techniques for Aging Problems in face recognition', *MIT International Journal of Computer Science and Information Technology,* Vol. 4, No. 2, August 2014.

Council of Europe, Committee of Ministers (1984), Recommendation on the Criminal Record and Rehabilitation of Convicted Persons, No. R(84)10, 21 June 1984.

Council of Europe, Ad Hoc Committee on Data Protection (CAHDATA) (2016), Draft explanatory report.

Council of the European Union (2014), *Best Practices for upholding the Obligation in the Eurodac Regulation to take fingerprints*, Brussels, 30 October 2014.

Council of the European Union (2016), *Renewed Information management Strategy – draft 5th Action List,* 5175/3/16 REV 3, 27 June 2016.

Council of the European Union, Working Party on Information Exchange and Data Protection (DAPIX) (2016), *Renewed Information Management Strategy (IMS) – 5th Action List*, 10824/16, 30 June 2016.

Council of the Baltic Sea States (2011), Handbook for consular and diplomatic staff on how to assist and protect victims of human trafficking.

De Hert, P. (2013), 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in: Campisi, P. (ed.), *Security and Privacy in Biometrics*, London, Springer, 2013, p. 391.

European Asylum Support Office (EASO) (2013), *Age assessment practice in Europe*, December 2013, Luxembourg, Publications Office.

European Commission (2013a), *Guidelines for the identification of victims of trafficking in human beings: Especially for Consular Services and Border Guards*, Luxembourg, Publications Office.

European Commission (2013b), *SIS II, Schengen information system, Helping you move freely, helping you live safely*, leaflet, 18 April 2013.

European Commission (2014a), Summary of contextual overviews on children's involvement in criminal judicial proceedings in the 28 Member States of the European Union.

European Commission (2014b), Summary of EMN Ad-Hoc Query No. 588, Eurodac fingerprinting, September 2014.

European Commission (2015a), A European Agenda on Migration, COM(2015) 240 final, 13 May 2015.

European Commission (2015b), Commission Staff Working Document on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints, SWD(2015) 150 final, 27 May 2015.

European Commission (2015c), Progress Report on the Implementation of the hotspots in Italy, COM(2015) 679 final, Strasbourg, 15 December 2015.

European Commission (2015d), 'Visa Information System now fully operational worldwide', 2 December 2015.

European Commission (2016a), Commission Staff Working Document, *Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) / REFIT Evaluation*, SWD(2016) 328 final, Brussels, 14 October 2016.

European Commission (2016b), Communication from the Commission to the European Parliament and the Council, "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, Brussels, 6 April 2016.

European Commission (2016c), 'Italy: Progress report', 10 February 2016.

European Commission (2016d), *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 of the European Parliament and of the Council establishing the Visa Information System (VIS), the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation*, COM(2016)655 final, Brussels, 14 October 2016.

European Commission (2016e), *Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with Art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and Art. 59 (3) and 66 (5) of Decision 2007/533/JHA*, COM(2016) 880 final, Brussels, 21 December 2016.

European Commission (2016f), *Report from the Commission to the European Parliament and the Council: The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)*, COM(2016) 93 final, 29 February 2016.

European Commission (2017a), Communication from the Commission to the European Parliament and the Council on a more effective return policy in the European Union – A Renewed Action Plan, COM(2017) 200 final, 2 March 2017.

European Commission (2017b), Commission Staff Working Document, *Implementation of the Action Plan on UAMs (2010-2014)*, SWD(2017) 129 final, 12 April 2017.

European Commission (2017c), The protection of children in migration, COM(2017) 211 final, Brussels, 12 April 2017.

European Council of Refugees and Exiles (ECRE) (2013), Bulgaria accused of putting asylum seekers at risk by providing information on Syrians to Syrian embassy, Brussels, 31 October 2013.

ECRE (2015), Comments on the European Commission Staff Working Document "on Implementation of the Eurodac Regulation as regards the obligation to take fingerprints", June 2015.

European Data Protection Supervisor (EDPS) (2015), Guide for exercising the right of access, 15 October 2015.

Eurostat, Asylum applicants considered to be unaccompanied minors, 11 May 2017.

eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice) (2015a), *Biometrics in Large-Scale IT: Recent trends, current performance capabilities, recommendations for the near future.*

eu-LISA (2015b), *Smart Border Pilot Project: Report on the technical conclusions of the Pilot,* Vol. 1, November 2015.

eu-LISA (2016), *VIS Report pursuant to Article 50(3) of Regulation (EC) No 767/2008, VIS Report pursuant to Article 17(3) of Council Decision 2008/633/JHA*, July 2016.

eu-LISA (2017a), *Annual report on the 2016 activities of the Eurodac central System, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013*, May 2017.

eu-LISA (2017b), *List of designated authorities which have access to data recorded in the Central System of Eurodac pursuant to Article 27 (2) of the Regulation (EU) No. 603/2013, for the purpose laid down in Article 1 (1) of the same Regulation*, April 2017.

eu-LISA (2017c), *List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31 (8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46 (8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System*, OJ 2017 C 228/1.

eu-LISA (2017d), *SIS II – 2016 Statistics*, February 2017.

Feng, J., Jain, A.K. and Ross, A. (2009) *Fingerprint Alteration,* MSU Technical Report, December 2009.

Finland, Refugee Advice Centre (*Pakolaisneuvonta RY*), Single children with asymlum procedure: Challenges (*Yksintulleet lapset turvapaikkamenettelyssä: Haasteet*).

FRA (2010a), Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II), Luxembourg, Publications Office, May 2010.

FRA (2010b), *The duty to inform applicants about asylum procedures: The asylum-seeker perspective*, Luxembourg, Publications Office.

FRA (2010c), *Separated, asylum-seeking children in European Union Member States: Comparative report*, Luxembourg, Publications Office.

FRA (2011), *Fundamental Rights of migrants in an irregular situation in the European Union: Comparative report,* Luxembourg, Publications Office, November 2011.

FRA (2012), *Access to justice in cases of discrimination – Steps to further equality*, Luxembourg, Publications Office, December 2012.

FRA (2013), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office, January 2014.

FRA (2014), *Criminalisation of migrants in an irregular situation and of persons engaging with them*, Luxembourg, Publications Office, March 2014.

FRA (2015a), Annual Work Programme 2015, Vienna, December 2014.

FRA (2015b), *Fundamental rights implications of the obligation to provide fingerprints for Eurodac*, No. 05/2015, Vienna, October 2015.

FRA (2015c), *Opinion of the European Union Agency for Fundamental Rights concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information System, 1/2015 [ECRIS]*, FRA Opinion – 1/2015 [ECRIS], Vienna, 4 December 2015

FRA (2015d), *Severe labour exploitation: workers moving within or into the European Union States' obligations and victims' rights*, Luxembourg, Publications Office, June 2015.

FRA (2016a), *The impact of the proposal for a revised Eurodac Regulation on fundamental rights. Opinion of the European Union Agency for Fundamental Rights,* FRA Opinion - 6/2016 [Eurodac], Vienna, 22 December 2016.

FRA (2016b), *Opinion of the European Union Agency for Fundamental Rights on the impact on children of the proposal for a revised Dublin Regulation (COM(2016)270 final 2016/0133 COD), 4/2016 [Dublin]*, Vienna, 23 November 2016.

FRA (2017a), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update, Luxembourg, Publications Office.

FRA (2017b), *Fundamental rights and the interoperability of EU information systems: borders and security,* Luxembourg, Publications Office, July 2017.

FRA (2017c), *Mapping minimum age requirements concerning the rights of the child in the EU*, November 2017.

FRA and Council of Europe (2014), *Handbook on European data protection law*, Luxembourg, Publications Office.

FRA and Council of Europe (2016), *Handbook on European law relating to access to justice*, Luxembourg, Publications Office.

France, Code on the entry and stay of aliens and on the right of asylum (*Code de l' entrée et du séjour des étrangers et du droit d'asile*), Article R611-9.

France, CNIL (*La Commission nationale de l'informatique et des libertés*), Délibération No. 2012-293 of 13 September 2012.

France, Le Monde (2018), *Pau : des migrants portent plainte pour tortures et mauvais traitements subis en Italie*, 11 January 2018.

Germany, Berlin State Assembly (*Abgeordnetenhaus Berlin*), *Erkennungsdienstliche Behandlung von unbegleiteten minderjährigen Flüchtlingen in Berlin II – bei der Polizei*, Printed Paper 17/11992, 11 June 2013.

Goncalves, M. E. and Gameiro, M. I. (2014), 'Does the Centrality of Values in the Lisbon Treaty Promise more than it can actually offer? EU Biometrics policy as a case study', *European Law Journal*, Vol. 20, No. 1.

Hallinan, D. (2015), 'Effects of surveillance on freedom of assembly, association and expression' in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, New York, Routledge.

High Level Expert Group on information systems and interoperability (HLEG) (2017), *Final report*, May 2017.

Human Rights Council (2015), 'Report of the detailed findings of the Commission of Inquiry on Human Rights in Eritrea', A/HRC/29/CRP.1, 5 June 2015.

International Civil Aviation Organization (ICAO) (2015), *Doc 9303, Machine Readable Travel Documents Part 3 — Specifications Common to all MRTDs*.

Ireland, Data Protection Commissioner, *An Garda Síochána: Final Report of Audit*, Portarlington, March 2014.

Italy, Ministry of Interior (2014), Circular letter 400/A/2014/1.308.

Italy, Commissione Straordinaria per la tutela e la promozine dei diritti umani, Senato della Repubblica (XVII Legislatura) (2017), *Rapporto sui Centri di permanenza per il rimpatrio in Italia - Dicembre 2017*, December 2017.

Jain, A. K. and Feng, J. (2011), 'Latent Fingerprint Matching', IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 33, No. 1, January 2011.

Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen (2013), *Fingerprint Recognition for Children,* Luxemburg, Publications Office of the European Union (Publications Office), September 2013, Report EUR 26193 EN.

Kindt, E. J. (2013), *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis*.

Łysienia, M. (2014), 'Correct functioning of the System POBYT as a guarantee of respect for the foreigners' rights' (*Prawidłowe funkcjonowanie systemu POBYT jako gwarancja przestrzegania praw cudzoziemców*) in: Białas, J., Fagasiński, M., Górczyńska, M., Jaźwińska, M., Łysienia, M., Ostaszewska-Żuk, E., Rusiłowicz, K., Witko, D., Looking for protection. Selected problems regarding realization of the rights of foreigners who seek granting refugee status and covered by the international protection in the period 2012-2014. Observations of the Program for Legal Aid for Refugees and Migrants of the HFHR (*W poszukiwaniu ochrony. Wybrane problemy dotyczące realizacji praw cudzoziemców ubiegających o nadanie statusu uchodźcy i objętych ochroną międzynarodową w latach 2012-2014. Obserwacje Programu Pomocy Prawnej dla Uchodźców i Migrantów Helsińskiej Fundacji Praw Człowieka*), Warsaw, 2014, pp. 50–51.

MigSzol (2016), 'Hungary's long summer of migration – irresponsible governance fails people seeking international protection', August 2016.

Missing Children Europe (2016), *SUMMIT Report: Best practices and key challenges on interagency cooperation to safeguard unaccompanied children from going missing*, February 2016.

Newton, E., Coleman, G. and Yuh P. (eds.), National Institute of Standards and Technology (2008), *American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2: XML Version*, NIST Special Publication 500-275, 12 August 2008.

Oxfam (2016), *Hotspot, rights denied*, May 2016.

ProAsy (2015), *Erniedrigt, misshandelt, schutzlos: Flüchtlinge in Bulgarien*, April 2015.

Raab C. (2015), 'Surveillance: Effects on Privacy, autonomy and dignity' in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, New York, Routledge.

Ramanathan, N., Chellappa, R., Biswas, S. (2009), 'Computational methods for modelling facial aging: A survey', *Journal of Visual Languages and Computing 20*, pp. 131–144.

Redattore Social (2015), *Eritrei, cartelli e slogan a Lampedusa. "Siamo rifugiati, niente impronte"*, 17 December 2015.

Repubblica (2016), *Lampedusa, "Mandateci via da questa prigione"*, 7 May 2016.

Sanchez del Rio, J., Conde, C., et.al., (2015), *Face-based recognition systems in the ABC e-Gates*, Department of Computer Science and Statistics, Rey Juan Carlos University, Madrid, Spain.

SIRENE Manual, OJ 2017 L 231/6.

SIS II Supervision Coordination Group (SIS II SCG), *Activity Report 2013-2015*.

SIS II Supervision Coordination Group (SIS II SCG) (2014), *Report on the exercise of the rights of the data subject in the Schengen Information System (SIS)*, October 2014.

Statewatch (2015), Briefing – Coercive measures or expulsion: Fingerprinting migrants, May 2015.

Sweden, Registers of suspects and convicted crimes (*Misstankeregistret och brottsregistret*).

Sweden, Migration Agency (*Migrationsverket*), This is how it works to apply: For you who will apply for asylum without a parent or other care taker (*Så fungerar det att söka: till dig som söker asylum utan förälder eller annan vårdnadshavare*), November 2017, Webpage.

United Kingdom, UK Visas and Immigration Department (2013), *Asylum Instruction: Fingerprinting*.

United Nations (UN) (1985), *Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules')*, General Assembly resolution 40/33 of 29 November 1985.

UN Children's Fund (UNICEF) (2016), *Danger every step of the way: A harrowing journey to Europe for refugee and migrant children*, June 2016.

Veigel, S. and Wenk-Ansohn, M. (2015), *Gewalt mit Methode? Das »Dublinverfahren« und Menschenrechtsverletzungen an den EU-Außengrenze*, ASYLMAGAZIN 6/2015 pp. 187–193, June 2015.

VIS Supervision Coordination Group (VIS SCG) (2016), *Report on access to the VIS and the exercise of data subjects' rights*, February 2016.

Zhang, D. (2013), *Automated Biometrics: Technologies and Systems*, Springer, 2013.

Getting in touch with the EU

In person

All over the European Union, there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: http://europa.eu/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU.
Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

Notes: (continued)

[1] *Ireland and the United Kingdom do not participate in VIS. Denmark is not bound by the Regulation but has opted in for VIS. VIS does not yet apply to Croatia and Cyprus, and only partially applies to Bulgaria and Romania as per Council Decision (EU) 2017/1908 of 12 October 2017.*

[2] *Cyprus and Ireland are not yet connected to SIS. Denmark is not bound by the Regulation or the Council Decision but has opted in for the SIS II, and must decide whether to opt in again upon the adoption of the SIS II proposals. The United Kingdom is participating in SIS but cannot use or access alerts for refusing entry or stay into the Schengen area. Bulgaria, Croatia and Romania cannot issue Schengen-wide alerts for refusing entry or stay in the Schengen area as they are not yet part of the Schengen area.*

[3] *Denmark may decide to opt in for EES and ETIAS.*

[4] *ECRIS-TCN does not apply to Denmark. The United Kingdom and Ireland may decide to opt in.*

[5] *Denmark, Ireland and the United Kingdom will take part as they participate in the IT systems made interoperable.*

Existing and planned EU large-scale IT systems

IT system	Main purpose	Persons covered	Applicability	Biometric identifiers
European dactylography (Eurodac)	Determine the Member State responsible to examine an application for international protection *Assist with the control of irregular immigration and secondary movements*	Applicants and beneficiaries of international protection, *migrants in an irregular situation*	all EUMS + SAC	
Visa Information System (VIS)	Facilitate the exchange of data between Schengen Member States on visa applications	Visa applicants and sponsors	24 EUMS (not CY, HR, IE, UK)[1] + SAC	
Schengen Information System (SIS II) - police	Safeguard security in the EU and Schengen Member States	Missing or wanted persons	26 EUMS (not CY, IE)[2] + SAC	
Schengen Information System (SIS II) - borders	Enter and process alerts for the purpose of refusing entry into or stay in the Schengen Member States	Migrants in an irregular situation	25 EUMS (not CY, IE, UK)[2] + SAC	
Schengen Information System (SIS II) - return	*Enter and process alerts for third-country nationals subject to a return decision*	*Migrants in an irregular situation*	*25 EUMS (not CY, IE, UK)[2] + SAC*	
Entry-Exit System (EES)	*Calculating and monitoring the duration of authorised stay of third-country nationals admitted and identify over-stayers*	*Travellers coming for a short-term stay*	*22 EUMS (not BG, CY, HR, IE, RO, UK)[3] + SAC*	
European Travel Information and Authorisation System (ETIAS)	*Assess if a third-country national who does not need a visa poses a security, irregular migration or public health risk*	*Visa free travellers*	*26 EUMS (not IE, UK)[3] + SAC*	*None*
European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)	*Share information on previous convictions of third-country nationals*	*Third-country nationals with a criminal record*	*27 EUMS (not DK)[4]*	
Interoperability – Common Identity Repository	*Establish a framework for interoperability between EES, VIS, ETIAS, Eurodac, SIS II and ECRIS-TCN*	*Third-country nationals covered by Eurodac, VIS, SIS II, EES, ETIAS, and ECRIS-TCN*	*28 EUMS[5] + SAC*	

Notes: *Planned systems and planned changes within systems are in italics, or shown by a light blue background*

 : *Fingerprints;*  : *Palm prints;*  : *Facial image;*  : *DNA profile.*

EUMS: EU Member States; SAC: Schengen Associated Countries, i.e. Iceland, Liechtenstein, Norway and Switzerland.

Source: *FRA, based on existing and proposed legal instruments, 2018*

doi:10.2811/136698 TK-02-18-068-EN-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

Europe's migration and security challenges have prompted the European Union (EU) to develop and enhance multiple large-scale information technology systems (IT systems). Policy and legal developments in this area are evolving rapidly. The European Commission has proposed amending the legal bases for Eurodac and the Schengen Information System (SIS II), and is expected to propose amending the Visa Information System (VIS) in 2018. In addition, four new systems are planned: the Entry-Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) and, most crucially, an IT system that seeks to ensure interoperability across existing and planned systems.

Such systems provide invaluable support to border management efforts, but also have wide-ranging fundamental rights implications. The persons affected – including both regular travellers and persons who may be in situations of vulnerability – typically do not fully understand the implications of the use of such systems. This report therefore outlines the fundamental rights implications of collecting, storing and using biometric and other data in EU IT systems in the area of asylum and migration.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 1580 30-0 – Fax +43 1580 30-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office

ISBN 978-92-9491-925-0