FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

FRA Opinion – 2/2018
[VIS]

Vienna, 30 August 2018

The revised Visa Information System and its fundamental rights implications

Opinion of the European Union Agency for Fundamental Rights

Contents

Acronyms

AFIS	Automated Fingerprint Identification System
CVCA	Country Verifying Certificate Authorities
CIR	Common Identity Repository
CISA	Convention implementing the Schengen Agreement
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)
ECHR	European Convention on Human Rights
ECRIS-TCN	European Criminal Records Information System on Third Country Nationals
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
eMRTD	electronic Machine Readable Travel Document
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation 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
Eurodac	European Dactyloscopy
Europol	European Union Agency for Law Enforcement Cooperation
FRA	European Union Agency for Fundamental Rights
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
Interpol	International Criminal Police Organization
IT system	Information technology system
JRC	Joint Research Centre
MID	Multiple-Identity Detector
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TDAWN	Travel Documents Associated with Notices
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
VIS	Visa Information System

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA),

Bearing in mind the Treaty on European Union (TEU), in particular Article 6 thereof,

Recalling the obligations set out in the Charter of Fundamental Rights of the European Union (the Charter),

In accordance with Council Regulation (EC) No. 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (FRA), in particular Article 2 with the objective of FRA "*to provide the relevant institutions, bodies, offices and agencies of the Community and its EU Member States when implementing Community law with assistance and expertise relating to fundamental rights in order to support them when they take measures or formulate courses of action within their respective spheres of competence to fully respect fundamental rights*",

Having regard to Article 4 (1) (d) of Council Regulation (EC) No. 168/2007, with the task of FRA to "*formulate and publish conclusions and opinions on specific thematic topics, for the Union institutions and the EU Member States when implementing Community law, either on its own initiative or at the request of the European Parliament, the Council or the Commission*",

Having regard to Recital (13) of Council Regulation (EC) No. 168/2007, according to which "*the institutions should be able to request opinions on their legislative proposals or positions taken in the course of legislative procedures as far as their compatibility with fundamental rights are concerned*",

Having regard to previous opinions of FRA on related issues; in particular the FRA opinion on the future European Criminal Records Information System for third-country nationals,[1] FRA opinion relating to the proposal for a revised Eurodac Regulation,[2] FRA opinion on the proposed Regulation on the European Travel Information and Authorisation System,[3] and FRA opinion on interoperability,[4]

Building on the mapping of fundamental rights implications of interoperability FRA published in July 2017 in the context of the work of the High Level Expert Group on Information Systems and Interoperability in the report 'Fundamental rights and the

---

1 European Union Agency for Fundamental Rights (FRA) (2015), *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*, FRA Opinion – 1/2015 [ECRIS], Vienna, 4 December 2015.

2 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016.

3 FRA (2017), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], Vienna, 30 June 2017.

4 FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018.

interoperability of EU information systems: borders and security'[5] as well as on the findings of the FRA research project on the processing of biometric data in large-scale information technology systems established by the European Union to manage asylum and migration published on 28 March 2018,[6]

Having regard to the request of the European Parliament of 21 August 2018 to FRA for an opinion "on the fundamental rights implications of the proposal, such as, but not limited to, the right to the protection of personal data" which also included the request to assess "the fundamental rights aspects of the access by law enforcement authorities and Europol to the VIS",

SUBMITS THE FOLLOWING OPINION:

[5] FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017.

[6] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018.

Opinions

FRA Opinion 1

The implementation of the VIS Regulation may affect several fundamental rights, as listed in proposed Recital (47). However, the operative part of the regulation only contains provisions reminding Member State authorities to implement the VIS Regulation in a non-discriminatory manner and fully respecting human dignity and integrity of the person. The proposal will also add a provision on the rights of the child. A comprehensive fundamental rights clause is only contained in the Recitals of the VIS Regulation and of the proposal.

One of the fundamental rights protected by the Charter is the right to non-discrimination, which is presently reflected in the VIS Regulation and in the Visa Code. However, both legislative acts prohibit discrimination only on limited grounds.

To promote a fundamental rights compliant implementation of VIS, the EU legislator should include a general fundamental rights safeguard clause in the operative part of the VIS Regulation, for example in Article 7, drawing upon the language used in Recital (47) of the proposal and in Article 14 of the compromise text of the European Travel Information and Authorisation System Regulation (ETIAS compromise text). Such clause should re-affirm Member States' obligation to implement the regulation in full compliance with the Charter. It should contain a specific provision on child protection as suggested by amended Article 7 (3) of the proposal.

Furthermore, the EU legislator should amend Article 7 (2) of the VIS Regulation and Article 39 (3) of the Visa Code by including all other discrimination grounds prohibited by Article 21 of the Charter, namely "colour, social origin, genetic features, language, political or any other opinion, membership of a national minority, property and birth".

FRA Opinion 2

The EU-wide storage of personal data, including biometrics, of all third-country nationals holding a residence permit issued by a Member State, including long-term residents, does not meet the necessity and proportionality requirements under the Charter. A mechanism to store the personal data in VIS only of those third-country nationals who enter the EU with a long-stay visa or a residence permit for the first time would store data of fewer people, and thus be less intrusive on fundamental rights, although the necessity and proportionality of such data processing would still need to be shown.

The EU legislator should refrain from adding residence permit holders to VIS, thereby limiting the expansion of the personal scope of VIS to long-stay visas, and amend the relevant parts of the proposal accordingly.

Should the EU legislator consider it necessary to include certain categories of residence permit holders in an EU-wide information system, this should be limited to those individuals who are entering the EU with a residence permit for the first time. To achieve this, the EU legislator could explore the feasibility of amending the Visa Code or other relevant EU legislation to oblige EU Member States to issue a short-stay or long-stay visa for the first entry of persons to whom they granted a residence permit.

FRA Opinion 3

As pointed out in FRA Opinion 2, processing personal data of long-term residence permit holders in VIS is not necessary and proportionate. Their inclusion in VIS would, in practice, result in an open-ended retention of their personal data, as residence permits get extended. In such cases, also links to applications of other members of a group travelling together, not being family members, could in practice be retained beyond five years. This would not be justified, unless specific criminal investigations are ongoing.

As pointed out in FRA Opinion 2, the personal data of long-term residence permit holders should not be processed in VIS. This would avoid that data of long-term residence permit holders are, in practice, retained forever. In case the EU legislator would, nevertheless, decide to retain individual files on residence permit holders in VIS, a solution must be found to avoid that data (including links to other applications) stored in individual files is retained beyond five years, unless the retention is necessary for specific ongoing criminal investigations.

The incorrect cross-reference to Article 22a (5) should be deleted from proposed Article 23 (2).

FRA Opinion 4

The storing of sponsor data in VIS under proposed Articles 22c may put victims of violent crimes perpetrated by the sponsor at risk.

The EU legislator should include a safeguard in proposed Article 22c for victims of violent crimes, such as domestic violence or trafficking in human beings, committed by their sponsor. In these cases, to protect the victim from further risks, the victim's file in VIS should be de-linked from the sponsor.

FRA Opinion 5

The proposed Article 22h of the VIS Regulation will allow police and immigration law enforcement authorities to consult VIS data of long-stay visa and residence permit holders when they carry out checks within the territory. The purpose of such checks is formulated in a broad manner, providing police with broad powers that entail a risk of discriminatory police stops and of arbitrary deprivation of liberty.

The EU legislator should remove the wording "whether the person is not a threat to public policy, internal security or public health of any of the Member States" from Article 22h (1), as it entails a risk for discriminatory police stops and/or arbitrary deprivation of liberty.

FRA Opinion 6

In spite of quality assurance safeguards included in proposed Article 29a (2) (c) and proposed Article 29a (2a) of the VIS Regulation, the absence of a requirement to subject biometric searches with facial images to a technical feasibility test may result in false biometric matches. These can lead to decisions that may negatively affect the rights of the data subjects.

The EU legislator should make the introduction of biometric searches with facial images conditional upon the technical possibility to guarantee a reliable match, in line with the approach taken for other EU IT systems.

FRA Opinion 7

The proposal seems to use the terms 'photograph' and 'facial image' interchangeably, while other legislative proposals on large-scale IT systems use only the term 'facial image' or, as it is the case with SIS, appear to draw a distinction between 'photographs' and 'facial images'. Consistency in terminology would help to ensure legal clarity and foreseeability of the proposed amendments. If a photograph should be distinguished from a facial image because a photograph should not be used for automated biometric matching, for example, its meaning should be defined in the proposal.

The EU legislator should ensure consistency in terminology between 'photographs' and 'facial images' if both terms have the same meaning. Alternatively, the EU legislator should define the meaning of a 'photograph' if it has a different meaning than 'facial image'.

FRA Opinion 8

The processing of biometric data of children is very sensitive and must be subject to strict requirements. Children and older persons should not be put in a situation in which they would be disproportionately affected by the negative consequences of a false match. The reliability of fingerprint matches drops for persons older than 70 years due to problems in high quality data acquisition for persons of that age. For children below the age of 13, the reliability drops over time as the child grows. Moreover, the EU legislator could make an effort to reduce practical hurdles and costs, where children and older people need to travel long distances to provide their biometrics.

***To respect the rights of the child enshrined in Article 24 of the Charter and promote the rights of the elderly in Article 25 of the Charter, the EU legislator should complement the horizontal safeguard in proposed Article 7 (3) of the VIS Regulation with the following actions*:**

- ***If individual files in VIS are, contrary to FRA Opinions 2 and 3, kept for over five years, (for example, following the extension of a residence permit) stipulate in proposed Articles 9a and 22b that no automated queries will be carried out with biometric data of people aged 70 years or over and of children below the age of 13 years when more than five years have passed since their biometrics were collected.***

  Alternatively, postpone any automated querying until the results of a large-scale field trial make it possible to achieve high-quality matching from children and older people.

- ***Introduce an obligation to involve specialised dactyloscopic and facial recognition experts whenever comparisons are made using biometrics of people older than 70 years and when stored biometrics which are older than five years are used for children who are younger than 13 years of age.***

In addition, to avoid excessive burden and costs for families with children and for older persons when they need to travel long distances to give their biometrics, the EU legislator

- ***Should amend proposed Article 9 (8) of the VIS Regulation, allowing for the extraction of the facial image stored in the electronic Machine Readable Travel Document (eMRTD) also in those cases where in exceptional circumstances the travel involves excessive burden and costs for families with many children and for older persons.***

- ***Could consider amending the relevant provision of the Visa Code to allow taking fingerprints and facial images at the border. Article 16 of the EES Regulation (Regulation (EU) 2017/2226) should be adjusted accordingly.***

FRA Opinion 9

The purpose of the automated VIS query for long-stay visa and residence permit holders is unclear. The term "hit" is not defined and data processed through automated queries are excessive. Sensitive Eurodac data that appear irrelevant for the query are consulted, and a safeguard is missing to prevent the sharing of information on beneficiaries of international protection whose data are stored in Interpol databases.

The EU legislator should:

- ***Better define the purpose of the automated VIS query for long-stay visa and residence permit holders in proposed Articles 22b (1) and Articles 22b (5) in a manner which complies with the necessity and proportionality of restriction to the right to protection of personal data. More specifically, this could mean:***
    - ***carrying out automated VIS queries only if the file is created by the consular authority, thus excluding automated queries on files created within the territory;***
    - ***amending proposed Article 22b (1) and Article 22b (5) stipulating that automated queries are solely carried out for the purpose of supporting border management authorities to assess whether the person poses a threat to public policy or internal security (thus excluding public health considerations).***
- ***Amend proposed Article 9a (3) to exclude from the automated checks applicants for international protection whose data are stored under Chapter II of the Eurodac Regulation.***
- ***Define the meaning of "hit" used in Article 9a, 9b and 9c as well as in Article 22b.***
- ***Insert a clause in Articles 9a and 22b to make clear that a VIS user can only see hits to IT systems he or she is authorised to consult according to the legal instruments regulating the individual IT systems. This limitation must also apply to the verifying authority under Article 9c (1) and 22b (7) of the proposal.***
- ***Define expressly which "relevant data" contained in Article 9 (4) will be used for automated checks in case of short-stay visa applications.***
- ***Reformulate proposed Article 9c (5) to limit the duty to inform other EU Member States to specific situations where this is justified.***
- ***Introduce a safeguard for preventing that hits against Interpol databases are shared with the owners of Interpol data, similar to Article 9 (5) of the interoperability proposals.***

FRA Opinion 10

The data referred to in Article 1 (5) and Article 7 (2) of the proposal are not fully aligned. Consistency in defining the data processed would help to ensure legal clarity and foreseeability of the proposed amendments.

The EU legislator should:

- ***clarify in the proposed amendments to Article 5 (3) of the VIS Regulation which data is meant with the reference to Article 22d (cc) of the VIS Regulation;***
- ***clarify in the proposed amendments to Article 5 (3) of the VIS Regulation and in Article 7 (2) of the European Commission proposal (which amends Article 18 (1) (b) of the proposed Interoperability Regulation on borders and visa) whether data referred to in Article 9 (4) (aa) and (cc) of the VIS Regulation should be stored in the Common Identity Repository or not.***

FRA Opinion 11

Third-country nationals who are family members of a Union citizen, a national of the European Economic Area (EEA) or a Swiss national to whom Directive 2004/38/EC applies and who do not hold a residence card referred to under that directive fall within the personal scope of VIS. Adequate safeguards must be in place to protect their privileged status under EU law.

The EU legislator should build in a saving clause in proposed Article 9b emphasising that carrying out automated checks in other large-scale IT databases must not unduly and disproportionately affect the issuance of an entry visa. The absence of a safeguard clause could result in undue restrictions to the exercise of the right to free movement of those third-country nationals who are family members of EU citizens and of other non-EU nationals enjoying the right to free movement under EU law.

The EU legislator should remove the wording "high epidemic risks" from proposed Article 9b (1) as the checks carried out through the European Search Portal will not contribute to establish whether such risks exist and it raises issues in light of the object and purpose of Article 5 (2) of Directive 2004/38/EC. Public health risks should be assessed at the border based on epidemiological information provided by relevant official sources.

The EU legislator should also amend the relevant Recital to clarify that proposed Chapter IIIa does not apply to third-country national family members of EU citizens and of nationals of a third country enjoying the right to free movement under EU law.

FRA Opinion 12

The proposal introduces some relevant changes to Article 31 of the VIS Regulation on sharing VIS data with third parties. While the General Data Protection Regulation (GDPR) provides for general safeguards concerning data transfers, a more precise reference to these as well as inclusion of additional specific safeguards in the VIS Regulation would help to ensure the protection of the data subject's fundamental rights.

In regard to Article 31 of the VIS Regulation, the EU legislator should therefore:

- ***in Paragraph (1), replace the words "without prejudice to Regulation (EU) 2016/679" with an explicit reference to the relevant GDPR***

provisions by stating that "the data transfer shall comply with the relevant provisions of Union law, in particular Regulation (EU) 2016/679, including its Chapter V".

- ***keep the legal safeguard in Article 31 (2) (b) pursuant to which "the third country or international organisation agrees to use the data only for the purpose for which they were provided";***
- ***explicitly exclude sharing personal data of applicants for international protection with their country of origin to prepare their return as long as no final decision has been taken on their application for international protection;***
- ***building upon Article 50 of the GDPR and Article 40 of the Police Directive, consider encouraging the European Commission and the national supervisory authorities to cooperate with the data protection authorities of the third countries with which VIS data is shared.***

For legal clarity, the EU legislator should include an explicit prohibition of transferring data to third parties for law enforcement purposes. Should the EU legislator envisage such transfer of VIS data to third parties for law enforcement purposes, such transfers should be subject to safeguards equivalent to those included in Article 65 (2) and (5) of the ETIAS compromise text.

FRA Opinion 13

It is important that the data subjects are informed about all relevant aspects of the data processing, also in light of the fact that adequate information is a pre-condition for access to an effective remedy against inaccurate or unlawfully stored data in VIS.

The EU legislator should consider the following measures to strengthen the right to information included in Article 37 of the VIS Regulation:

- ***expressly require that the information provided should also cover the legal basis for the processing of personal data, the possibility to restrict the processing of personal data and, where applicable, the data transfer to third countries and international organisation, in line with the GDPR and the Police Directive;***
- ***adjust the wording of Article 37 (1) (c) of the VIS Regulation to ensure the provision of explicit information on the fact that personal data may be accessed by law enforcement authorities, drawing upon the existing VIS Regulation as well as Article 50 of the EES Regulation and Article 30 of the Eurodac proposal;***
- ***expressly require that the information should be provided in a concise, intelligible and easily accessible form, and, where applicable, in a transparent form, pursuant to the GDPR and the Police Directive.***
- ***consider adopting a standardised form for notifying the reasons for the rejection which will be stored in VIS as per proposed Article 22d (h), so as to enable a refused applicant to exercise his/her right to an effective remedy. Such form could be similar to Annex VI of the Visa Code or Annex V of the Schengen Borders Code.***

FRA Opinion 14

The proposal only suggests one change to Article 38 of the VIS Regulation. In light of the significant obstacles adversely affecting the effectiveness of the right to access, correction and deletion of personal data more substantial changes to this provision would support data subjects in exercising their rights more effectively.

In order to increase the effectiveness of the access, correction and deletion procedure, the EU legislator should:

- ***include in Article 38 (1) of the VIS Regulation a deadline for the reply by adding the following sentence: "The Member State shall reply to such requests without delay and no later than within 30 days of receipt of the request", in line with Article 12 (3) and (4) of the GDPR;***
- ***include in Article 38 (2) of the VIS Regulation a deadline for the correction or deletion of personal data by indicating that the "correction and deletion shall be carried out without delay and no later than in 30 days of receipt of the request", in line with Article 12 (3) and (4) of the GDPR;***
- ***cover in Article 38 (3) also requests for access to personal data;***
- ***include in Article 38 (3) a duty to inform in writing any person who has approached a Member State other than the one responsible to review the request, indicating to whom the request has been forwarded;***
- ***include in the VIS Regulation the right to restriction of data processing.***

FRA Opinion 15

Small inaccuracies between the data sent by the airline and the one stored in the IT system may result in a significant number of "NOT OK" to board, even when the mismatch is clearly caused by a data entry error. Steps should be taken to mitigate this risk.

The Commission implementing act setting up the authentication scheme in proposed Article 45b (5) should design the carrier gateway in such a way that mismatches that are clearly the result of data entry mistakes are not flagged as "NOT OK".

FRA Opinion 16

The right to information is a precondition to effectively exercise the right to access, correction and deletion of personal data. Therefore, it is crucial that the person concerned receives appropriate information if refused boarding due to a "NOT OK" message.

The EU legislator should include a specific provision in proposed Article 45b obliging the carriers to provide information to passengers refused boarding due to a "NOT OK" response from VIS, indicating also how to exercise their right to access, correction and deletion of personal data stored in VIS.

FRA Opinion 17

Carriers should be able to contact a functioning support centre where they can receive a reply within minutes when they have queries on a "NOT OK" to board reply. This will limit the number of cases in which genuine passengers are not allowed to board as a result of a wrong match based on inaccurate data stored in the system.

The EU legislator should consider establishing a support centre within each Member State and/or within Frontex as may be appropriate which is sufficiently staffed to provide real time response to all queries carriers have in relation to passengers for whom they received a "NOT OK" to board. Such a call centre would require significant resources, so that in most cases a decision on whether or not to board can still be taken before boarding is closed.

In addition, the EU legislator should establish that in the case of airport transit, the airline should not be obliged to verify whether the passenger is in possession of a valid short-stay visa (except for those third-country nationals who are required to hold an airport transit visa according to Annex IV of the Visa Code).

FRA Opinion 18

The obligation to verify the passport details of each passenger against VIS disproportionately affects the freedom to conduct a business of small carriers who operate bus connections or small ferry connections over the Schengen border. In such cases, the person could be checked when he or she reaches the border, where border guards have access to the relevant IT systems.

The EU legislator should revise the wording of Article 45c of the proposed amendments to the VIS Regulation to allow the European Commission to exempt small carriers from the duty of querying VIS by implementing acts.

FRA Opinion 19

The principle of proportionality enshrined in Article 52 (1) of the Charter, as interpreted by the Court of Justice of the EU, requires that access to personal data for law enforcement purposes is subject to adequate safeguards and that the retention of the data reflects its law enforcement relevance.

The EU legislator should ensure that any solution for allowing access to EU IT systems by law enforcement for the purposes of fighting terrorism and serious crime requires the authorities to first consult databases more directly linked to criminal investigations, similarly to the mechanism in place for the Entry/Exit System. More specifically, this would mean:

- ***conduct a prior search in relevant national databases, and***
- ***in case of searches with fingerprints, at least launching a prior search in the automated fingerprint identification system of the other EU Member States under Council Decision 2008/615/JHA (Prüm Decision).***

The EU legislator should allow law enforcement access to children's data, particularly those below the age of criminal responsibility, only to protect missing children or children who are victims of serious crimes (e.g. trafficking in human beings);

The EU legislator should align the slightly different wording of the safeguards in case of Europol's designated central access point (proposed Article 22l (2)) with the set of criteria applicable to national central access points (proposed Article 22k (3)), except for the requirement of separateness. This would mean inserting the word "fully" into the phrase "shall act independently", and adding the following half-sentence at the end of Article 22l (2): "which it shall perform independently".

FRA Opinion 20

Enabling law enforcement access to VIS to identify persons who have gone missing, been abducted or are victims of trafficking in human beings has beneficial effects to protect the legitimate interests of such vulnerable people. However, the modalities of such a "barrier-free" and simplified access for law enforcement authorities to VIS data need to be sufficiently detailed and contain built-in safeguards. These are needed to prevent that such simplified access is used to circumvent the requirements which need to be fulfilled when VIS is accessed to prevent, detect and investigate terrorist offences or other serious crimes.

Therefore, the EU legislator should

- ***align the formulation of the new objective in proposed Article 2 (1) (f) of the VIS Regulation with the persons covered by proposed Article 22o and complement Article 2 (2) with a new specific objective of identifying this group of vulnerable people;***
- ***remove the wording "and/or contribute in investigating specific cases of human trafficking" from proposed Article 22o, as it conflicts with the general rules of law enforcement access to investigate terrorism and other serious crimes (proposed Articles 22m-22n).***

FRA Opinion 21

The production of reliable statistics supports evidence-based policy decisions. The data used to produce reports and statistics, however, must not allow direct or indirect identification of the data subjects. Data categories to include in the Central Repository for Reporting and Statistics (CRRS) must be defined in a clear manner.

The EU legislator should consider enhancing safeguards to Article 45 (a) to prevent that data stored in the CRRS may lead to identification of data subjects. The safeguards should include:

- ***in Article 45a (1) (c), replacing the reference to "data of birth" with "year of birth" and complementing this provision with a safeguard according to which "this should not lead to the identification of the person concerned";***
- ***in Article 45a (1) (i) and Article 45a (1) (j), replacing "the location" of the competent authority with "the country" of the competent authority.***

For reasons of legal clarity, the EU legislator should also:

- ***clarify the term "document" in Article 45 (1) (h) and (l) or replace it with more specific wording;***
- ***include in Article 7 of the proposal an amendment to Article 39 (2) of the interoperability proposal (borders and visa) clarifying that data listed in proposed Article 45a (1) of the VIS Regulation should be contained in the CRRS.***

FRA Opinion 22

Article 50 regulates the monitoring and evaluation of the VIS Regulation but does not include an express duty to evaluate also how the implementation of the regulation will affect fundamental rights, in spite of the fact that this is announced in the Explanatory Memorandum. Moreover, the indicators listed in Article 50 (4) could be further

developed so that these could be used more effectively to evaluate the impact of law enforcement access on fundamental rights.

The EU legislator should add in Article 50 (5) of the VIS Regulation an explicit reference to "the impact on fundamental rights". Such reference could expressly mention that the evaluation should "in particular cover the right to protection of personal data, the right to non-discrimination, the rights of the child and the right to an effective remedy". Moreover, the evaluation should also examine whether law enforcement access to VIS has led to indirect discrimination against persons covered by the regulation.

In Article 50 (4), the EU legislator should:

- ***include a reference similar to the wording in Article 72 (8) (f) of the EES Regulation to "the number and type of cases in which the urgency procedures referred to in Article 22m (2) were used, including those cases where that urgency was not accepted by the ex post verification carried out by the central access point";***
- ***consider requesting EU Member States and Europol to present separate statistics on child trafficking under Article 50 (4) (a) and to specify under Article 50 (4) (b) and (c) how many of the cases concern persons below 18 years of age. Under Article 50 (4) (c), the EU legislator should furthermore consider adding the words "with a breakdown of granted and rejected requests".***

FRA Opinion 23

The manual verification of hits obtained after the automatic European Search Portal query is a welcome step to avoid automated decision making. The current provision does, however, not provide for any time limit for the manual verification. An appropriate time limit could help to ensure speedy procedures across EU Member States.

When assessing entry conditions, consulates will have to take into account the results from the manual verification and consider specific information contained in the connected IT databases. Regarding Eurodac, the information is not relevant to assess the entry conditions and could undermine the right to asylum enshrined in Article 18 of the Charter. The information requested from ECRIS-TCN will not be available in the IT system itself.

The EU legislator should include a time limit for the manual verification procedure in Article 9c of the VIS Regulation to ensure speedy processing of visa applications.

The EU legislator should amend proposed Article 21 (3a) of the Visa Code by:

- ***deleting proposed point (e) relating to Eurodac,***
- ***finding an appropriate solution so as to ensure that the relevant authorities examining a visa application can only see ECRIS-TCN hits which concern a terrorist offence or another serious crime and not entries which concern less serious crimes.***

FRA Opinion 24

Proposed Article 21a of the Visa Code introduces specific risk indicators that visa authorities should use when assessing whether or not the applicant presents an irregular immigration, security or high epidemic risk. Although safeguards will have to be applied

when using these specific risk indicators, certain risks for discrimination or unequal treatment, both prohibited by the Charter, exist.

To comply with Articles 20 and 21 of the Charter guaranteeing equality before the law and non-discrimination, the EU legislator should add the word "predominantly" in proposed Article 21a (4) of the Visa Code.

The EU legislator should delete point (f) in proposed Article 21a (3) of the Visa Code and thereby remove "current occupation" from the specific risk indicators due to the high risk it might lead to indirect discrimination.

The EU legislator should include a new provision in Article 21 of the Visa Code, expressly stating that every application must always be subject to an individual assessment based on all available information.

Introduction

This Opinion by the European Union Agency for Fundamental Rights (FRA) aims to inform the European Parliament's position on the legislative proposal amending the Visa Information System, the Visa Code and other related provisions of EU law. The European Commission presented the proposal on 16 May 2018 and EU legislators are currently discussing it.[7] Throughout the text, this opinion refers to the proposed amendments using the wording "the proposal" or "the Commission proposal".

The Visa Information System – generally referred to as VIS – is one of the EU's large-scale information technology systems (IT systems). It was established to facilitate the application procedure for Schengen visas (meaning short-stay visas for up to 90 days in a period of 180 days), although it also serves ancillary asylum, immigration control and security related purposes.

After the initial Council decision establishing VIS in 2004 (Decision 2004/512/EC[8]), the modalities of its functioning and the exchange of data between Member States on short-stay visas were determined in 2008 by Regulation (EC) No. 767/2008.[9] VIS was rolled-out worldwide only in November 2015.[10] By January 2018, data on more than 52 million Schengen visa applications, with over 52 million photographs and almost 50 million fingerprints were entered in VIS.[11] The proposal intends to change significantly the personal scope of VIS – which is currently limited to short-term visitors. In future, it should also include all third-country nationals who live in the EU with a residence permit or a long-stay visa. A Commission study projected that this would mean storing data, including biometric data, of over 20 million additional people (future holders of these documents for long-stay).[12] Many of them have their centre of life in the EU, where they are residing on a permanent basis.

Significant amendments are also proposed to the Visa Code (Regulation (EC) No. 810/2009) which establishes the procedures for examining applications for short-stay visa.

From a fundamental rights point of view, the most important changes of the proposal concern:

---

7 European Commission (2018), *Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No. 767/2008, Regulation (EC) No. 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA*, COM(2018) 302 final, Brussels, 16 May 2018 (*Commission proposal*).

8 Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213/5.

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

10 Commission Implementing Decision (EU) 2015/912 of 12 June 2015 determining the date from which the Visa Information System (VIS) is to start operations in the 21st, 22nd and 23rd regions, OJ L 148/28.

11 European Commission (2018), *Commission Staff Working Document – Impact Assessment – Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No. 767/2008, Regulation (EC) No. 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA*, SWD(2018) 195 final, Brussels, 16 May 2018 (*Commission proposal, Impact Assessment*), p. 5.

12 See Commission proposal, Impact Assessment, p. 49, fn. 118 as well as European Commission, DG Migration and Home Affairs (2017), Integrated Border Management (IBM), *Feasibility Study to include in a repository documents for Long-Stay visas, Residence and Local Border Traffic Permits*, Phase1: Analysis of Options, Final Report (version 6.0), September 2017.

- the plan to extend the personal scope of VIS to include also holders of long-stay visas and residence permits;
- the processing of facial images for biometric matching in VIS;
- the plan to process biometric data of children, including fingerprints as of the age of six years;
- the enhanced use of automated checks between IT systems;
- access to VIS data by carriers;
- the use of VIS data for reporting and statistics;
- new rules on access to VIS for law enforcement purposes; and
- the development of risk indicators to assess visa applications.

The main fundamental rights concern analysed in this opinion is the inclusion of residence permit holders in VIS. In essence, FRA believes that, although it may pursue a legitimate aim, the processing of data of residence permit holders in VIS, particularly those holding long-term residence, is not necessary and proportionate. The opinion encourages the EU legislator to explore alternative ways to address the aim pursued.

Concerning biometric data, the proposal continues the trend of complementing the processing of fingerprints with the processing of facial images, upgrading VIS to allow for biometric matching based on facial images of everyone, including very young children. In addition to the specific points raised in this FRA Opinion, FRA would also like to recall that the processing of facial images in large-scale IT systems may, as face-recognition technology develops, raise unchartered issues about the rights to protection of private and family life, and the right to protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: 'the Charter').[13]

The proposal tabled by the European Commission also responds to fundamental rights concerns identified in the past. Whereas this occurs at different instances throughout the proposal, efforts to address fundamental rights gaps are particularly important in two areas, namely data quality and child protection.

First, proposed changes to Article 29 and new Article 29a of the VIS Regulation include important provisions to enhance the quality of data processed in VIS. This responds to one of the main issues FRA identified in its March 2018 report "*Under watchful eyes: biometrics, EU IT systems and fundamental rights*" (see in particular the findings described in Section 4.2).

Second, the proposal gives considerable attention to the protection of the rights of the child, as the following examples illustrate. Proposed Recital (9) underlines that the best interests of the child must be a primary consideration in all procedures falling under the scope of the proposal. A new provision guaranteeing the best interests of the child is added to Article 7 of the VIS Regulation, which would also require that the child's well-being, safety and security, and the child's views are taken into account when implementing the regulation. New Article 2 (1) (f) of the VIS Regulation allows processing of VIS data to identify missing persons (adults as well as children). Proposed Article 20a of the VIS Regulation enables authorities to use fingerprints stored in VIS to enter alerts on missing persons in the Schengen Information System (SIS) in accordance with Article 32 (2) of the SIS proposal on police and judicial cooperation. Additionally, under proposed Article 20a (2) of the VIS Regulation,

[13] See for more details, FRA *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018, p. 12.

national child protection and judicial authorities may request access to VIS data, if there is a hit against a SIS alert on missing persons.[14]

This FRA Opinion contains 24 individual opinions which relate to various fundamental rights enshrined in the Charter. Central to this FRA Opinion is 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). The processing of personal data in VIS constitutes a limitation of these rights. 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.

In addition, this opinion also touches upon the following rights, namely:

- the right to the integrity of the person (Article 3 of the Charter);
- the prohibition of trafficking in human beings (Article 5 of the Charter);
- freedom to conduct a business (Article 16 of the Charter);
- the right to asylum guaranteed in Article 18 of the Charter;
- the protection in the event of removal, expulsion or extradition (Article 19 of the Charter);
- equality before the law (Article 20 of the Charter);
- non-discrimination (Article 21 of the Charter);
- the rights of the child (Article 24 of the Charter);
- freedom of movement and of residence (Article 45 of the Charter);
- the right to an effective remedy and to fair trial (Article 47 of the Charter).

The FRA Opinion should be read in conjunction with the opinion that the European Data Protection Supervisor (EDPS) will submit.

[14] Commission proposal, Art. 1 (19) [introducing Art. 20a (2) in the VIS Regulation].

1. Adding a general fundamental rights safeguard clause

This first chapter of the FRA Opinion deals with the need for a general fundamental rights safeguard clause in the VIS Regulation and proposes amendments to the non-discrimination grounds already included in the VIS Regulation and the Visa Code.[15]

The current VIS Regulation does not include a general fundamental rights clause in its operative part. Recital (24) says that the VIS Regulation respects the fundamental rights and principles recognised in particular by the EU Charter of Fundamental Rights. A similar provision is contained in Recital (29) of the Visa Code, which also includes an explicit reference to the European Convention on Human Rights (ECHR).

Pursuant to Article 7 (2) of the VIS Regulation and Article 39 (2) of the Visa Code, the authorities implementing the respective regulations must fully respect the human dignity of the person concerned. Moreover, under Article 13 (1) of the Visa Code, when Member States are collecting biometric identifiers of visa applicants, they must respect the safeguards included in the Charter, the ECHR and the UN Convention on the Rights of the Child.[16]

While acknowledging the importance of these clauses, it should be noted that VIS will affect several other fundamental rights protected by the Charter, such as the right to respect for private and family life (Article 7), the right to protection of personal data (Article 8), the right to asylum (Article 18), the principle of equality before the law (Article 20), the right to non-discrimination (Article 21), the rights of the child (Article 24), and the right to an effective remedy (Article 47). A general fundamental rights clause in the operative part of the VIS Regulation would promote a more comprehensive fundamental rights compliant implementation of the regulation in practice. Such a clause is, for example, included in Article 14 of the compromise text of the European Travel Information and Authorisation System (ETIAS) Regulation (ETIAS compromise text).[17]

The proposal gives increased attention to fundamental rights. It amends Article 7 of the VIS Regulation by including a new paragraph on the rights of the child and includes a more detailed list of fundamental rights affected by the proposal in Recital (47). Such Recital expressly refers to the "right to human dignity, the right to liberty and security, the respect for private and family life, the protection of personal data, the right to asylum and protection of the principle of *non-refoulement* and protection in the event of removal, expulsion or extradition, the right to non-discrimination, the rights of the

---

15 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 (*Visa Code*).

16 United Nations (UN), Convention on the Rights of the Child, 20 November 1989.

17 Council of the European Union (2018), *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 and (EU) 2016/1624 – Outcome of the European Parliament's first reading (Strasbourg, 2 to 5 July 2018)*, 2016/0357/A(COD), Brussels, 12 July 2018 (*ETIAS compromise* text). See also Art. 10 (2) of 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*), which stipulates that: "Each competent authority shall ensure that the use of the EES, including the capturing of biometric data, is in accordance with the safeguards laid down in the Convention for the Protection of Human Rights and Fundamental Freedoms, in the Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child. In particular, when capturing a child's data, the best interests of the child shall be a primary consideration."

child and the right to an effective remedy". This provision remains, however, in a Recital in the preamble and does not underline the obligation of Member States to implement the Regulation in full compliance with relevant fundamental rights. Moreover, only the provisions contained in the proposal have to be read in the light of the Recital and not the underlying legal acts as a whole.

Articles 20 and 21 of the Charter guarantee equal treatment and freedom from discrimination. Pursuant to Recital (12) and Article 7 (2) of the VIS Regulation, as well as Article 39 (3) of the Visa Code, authorities must not discriminate against the person concerned on grounds of "sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation". The respective provisions do, however, not address other grounds prohibited by Article 21 of the Charter, namely colour, social origin, genetic features, language, political or any other opinion, membership of a national minority, property and birth. While all these grounds must be respected in the context of VIS, an exhaustive non-discrimination provision could help to ensure a Charter compliant implementation of the VIS Regulation and the Visa Code. This approach was followed also in the EES Regulation and the ETIAS compromise text.[18]

FRA Opinion 1

The implementation of the VIS Regulation may affect several fundamental rights, as listed in proposed Recital (47). However, the operative part of the regulation only contains provisions reminding Member State authorities to implement the VIS Regulation in a non-discriminatory manner and fully respecting human dignity and integrity of the person. The proposal will also add a provision on the rights of the child. A comprehensive fundamental rights clause is only contained in the Recitals of the VIS Regulation and of the proposal.

One of the fundamental rights protected by the Charter is the right to non-discrimination, which is presently reflected in the VIS Regulation and in the Visa Code. However, both legislative acts prohibit discrimination only on limited grounds.

To promote a fundamental rights compliant implementation of VIS, the EU legislator should include a general fundamental rights safeguard clause in the operative part of the VIS Regulation, for example in Article 7, drawing upon the language used in Recital (47) of the proposal and in Article 14 of the compromise text of the European Travel Information and Authorisation System Regulation (ETIAS compromise text). Such clause should re-affirm Member States' obligation to implement the regulation in full compliance with the Charter. It should contain a specific provision on child protection as suggested by amended Article 7 (3) of the proposal.

Furthermore, the EU legislator should amend Article 7 (2) of the VIS Regulation and Article 39 (3) of the Visa Code by including all other discrimination grounds prohibited by Article 21 of the Charter, namely "colour, social origin, genetic features, language, political or any other opinion, membership of a national minority, property and birth".

[18] EES Regulation, Recital (19); ETIAS compromise text, Art. 14.

2. Necessity and proportionality of processing data of residence permits holders

This chapter analyses the fundamental rights implications of the significant expansion of the personal scope – meaning the categories of persons whose data will be stored – of the VIS Regulation to cover long-stay visa and residence permits holders. The proposal amends Articles 1 and 2 of the VIS Regulation changing its scope and purpose and introduces a new Chapter IIIa on entry and use of data on long-stay visas and residence permits.

Currently, VIS processes personal data of third-country nationals coming to the EU for short-term stay who need a visa. In future, it would also store personal data of all third-country nationals (including nationals from countries who do not need a visa for short-stay visits) coming for longer-term stay as well as those residing in the EU. This would transform VIS into a system storing data of virtually all third-country nationals who applied for a visa or a residence permit in one of the Member States. The name "VIS", indicating that it is a system for short-term visitors, would not appear appropriate anymore. In fact, it would appear that VIS has been chosen to store data on long-stay visa and residence permits holders, as this is the easiest and cheapest technical solution.[19]

Whereas conditions for issuing short-stay visas (Schengen visas) are determined in a uniform manner in the Visa Code (Regulation (EC) No. 810/2009), the conditions to issue a long-stay visa or a residence permit are within Member State competence and not laid down in EU law, except for certain EU-harmonised purposes of stay.[20] However, the format of residence permits issued by Member States is harmonised and includes biometric identifiers.[21] Long-stay visas also have to be issued in an EU-harmonised uniform format with enhanced security features, but do not include biometric data.[22]

---

19 Commission proposal, Impact Assessment, p. 62.

20 See, for example, Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification, OJ L 251/12; Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents, OJ L 16/44; Council Directive 2009/50/EC of 25 May 2009 on the conditions of entry and residence of third-country nationals for the purposes of highly qualified employment, OJ L 155/17; Directive 2011/98/EU of the European Parliament and of the Council of 13 December 2011 on a single application procedure for a single permit for third-country nationals to reside and work in the territory of a Member State and on a common set of rights for third-country workers legally residing in a Member State, OJ L 343/1; Directive 2014/36/EU of the European Parliament and of the Council of 26 February 2014 on the conditions of entry and stay of third-country nationals for the purpose of employment as seasonal workers, OJ L 94/375; Directive 2014/66/EU of the European Parliament and of the Council of 15 May 2014 on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer, OJ L 157/1; and Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing, OJ L 132/21.

21 Council Regulation (EC) No. 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals, OJ L 157/1 as amended by Regulation (EC) No. 380/2008 of 18 April 2008, OJ L 115/1, and Regulation (EU) 2017/1954 of 25 October 2017, OJ L 286/ 9.

22 Regulation (EU) No. 265/2010 of the European Parliament and of the Council of 25 March 2010 amending the Convention Implementing the Schengen Agreement and Regulation (EC) No. 562/2006 as regards movement of persons with a long-stay visa, OJ L 85/1, Art. 1 (1), which replaced Art. 18 of the CISA. The security features of such visa stickers are specified in Council Regulation (EC) No. 1683/95 of 29 May 1995 laying down a uniform format for visas, OJ L 164/1, as amended by Regulation (EC) No. 856/2008 of 24 July 2008, OJ L 235/1, and Regulation (EU) 2017/1370 of 4 July 2017.

2.1. Exploring less intrusive options

The rationale of processing personal data of long-stay visa and residence permit holders in VIS is set out in proposed amendments to Article 2 of the VIS Regulation, which list five different purposes of processing. In simplified terms, under Article 2 (2) these include processing (i) to vet applicants before they are allowed to come to the EU; (ii) to improve the effectiveness of border management and asylum procedures; (iii) to enhance the effectiveness of checks on persons carried out within the territory; (iv) to enhance internal security; and (v) to ensure a correct identification of the person concerned.

According to the European Commission's impact assessment, including long-stay visa and residence permit holders in an EU wide information system would help the authorities to better deal with individuals who are trying to deceive the authorities (for example, by using false documents to cross the border) and would reduce the administrative burden resulting from bilateral consultations between Member States by border guards and police when dealing with problematic or suspicious cases.[23]

The processing of personal data in VIS constitutes a limitation of the right to respect for private and family life and of the right to protection of personal data enshrined in Articles 7 and 8 of the Charter. 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.[24]

A study conducted for the European Commission concluded that it would be necessary and proportionate to process personal data of long-stay visa and residence permit holders in an EU-wide system.[25] The study provides a thorough analysis from a border control and migration management perspective. However, the analysis does not sufficiently differentiate between the different categories of third-country nationals affected, which range from persons coming to the EU for relatively short visit (e.g. a six months study visit or a traineeship) to individuals who were born in the EU or have their centre of life here.

To understand the implications of the expansion of the personal scope of VIS, a closer look at the categories of persons which would be affected is needed. Figure 1 illustrates the category of third-country nationals which VIS includes now and those that it would include in future.

---

[23] Commission proposal, Impact Assessment, pp. 58-60, 110, 111.

[24] As reiterated and further explained by the CJEU, see for example, CJEU, C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 December 2015, paras. 69 and 80-82.

[25] European Commission, Directorate-General for Migration and Home Affairs, *Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long-stay visas and residence documents*, Luxembourg, Publications Office of the European Union, March 2018.

Figure 1: Categories of persons included in VIS

Notes: *Categories currently included in VIS*

Categories planned for inclusion in VIS under the proposal

TCN -Third-country nationals

Source: FRA, 2018

When assessing the impact of the proposal on the third-country nationals concerned, a distinction must be made between persons coming to the EU temporarily and those who reside in the EU on a long-term basis. The characteristics of those residing and living in the EU on a long-term or permanent basis are significantly different from tourists, students, researchers or business travellers who come to the EU only for a short visit or temporary stay. The situation of long-term residents is, generally speaking, closer to that of EU citizens than that of short-term visitors.

By assimilating residence permit holders with visa applicants, the proposal risks to reinforce a "we" versus "them" approach and goes against the idea of an inclusive society conducive to integrating third-country nationals living in the EU. It can also be argued that this is inconsistent with the purpose of Council Directive 2003/109/EC of 23 November 2003 concerning the status of third-country nationals who are long-terms residents (Long-Term Residents Directive). The directive, in its Recital (4), explicitly states that: "[t]he integration of third-country nationals who are long-term residents in the Member States is a key element in promoting economic and social cohesion, a fundamental objective of the [Union] stated in the Treaty". With some restrictions, the Long-Term Residents Directive grants rights, which are almost identical to those enjoyed by EU citizens, to non-EU nationals legally residing in the EU Member States.[26] It can be argued that including long-term residents in a data system that is conceived for short-term stayers can foster sentiments of exclusion.

Long-stay visas are issued at diplomatic or consular representations. Under Regulation (EU) No. 265/2010, such visas can have a maximum validity of one year. Pursuant to Article 1 (1) of this Regulation, if the right to stay is extended, "the long-stay visa shall be replaced before the expiry of its period of validity *by a residence permit*" [*italics added*]. Residence permits can be issued either at diplomatic or consular representations before the person concerned travels to the EU or by authorities within the EU (for example, residence permits issued to beneficiaries of international protection). Some Member States assess the application for the residence permit at the diplomatic or consular representation, but then issue first a short-stay visa or a visa with limited territorial validity allowing the person to travel to the EU Member State in question where the residence permit is consequently issued.

A residence permit may be temporary, e.g. not exceeding the period of validity of a long-stay visa or valid for a limited number of years, or it may be long-term. Therefore,

[26] Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents, OJ L 16/44; European Commission, Migration and Home Affairs, *Long-term residents*, last updated on 26 July 2018.

the ties residence permit holders have with the EU can differ significantly, ranging from persons who come for a visit for little more than three months to individuals who were born and lived all their life in the EU.

Overall, in 2016 (the year for which the most recent Eurostat statistics are available), there were more than 20 million third-country nationals in the EU-28, representing 4.1 % of the total EU population.[27] Also, in 2016, there were 19 million valid residence permits in the EU-28, the overwhelming majority of which were valid for more than 12 months (92 %).[28]

Approximately two out of three residence permit holders have a long-term permit: Out of the 19 million valid residence permits holder, around 12 million third-country nationals held long-term residence in the EU in 2016.[29] Long-term residents have typically strong links with their EU Member State of residence.

Furthermore, many holders of residence permits were born in the European Union – according to the Labour Force Survey, there were over 850,000 native-born third-country nationals in the EU in 2014. The numbers are particularly high in Germany at approximately 545,000, but also in Latvia (84,000), Estonia (66,000), Spain (50,000), Austria and Italy (32,000 each).[30] These figures cover the population aged 15 to 64, thus the actual numbers are considered to be higher, as illustrated also by statistics compiled at a national level. For example, in 2017, in Germany, 817,000 persons or 13.8 % of the 6 million third-country nationals residing there were born in Germany.[31] In Austria, almost 100,000 or approximately 15.5 % of the 646,200 third-country nationals living in Austria in 2017 were born there.[32]

The expansion of the personal scope of VIS to include holders of long-stay visas and residence permits responds to the need to "fill the current information gaps for border management and law enforcement" (Recital (5) of the proposal). As illustrated in Figure 2, third-country nationals who reside in the EU and who come for a long stay are the only category of third-country nationals whose data are not stored in an EU-wide information system. With the changes proposed to VIS, virtually all non-nationals staying in the EU Member States, except EU citizens and nationals of the European Economic Area and Switzerland will be stored in an EU-wide information system.

---

27 Eurostat, *Population on 1 January by age group, sex and citizenship,* data extracted on 10 July 2018.

28 Eurostat, *All valid permits by reason, length of validity and citizenship on 31 December of each year*, data extracted on 10 July 2018.

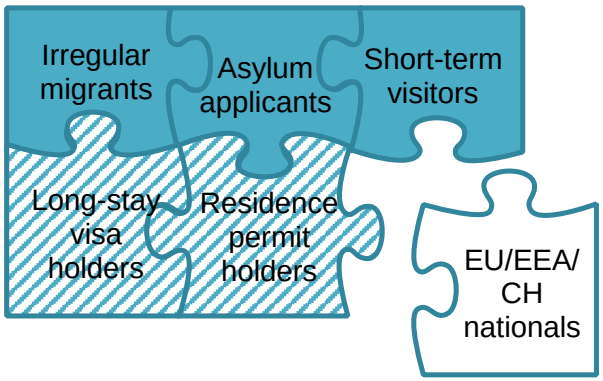
29 Eurostat, *Long-term residents by citizenship on 31 December of each year*, data extracted on 10 July 2018. It is worth noticing that slightly less than 3 million of long-term residence permit holders hold a long term residence status according to the EU Long-Term Residents Directive (the remaining ones are national definition long term residence holders). Furthermore, other third-country nationals may be living in the EU on a long-term basis but without having been granted a long-term residence permit.

30 Eurostat, *Population by sex, age, migration status and citizenship*, data extracted on 12 July 2018. Native born third-country nationals include native born persons with mixed and foreign background and with native background who are non-EU-28 citizens.

31 Germany, Federal Statistical Office (*Statistisches Bundesamt*), *Bevölkerung und Erwerbstätigkeit, Ausländische Bevölkerung, Ergebnisse des Ausländerzentralregister*, 12 April 2018, p. 152. The number is much higher than the above mentioned Eurostat number, most probably since it does not include any age limitations (see p. 35 onwards).

32 Austria, *Statistik Austria*, *Bevölkerung mit Migrationshintergrund im Überblick (Jahresdurchschnitt 2017)*, as last changed on 20 June 2018.

Figure 2: People in the EU with data stored in an EU-wide information system



Notes: *EU-wide storage*
Planned EU-wide storage
No EU-wide storage planned

EEA: European Economic Area
CH: Switzerland

Source: FRA, 2018

In reality, data on holders of long-stay visas and residence permits may already feature in existing or future EU systems. Data on residence permit holders who were granted asylum are stored in Eurodac for a period of up to 10 years.[33] Persons who are issued a residence permit inside the EU after having entered the Schengen area with a short-stay visa or as visa-free travellers will be in the Entry/Exit System (EES) as well as VIS or ETIAS depending on whether they come from a visa-free country or not. Finally, some persons holding a long-stay visa or a residence permit may be in the Schengen Information System (SIS) if they in the past have been issued an alert for criminal or judicial purpose, an entry ban, or a refusal of entry at the border.

The aim of ascertaining that the bearer is the genuine holder of a resident permit and that the permit has not been tampered with does not necessitate the inclusion of holders of residence permits in VIS. This objective can to a considerable extent be achieved by enhancing the "one-to-one verification" between document and bearer, followed by usual checks in IT-systems, expected to be additionally enhanced through interoperability. All residence permits – and in future also residence cards of third-country national family members enjoying free movement rights[34] – store biometric data. During a second line check the two fingerprints stored in the chip can be used to verify the identity of the bearer. To achieve this, the "Country Verifying Certificate Authorities" (CVCA) would need to be systematically exchanged between Member States, which they are not.[35] In addition, through so called "passive authentication" the border guard can check that the data on the chip was written by the official issuing authority and that this data has not been altered afterwards. Passive authentication relies on Member States' authorities exchanging their public keys (the so called cryptographic certificates) for the verification of the document. According to the

[33] Eurodac Regulation, Art. 12 (1).

[34] European Commission (2018), *Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement*, COM(2018) 212 final – 2018/0104 (COD), Brussels, 17 April 2018.

[35] European Commission (2018), *Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents*, Final report, 29 June 2018, pp. 42, 53.

European Commission study, EU Member States do exchange these,[36] but only five Member States, out of 16 that answered, perform such passive authentication, mainly due to additional work this entails.[37] Gaps in cooperation between Member States and the limited use of currently existing possibilities to enhance border checks should not be used to legitimise the expansion of VIS to all residence permit holders.

Considering that the proposal implies storing data of some additional 20 million people, 12 million of whom are long-term residents with close ties to a Member State, it is questionable if the inclusion of personal data of all residence permit holders, including sensitive biometric data, in VIS, is necessary and proportionate. It is particularly hard to justify the creation of a repository of third-country nationals applying for a residence permit from inside the EU. In case the permit is issued for protection reasons data on the holders are already included in Eurodac and if the person first entered the EU on a short-term basis, his or her data will be in the EES (in addition to ETIAS or VIS, depending if the third-country national is from a visa-free country or not). If the third-country national was born inside the EU, his/her situation is very similar to that of an EU national and the creation of an individual file in VIS would not be justified.

Taking these reasons together with the issue of open-ended retention explained in Section 2.2, the processing of personal data of individuals who are staying in the EU on a long-term basis in VIS does not appear to be necessary and proportionate.

However, what could be conceived is a mechanism to store the personal data in VIS of all those third-country nationals who enter the EU with a long-stay visa or a residence permit for the first time. Taking such an approach would result in storing personal data, including sensitive biometric data, for a smaller group of persons, compared to the proposal.

The category of persons Member States have less information about is those who enter the EU for the first time. Member States would, normally, have extensive information on third-country nationals already living in the EU with a residence permit. In addition, in some cases, their personal data would still be stored Eurodac (for international protection beneficiaries) or in the EES (as well as VIS or ETIAS), if they first entered the EU for short-term stay. When there is no information on them in an existing EU IT system, Member States could still request information on residence permit holders through bilateral cooperation.

One way to achieve this could be to store in VIS only short-stay and long-stay visas, combined with a duty for Member States to issue a visa (either for short or for long-stay) to those third-country nationals who currently enter the EU with a residence permit issued at diplomatic or consular representations.

By taking an approach which stores data of fewer people, it appears, to a considerable extent, possible to achieve the objective envisaged by the proposal through a less intrusive option. The limitations to the right to respect for private and family life and to the right to protection of personal data would be easier to justify if such a solution would be chosen.

---

[36] European Commission (2018), *Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents,* Final report, 29 June 2018, Figure 11 on p. 95.

[37] European Commission (2018), *Legal analysis on the necessity and proportionality of extending the scope of the Visa Information System (VIS) to include data on long stay visas and residence documents,* Final report, 29 June 2018, pp. 26, 95.

FRA Opinion 2

The EU-wide storage of personal data, including biometrics, of all third-country nationals holding a residence permit issued by a Member State, including long-term residents, does not meet the necessity and proportionality requirements under the Charter. A mechanism to store the personal data in VIS only of those third-country nationals who enter the EU with a long-stay visa or a residence permit for the first time would store data of fewer people, and thus be less intrusive on fundamental rights, although the necessity and proportionality of such data processing would still need to be shown.

The EU legislator should refrain from adding residence permit holders to VIS, thereby limiting the expansion of the personal scope of VIS to long-stay visas, and amend the relevant parts of the proposal accordingly.

Should the EU legislator consider it necessary to include certain categories of residence permit holders in an EU-wide information system, this should be limited to those individuals who are entering the EU with a residence permit for the first time. To achieve this, the EU legislator could explore the feasibility of amending the Visa Code or other relevant EU legislation to oblige EU Member States to issue a short-stay or long-stay visa for the first entry of persons to whom they granted a residence permit.

2.2. Avoiding open-ended data retention

The proposal suggests introducing new rules on data retention. Proposed changes to Article 23 (1) of the VIS Regulation envisage that the files be kept in VIS for a maximum of five years from the date of expiry, refusal, withdrawal or revocation of a short-stay visa, a long-stay visa or a residence permit.

Pursuant to proposed Article 23 (1) (b) of the VIS Regulation, every time a short-stay visa, a long-stay visa or a residence permit is extended, a new retention time of five years will start to apply. In practice, this means that holders of a long-term residence permit will have their data stored in VIS for an unlimited period of time, as their residence permits will be automatically renewed upon expiry.[38] Their data will only be erased from VIS if they acquire the nationality of an EU Member State (Article 25 (1) of the VIS Regulation), which, for a variety of reasons, does not necessarily happen in case of long-term residents.

The jurisprudence of the ECtHR requires data retention to be limited in time.[39] For example, in *S. and Marper*, the ECtHR ruled that indefinite retention of fingerprints, cellular samples and DNA profiles of the two applicants was disproportionate and unnecessary in a democratic society.[40] Article 5 (1) (e) of the General Data Protection Regulation (Regulation (EU) 2016/679 – hereinafter: "GDPR") stipulates that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". Under the EU general data protection rules, this requires, in particular, "ensuring that the period for which the personal data are stored is limited to a strict minimum [and that]

---

[38] See, for example, Art. 8 (2) of Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents, OJ L 16/44.

[39] ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, para. 99; ECtHR, *M.M. v. the United Kingdom*, No. 24029/07, 13 November 2012, para. 195.

[40] ECtHR, *S. and Marper v. the United Kingdom* [GC], Nos. 30562/04 and 30566/04, 4 December 2008, para. 125.

time limits should be established [...] for erasure or for periodic review"[41] to make sure that the data are kept for no longer than is necessary. As a result, open-ended data retention periods are not lawful under EU law.

The individual VIS file also contains links to previous applications by the person (Article 8 (3) of the VIS Regulation), as well as between applications of family members and other persons travelling together (Article 8 (4) and proposed Article 22a (3) of the VIS Regulation). Pursuant to proposed Article 23 (2), the links to a VIS file will be automatically erased when the retention time expires. However, in case the linked VIS files are kept beyond five years, which could occur when residence permits are extended, also these links would remain active. Keeping links with persons travelling in the same group who are not family members for more than five years does not appear to be justified. For example, two third-country nationals who arrived in a group of seasonal workers with a long-term visa and who later received a residence permit for different reasons would continue to be connected in VIS, as long as their permit gets extended. In case one of them commits a crime or overstays, this could possibly create a bias in the way the other is treated when authorities access VIS.

In proposed Article 23 (2), a reference is made to Article 22a (5), but this provision does not appear to exist.

FRA Opinion 3

As pointed out in FRA Opinion 2, processing personal data of long-term residence permit holders in VIS is not necessary and proportionate. Their inclusion in VIS would, in practice, result in an open-ended retention of their personal data, as residence permits get extended. In such cases, also links to applications of other members of a group travelling together, not being family members, could in practice be retained beyond five years. This would not be justified, unless specific criminal investigations are ongoing.

As pointed out in FRA Opinion 2, the personal data of long-term residence permit holders should not be processed in VIS. This would avoid that data of long-term residence permit holders are, in practice, retained forever. In case the EU legislator would, nevertheless, decide to retain individual files on residence permit holders in VIS, a solution must be found to avoid that data (including links to other applications) stored in individual files is retained beyond five years, unless the retention is necessary for specific ongoing criminal investigations.

The incorrect cross-reference to Article 22a (5) should be deleted from proposed Article 23 (2).

2.3. Addressing risks created by stored data about the sponsor

Pursuant to proposed Article 22a an individual file is created in VIS upon decision to issue or refuse an application for a long-stay visa or a residence permit. Proposed Article 22c lists the data which the file must contain if the visa or permit is issued and Article 22d the data which must be included if the visa or permit is refused for a number of specific reasons – namely, when the applicant was considered to pose a

[41] 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 L 119/1, (*GDPR*), Recital (39). See also, in this sense, Art. 23 (2) (f) of the GDPR ("In particular, any [EU or Member State] legislative measure [...] shall contain specific provisions at least, where relevant, as to [...] the storage periods...").

threat to public policy, internal security or public health, and when presented fraudulently acquired, falsified or tampered documents.

Under proposed Articles 22c and 22d, VIS will contain information about the sponsor, meaning the person or organisation that supports the visa applicant. When a residence permit is issued to a victim of crime perpetrated by the sponsor – as may be the case in situations of domestic violence pursuant to Article 59 of the Istanbul Convention[42] or to victims of trafficking in human beings on the basis of Directive 2004/81/EC[43] – there is no provision in the proposal which would de-link the individual from the sponsor. Maintaining such a link in VIS would result in the victim remaining associated with the criminal sponsor, exposing him or her to further security risks, including the risk of violations of the victim's right to physical integrity protected by Article 3 of the Charter and to trafficking in human beings prohibited by Article 5 of the Charter.

FRA Opinion 4

The storing of sponsor data in VIS under proposed Articles 22c may put victims of violent crimes perpetrated by the sponsor at risk.

The EU legislator should include a safeguard in proposed Article 22c for victims of violent crimes, such as domestic violence or trafficking in human beings, committed by their sponsor. In these cases, to protect the victim from further risks, the victim's file in VIS should be de-linked from the sponsor.

2.4.Reducing the risks for discriminatory checks within the territory

The proposed Article 22h (1) of the VIS Regulation envisages access to VIS data concerning long-stay visa holders and residence permit holders for checks within the territory. This reflects a similar provision included in Article 19 (1) of the VIS Regulation for short-stay visa holders. The main purpose of such checks is to verify the identity of the holder and whether the visa or the permit is genuine and valid.

Checks carried out on long-stay visa holders and residence permit holders may also be carried out for the purpose of verifying whether "the person is not a threat to public policy, internal security or public health of any of the Member States". This formulation provides broad powers to national police and immigration law enforcement authorities to consult VIS when a person is considered suspicious.

If the search indicates that VIS holds data on the person, the information which the officer querying VIS will see, will in itself not be enough to assess whether "the person is not a threat to public policy, internal security or public health of any of the Member States". The data in the individual file which the officer can access is limited to information indicating whether a long-stay visa or residence permit has been issued, withdrawn or extended as well as to information on the validity of the document, in addition to the picture of the person. The police officer will also have access to linked files of family members of other persons travelling in a group (proposed Article 22h (2)). The existence of a threat to public policy, internal security or public health could only be deduced through checks in other national or EU information systems.

---

[42] Council of Europe (2011), Convention on preventing and combating violence against women and domestic violence, CETS No. 210, 11 May 2011.

[43] Council Directive 2004/81/EC of 29 April 2004 on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration, who cooperate with the competent authorities, OJ L 261/19.

The broad powers given to national authorities to query VIS to verify whether "the person is not a threat to public policy, internal security or public health of any of the Member States" can easily be abused. The mere existence of a tool to check the status of "foreign-looking" persons in an easy manner may encourage immigration police to check any person or group of persons they find suspicious. This could lead to discriminatory police stops, based on race, colour or presumed ethnicity, which is prohibited under Article 21 of the Charter. When police stops entail deprivation of liberty (for example, when individuals stopped are brought to the police station for the VIS checks), other fundamental rights may be affected, including the right to liberty and security in Article 6 of the Charter.

This is even more the case, if the provision is viewed in light of the proposed Article 20 of the interoperability proposals on police checks, which gives wide powers to immigration and law enforcement authorities to check third-country nationals against all interoperable IT systems. FRA has highlighted the fundamental rights risks emerging from a lack of legal foreseeability of such provision as well as the risks for discriminatory profiling it entails.[44] Such risks are magnified should long-term residence permit holders be included in VIS.

FRA Opinion 5

The proposed Article 22h of the VIS Regulation will allow police and immigration law enforcement authorities to consult VIS data of long-stay visa and residence permit holders when they carry out checks within the territory. The purpose of such checks is formulated in a broad manner, providing police with broad powers that entail a risk of discriminatory police stops and of arbitrary deprivation of liberty.

The EU legislator should remove the wording "whether the person is not a threat to public policy, internal security or public health of any of the Member States" from Article 22h (1), as it entails a risk for discriminatory police stops and/or arbitrary deprivation of liberty.

[44] FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018, pp. 26-28.

3. Fundamental rights implications of expanded data processing

Chapter 3 examines the impact on fundamental rights of some of the new data categories that the proposal envisages to process in VIS for both groups of persons, namely short-stay visa applicants as well as long-stay visa and residence permit holders. It first examines the processing of facial images and the lowering of the fingerprinting age of children. It also reviews how the automated queries may affect the fundamental rights of different categories of persons, including third-country nationals enjoying free movement rights. The chapter also covers proposed changes for transferring VIS data to third parties. It does not deal with access to VIS data by carriers and by law enforcement authorities, which are analysed respectively in Chapters 5 and 6 of this FRA Opinion.

3.1. Reducing the risk of false matches based on facial images

VIS will process facial images as an additional biometric identifier to fingerprints.

The application file in VIS currently includes a photograph of the visa applicant pursuant to Regulation (EC) No. 1683/95.[45] This photograph is collected as a biometric identifier;[46] however, it is not yet used for biometric matching (facial recognition) purposes.[47] The availability of a photograph helps to confirm the identity of a person in case of a match resulting from a fingerprint search.[48]

The proposal suggests changing Article 9 (5) of the VIS Regulation so as to store the "facial image" as defined in Article 13 (1) of the Visa Code instead of the "photograph" of the applicant.[49] The change introduced with the proposal is that the photograph will no longer be scanned, but taken live and collected digitally at the time of the application.[50] Only in exceptional cases, where these requirements cannot be met by taking a live picture, the facial image may be obtained electronically from the electronic Machine Readable Travel Document's chip.[51]

Pursuant to the proposal, the facial image will have to be of sufficient quality and image resolution for the use in automated biometric matching. Under proposed Article 29a (2) (c), VIS will check the quality of the biometrics to ascertain that it fulfils the standards required for biometric matching. Moreover, according to proposed Article 29 (2a), the management authority (i.e. eu-LISA) will have to report regularly on the automated data quality control mechanisms and procedures.

All planned large-scale EU IT systems envisage the possibility to undertake biometric searches with facial images. Typically, they provide that this should be done only as

---

45 VIS Regulation, Art. 9 (4)-(5). Regulation (EC) No. 1683/95 defines the photograph in its Annex as "an integrated colour portrait of the holder […] produced to high security standards".

46 Visa Code, Art. 13 (1).

47 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. 13.

48 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 90.

49 According to the proposal, Art. 13 (1) of the Visa Code will remain unchanged.

50 See Art. 3 (2) of the proposal amending Art. 13 (2) of the Visa Code.

51 See Art. 1 (11) [amending Art. 9 (8) of the VIS Regulation].

soon as technically possible to guarantee a reliable match.[52] Such a safeguard is missing in the proposed amendments to the VIS Regulation. This may result in a premature implementation of biometric searches with facial images, leading possibly to a significant degree of wrong matches, which could negatively affect the right of the data subject to travel or to have a permit issued or renewed. This danger should also be considered in light of the fact that there is no lower age limit excluding automated matches for small children (see Section 3.3).

FRA Opinion 6

In spite of quality assurance safeguards included in proposed Article 29a (2) (c) and proposed Article 29a (2a) of the VIS Regulation, the absence of a requirement to subject biometric searches with facial images to a technical feasibility test may result in false biometric matches. These can lead to decisions that may negatively affect the rights of the data subjects.

The EU legislator should make the introduction of biometric searches with facial images conditional upon the technical possibility to guarantee a reliable match, in line with the approach taken for other EU IT systems.

3.2. Clarifying the meaning of photographs

According to the proposed changes of the VIS Regulation, the terms 'photograph' and '*facial* image' seem to be used interchangeably.[53] It defines the term 'facial image' as a 'digital image of the face'[54] but does not define 'photograph'. The proposed Articles 22g (2) (e), 22h (2) (e) and 22i (2) (f) talk about "*photographs* as referred to in Article 22c (2) (f)", while the corresponding proposed Article 22c (2) (f) speaks

---

[52] 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*), Art. 42 (4); European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No. 515/2014 and repealing Regulation (EC) No. 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU COM(2016) 883 final, Brussels, 21 December 2016 (*SIS II proposal (police and judicial cooperation)*), Art. 42 (4); European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No. 515/2014 and repealing Regulation (EC) No. 1987/2006*, COM(2016) 882 final, Brussels, 21 December 2016 (*SIS II proposal (border checks)*), Art. 28 (4); European Commission (2016), *Proposal for a regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals*, COM(2016) 881 final, Brussels, 21 December 2016 (*SIS II proposal (return)*), Art. 13; 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, Brussels, 29 June 2017 (*ECRIS-TCN proposal*), Art. 6 (2).

[53] See "photograph" used for example in Commission proposal, Art. 1 (20) [amending Art. 22 (2) (c) of the VIS Regulation], Art. 1 (40) [introducing Art. 22h (2) (o) in the VIS Regulation], Art. 1 (30) [amending Art. 37 (2) of the VIS Regulation] as well as existing Art. 18 (4) (b), Art. 18 (5) (b), Art. 19 (2) (b), Art. 19a (5) (b), Art. 20 (2) (c) and Art. 21 (2) (f) of the VIS Regulation; see "facial image" used in Commission proposal, Art. 1 (4) [introducing Art. 4 (15) of the VIS Regulation], Art. 1 (5) [amending Art. 5 (1) (b) of the VIS Regulation], Art. 1 (11) [amending Art. 9 (5) and Art. 9 (8) of the VIS Regulation], Art. 1 (14) [introducing Art. 15 (2) (ea) in the VIS Regulation], Art. 1 (14) [introducing Art. 15 (2a) in the VIS Regulation], Art. 1 (18) [amending Art. 18 (6) (b) of the VIS Regulation], Art. 1 (40) [introducing Art. 22c (2) (f), Art. 22d (f) and Art. 22n (3) (e) in the VIS Regulation], Art. 1 (27) [introducing Art. 29a (2) (c) in the VIS Regulation], Art. 1 (33) [introducing Art. 45 (3) in the VIS Regulation].

[54] See Commission proposal, Art. 1 (4) [amending Art. 4 (15) of the VIS Regulation].

about "a *facial image* of the holder, where possible taken live" [emphasis *added*]. The Visa Code, including its proposed amendments, uses only the term 'photograph'.[55]

The legislative proposals creating new or upgrading existing large-scale IT systems in the area of asylum and migration,[56] as well as the interoperability proposals, all use the term 'facial image'.[57] The term 'photograph' is used only in the three SIS proposals on police and judicial cooperation, border checks and return, however, in addition – and not interchangeably – to the term 'facial image'.[58] Due to this distinction, it appears that there is a more substantive difference between a photograph and a facial image. Table 1 provides an overview of the terminology used in other texts.

Table 1: Use of the terms 'photograph' and 'facial image' in the legal instruments on large-scale IT systems and their definitions

Legal instrument	Term 'photograph'	Term 'facial image'
EES Regulation	N*	Y; definition: *digital images of the face* (Art. 3 (17))
Eurodac Regulation	N	N
Eurodac recast proposal	N	Y; definition: *digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching* (Art. 3 (o))
ECRIS-TCN proposal	N	Y; definition: *a digital image of the face* (Art. 3 (m))
SIS Regulation	Y; no definition	N
SIS Decision	Y; no definition	N
SIS proposal on police and judicial cooperation	Y; no definition	Y; no definition
SIS proposal on border checks	Y; no definition	Y; no definition
SIS proposal on return	Y; no definition	Y; no definition
Interoperability proposals	N	Y; definition: *digital images of the face* (Art. 4 (11))

Notes: *Y= yes, N = no*
** The term 'photograph' appears only in Art. 61, which introduced amendments to the VIS Regulation.*

Source: FRA, 2018

---

55 European Commission Proposal. Art. 3 (1) [amending Art. 10 (3) (c) of the Visa Code], Art. 3 (2) [amending Art. 13 (2) (a) and Art. 13 (3) of the Visa Code]; existing Visa Code, Art. 13 (1) and (4), Annex VII.

56 The existing systems do not contain facial images. Moreover, ETIAS will not include biometrics.

57 See for, example, EES Regulation, Art. 3 (1) (17); Eurodac proposal, Art. 3 (1) (o), ECRIS-TCN proposal, Art. 3 (m); SIS II proposal (police and judicial cooperation), Art. 12 (3), Art. 18 (3), Art. 20 (3) (w), Art. 22, Art. 42, Art. 59 (3) (i); SIS II proposal (border checks), Art. 12 (3), Art. 18 (3), Art. 20 (2) (w), Art. 22, Art. 28, Art. 42 (3) (i); SIS II proposal (return), Art. 4 (t), European Commission (2018), *Amended 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, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, COM(2018) 478 final, Brussels, 13 June 2018, Art. 4 (11); European Commission (2018), *Amended 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) and amending Regulation (EU) 2018/XX [the Eurodac Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]*, COM(2018) 480 final, Brussels,13 June 2018, Art. 4 (11).

58 See SIS II proposal (police and judicial cooperation), Art. 20 (3) (w), Art. 22, Art. 42, Art. 59 (3) (i); SIS II proposal (border checks), Art. 20 (2) (w), Art. 22, Art. 28; SIS II proposal (return), Art. 4 (t).

FRA Opinion 7

The proposal seems to use the terms 'photograph' and 'facial image' interchangeably, while other legislative proposals on large-scale IT systems use only the term 'facial image' or, as it is the case with SIS, appear to draw a distinction between 'photographs' and 'facial images'. Consistency in terminology would help to ensure legal clarity and foreseeability of the proposed amendments. If a photograph should be distinguished from a facial image because a photograph should not be used for automated biometric matching, for example, its meaning should be defined in the proposal.

The EU legislator should ensure consistency in terminology between 'photographs' and 'facial images' if both terms have the same meaning. Alternatively, the EU legislator should define the meaning of a 'photograph' if it has a different meaning than 'facial image'.

3.3. Respecting the rights of the child and older people when processing biometrics

The processing of biometric data from children is particularly sensitive. Under Article 24 of the Charter, children have the right to such protection and care as is necessary for their well-being. This means that any processing of children's biometric data in a large-scale IT system must be subject to a stricter necessity and proportionality test, compared to adults. It will not be sufficient to show that technology meanwhile allows for reliable matching of biometric data collected from children (an issue that was questioned in the past, when comparing fingerprints for children below 12 years of age). The processing of children's biometrics must be necessary to protect them, for example, from risk of abduction, involuntary separations from their families, or trafficking in human beings. The processing of children's biometric data would not be legitimate if the purpose of the data processing could also be achieved by processing only the biometric data of their parents.

Article 25 of the Charter is one of the first legally binding human rights provisions addressing expressly the rights and principles regarding the treatment of older people. It stipulated that the EU "recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life". EU policies and relevant legislative measures need to be designed and implemented in light of these rights and principles, whereas adopted EU secondary legislation should be interpreted accordingly. With increased mobility of older people, Article 25 is also relevant for VIS.

Fingerprints

Recital (8) of the proposal justifies the lowering of fingerprinting age by referring, among other things, to two studies prepared by the Joint Research Centre (JRC) of the European Commission, according to which capturing fingerprints of children who are at least six years old meet acceptable quality standards under certain conditions. A sufficiently high quality of the captured fingerprints is a precondition for a reliable match. However, the growth of the child also affects the reliability of the match. The 2018 JRC study complementing an earlier study from 2013 focuses on the impact of age, including the growth process of a child. The results concluded that fingerprint matches of very young children (0-4) present lower matching scores, compared to older children. Fingerprint matches of children in the range of 5-12 years are not fully

reliable after 7 years have passed since they were collected. Only results for children between 13-17 years of age are very similar to those of adults.[59]

The JRC study also found that challenges exist to match fingerprints of older people, especially those above 70 years of age. The accuracy of any fingerprint match for this group is comparable to that of children aged 5-12.[60]

Whereas, in principle VIS retains data only for a period of five years, Section 2.2 of this FRA Opinion describes that in case of extension of residence permits, in practice VIS data may be retained for much longer. A retention of fingerprints for more than seven years would considerably increase the risks for false matches for persons younger than 12, according to the Joint Research Centre. This risk could be mitigated by replacing the fingerprints in VIS when the permit is extended.

Facial images

According to amendments proposed to Art. 13 (2) of the Visa Code facial images will be collected digitally and taken live at the time of the application. The proposal does not introduce an age limit for the collection of facial images. This means, that, at least theoretically, facial images of children at all ages, including babies, could be used for automated biometric matching. The automated matching of in particular babies' data would be difficult to justify under Article 24 of the Charter, unless the matching is carried out to protect the child from abuse or exploitation.

Changes in the facial shape of a child are likely to impact on the reliability of a match. The Joint Research Centre of the European Commission has said that facial recognition of children can be particularly challenging if the enrolment would be at a young age, and then compared to newer images enrolled more than 5 years later. No study has analysed the "safe" minimum age at which face recognition of children reaches the same reliability as face recognition of adults.[61]

Practical implications

The taking of fingerprints and facial images of children and of older persons also has practical implications. Older persons and children would have to travel to embassies or consulates or to their service providers tasked with accepting visa applications and taking biometrics under Articles 10, 42, and 43 of the Visa Code. Depending on the network of consulates and service providers, in some third countries travelling to embassies, consulates or service providers to give fingerprints and facial images could pose significant practical hurdles or involve considerable costs, particularly for families with more children. As VIS is interoperable with EES and allows that visa related data be up-dated at the border, to avoid complications for children and older persons, fingerprints could be collected at the borders in such cases, similarly to what is provided for visa-free third-country nationals under the EES.[62] The facial image could be taken from the photograph in the electronic Machine Readable Travel Document (eMRTD). If the child does not have a travel document of his or her own, but is included in that of the parents, exceptionally the facial image could be taken at the border.

---

59 European Commission (2018), *Automatic fingerprint recognition: from children to elderly, Ageing and age effects*, JRC technical reports, 2018, pp. 40, 43.

60 *Ibid*, pp. 40, 61.

61 Joint Research Centre of the European Commission, Fingerprints and Alternative Biometric Modalities in EURODAC, Günter Schumacher (2016), limited distribution, pp. 23-24.

62 EES Regulation, Art. 17.

FRA Opinion 8

The processing of biometric data of children is very sensitive and must be subject to strict requirements. Children and older persons should not be put in a situation in which they would be disproportionately affected by the negative consequences of a false match. The reliability of fingerprint matches drops for persons older than 70 years due to problems in high quality data acquisition for persons of that age. For children below the age of 13, the reliability drops over time as the child grows. Moreover, the EU legislator could make an effort to reduce practical hurdles and costs, where children and older people need to travel long distances to provide their biometrics.

***To respect the rights of the child enshrined in Article 24 of the Charter and promote the rights of the elderly in Article 25 of the Charter, the EU legislator should complement the horizontal safeguard in proposed Article 7 (3) of the VIS Regulation with the following actions*:**

- ***If individual files in VIS are, contrary to FRA Opinions 2 and 3, kept for over five years, (for example, following the extension of a residence permit) stipulate in proposed Articles 9a and 22b that no automated queries will be carried out with biometric data of people aged 70 years or over and of children below the age of 13 years when more than five years have passed since their biometrics were collected.***

  Alternatively, postpone any automated querying until the results of a large-scale field trial make it possible to achieve high-quality matching from children and older people.

- ***Introduce an obligation to involve specialised dactyloscopic and facial recognition experts whenever comparisons are made using biometrics of people older than 70 years and when stored biometrics which are older than five years are used for children who are younger than 13 years of age.***

In addition, to avoid excessive burden and costs for families with children and for older persons when they need to travel long distances to give their biometrics, the EU legislator

- ***Should amend proposed Article 9 (8) of the VIS Regulation, allowing for the extraction of the facial image stored in the electronic Machine Readable Travel Document (eMRTD) also in those cases where in exceptional circumstances the travel involves excessive burden and costs for families with many children and for older persons.***

- ***Could consider amending the relevant provision of the Visa Code to allow taking fingerprints and facial images at the border. Article 16 of the EES Regulation (Regulation (EU) 2017/2226) should be adjusted accordingly.***

3.4.Avoid excessive data processing through automated queries

Pursuant to proposed Articles 9a (3) and 22b (2), every time an individual file is created in VIS, the system will automatically compare the applicant's data against past data stored in VIS itself as well as data stored in other IT systems. Under proposed Articles 9a (4) and 22b (3), resulting hits will be saved in the individual VIS file. Such hits will indicate also which Member State provided the data which triggered the hit.

The automated VIS query is different from and additional to the verification of multiple identities envisaged under Article 27 of the proposed interoperability regulation (see also new proposed Article 21 (3b) of the Visa Code).

Purpose of the automated check

The purpose of the automated check appears to differ depending on the category of persons. In case of short-stay visa applicants, the automated query is made as soon as the application file is created in VIS. Thus, the query serves to help the authorities in deciding whether to issue a visa or not. More specifically, it is intended to support the verification required by Article 21 (1) and Article 21 (3) (a), (c) and (d) of the Visa Code, namely to assess if the applicant fulfils the entry conditions,[63] presents an irregular migration or security risk and whether he/she intends to leave before the visa expiry date, to check that the travel document is genuine, to verify any entry ban in SIS and to determine if the applicant poses a threat to public policy, internal security or public health, or to the international relations of the Member States.

In case of long-stay visas or residence permits, the VIS file is only created after a decision on the issuance is taken (proposed Article 22a of the VIS Regulation). Therefore, the hits resulting from the automated query will not anymore be useful to decide whether to issue a long-stay visa/residence permit or not (although these could potentially trigger the revocation or the termination of the residence permit or long-stay visa in future). The proposed Article 22b is contradictory on the purpose of the automated query:

- According to proposed Article 22b (1), the purpose of these queries is to assess whether the third-country national "could pose a threat to public policy, internal security or public health pursuant to Article 6 (1) (e) of [...the Schengen Borders Code]". This rationale clearly applies only to visas and permits issued abroad.
- Proposed Article 22b (5) stipulates, however, that hits with EES, ETIAS and VIS are limited to refusals "which are based on security grounds". This indicates that the primary purpose of the automated query is to store hits which alert officers who will query VIS in future about potential security risks the individual may pose. Such information would primarily be useful for border guards, when they need to decide whether to allow the individual to enter the EU or not.

From a joint reading of proposed Articles 22b (1) and 22b (5) it seems that the primary purpose of the automated check is to support policies on border checks pursuant to Article 77 of the Treaty on the Functioning of the EU (TFEU). More specifically, it would help border guards when deciding to admit a person who reaches the border with a long-stay visa or a residence permit.

If, on the contrary, the purpose of the automated query is broader (such as, informing future decisions relating to the individual on potential security risks), then this should be clarified providing evidence of its necessity and proportionality.

In addition, it is difficult to imagine how querying other IT systems may help identifying public health threats. Only ETIAS may contain personal health-related information. Such information may however be outdated. FRA has, in its legal opinion on ETIAS,

[63] As set out in Art. 6 (1) (a), (c), (d) and (e) of the 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 L 77/1.

underlined that public health risks should be assessed at the border.[64] It should be based on epidemiological sources. Focusing the purpose of the query on supporting the assessment of whether the person constitutes a threat to security upon entry, as proposed Article 22b (5) suggests, would raise less issues with regard to the necessity and proportionality of the query, compared to extending the assessment to "a threat to public policy, internal security or public health". Article 18 (4) of the EES Regulation (EU) 2017/2226, also excludes the collection of biometric data if the refusal of entry is based on public health grounds.

Information systems queried and data which authorities can access in case of a hit

The information systems queried are the same for short-stay visas and for long-stay visas or residence permits. They include VIS itself, and four of the five information systems which the EU has set or is setting up (SIS, EES, ETIAS and ECRIS-TCN), the Europol databases and the two Interpol databases on Stolen and Lost Travel Documents (SLTD) and TDAWN, the database on individuals who are subject to an Interpol alert. The automated query is carried out using the European Search Portal which will be established by the interoperability regulations.

If the file is created outside the EU territory by a consular authority, the automated search also includes Eurodac and the list of recognised travel documents referred to in Article 5a of the proposal, according to proposed Articles 9a (3) and 22b (6). Considering that Eurodac contains data on migrants in an irregular situation apprehended within the territory, querying selected Eurodac data in case of files created at consulates would appear justified, but the necessity of querying Eurodac data on asylum applicants is not legally convincing.

For short-stay visas, the query has the purpose to support the examination of the visa application. For long-stay visas and residence permits issued abroad, the automated query seems mainly intended to support the border guards when they will check the individual at the border crossing point upon entry. Information on whether the person submitted an asylum application in the past and whether such application was rejected should not impact on the decision to issue a short-stay visa or on the decision on whether to allow entry or not, when the individual comes to the border.

Attaching possible negative consequences to a past asylum application would result in discouraging third-country nationals in need of international protection to submit an asylum application or to delay a submission until they are confronted with a risk of removal from the EU. As such, it would undermine the right to seek asylum in the EU under Article 18 of the Charter and, in case of last-minute applications, possibly expose them to a risk of *refoulement* prohibited by Article 19 of the Charter.

At the same time, information on whether the individual refused to leave the EU after a negative asylum decision is already available through SIS which stores entry bans and in future will also store information on whether a person was subject to a return decision. Information on whether the individual used different identities in the past and is thus deceiving the authorities will become available through the Multiple Identity Detector which will be established as part of the interoperability proposals.

[64] FRA (2017), *The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], 30 June 2017, p. 20.

For these reasons, it does not appear necessary for visa or consular authorities to have access to information on applicants for international protection covered in Chapter II of the Eurodac Regulation.[65]

Content of the hit and purpose limitation

The proposal does not define what a hit consists of. Presumably, it will be limited to a reference to the other file stored in the IT systems but for purposes of legal clarity this should be expressly stated.

In addition, in line with the principle of purpose limitation, a VIS user should only be allowed to view the hits which concerns IT system he/she is authorised to consult according to the legal instruments regulating the individual IT systems. Otherwise, it would violate the principle of purpose limitation mirrored in Article 8 (2) of the Charter, as well as in Article 5 (1) (b) of the General Data Protection Regulation.[66] This should be clarified in the proposal.

Duty to inform the central authority of the other Member State

In case of a hit, proposed Article 9c (5) will require the central visa authority processing the application to inform the central authority of the other Member State which entered or supplied the data which triggered the hit.

The proposal does not specify the rationale for sharing such information. Whereas in certain cases a duty to inform the Member State may be necessary, for example, for internal security reasons, sharing data of all hits, including those where the hit concerns data entries on a trusted traveller, would be difficult to justify under the principle of purpose limitation. In addition, it could create a significant administrative burden.

Data used for the query

For long-stay visas and residence permits, Article 22b (2) defines expressly the VIS data which the system will use for the automated query as follows: "the relevant data referred to in Article 22c (2) (a), (b), (c), (f), and (g)". For short-term visas, Article 9a (3) refers to a longer list of "relevant data" contained in paragraph (4) of Article 9. Annex 1 lists the individual data which are used by the automated query. Significantly more data are used for the automated query prior to a decision on short-stay visas. Some of the items listed under Article 9 (4) appear, however, not to be relevant. For example, the travel information under Article 9 (4) (g), (h) and (i) will not be available in any other IT systems, at least not before the individual has crossed the border, if subject to the EES.

Mitigating risks for persons in need of protection

The automated query includes the two Interpol databases on Stolen and Lost Travel Documents (SLTD) and TDAWN, the database on individuals who are subject to an Interpol alert.

Interpol databases are fed by information provided by national police authorities. In spite of Interpol's checks to exclude alerts based on political, military, religious or racial

---

65 Regulation (EU) No. 603/2013 of 26 June 2013 on establishment of Eurodac (recast) OJ 2013 L 180/1 (*Eurodac Regulation*).

66 See in this context FRA (2017), Fundamental rights and the interoperability of EU information systems: borders and security, p. 14 as well as FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018, FRA Opinion 4.

reasons, regimes in third countries may manage to include an alert on one of their nationals or on a document held by that person in an Interpol database to prevent the person from travelling or to find out where the person is hiding. To shield the person and his/her family members in the country of origin from protection risks, including a risk of kidnapping, queries to the Interpol databases must be adequately designed.[67] However, a safeguard for preventing that the hits are shared with the owners of Interpol data, similar to Article 9 (5) of the Interoperability proposals is missing in the proposal. Having such a safeguard would be particularly important, if VIS stores residence permits issued to recognised refugees.

Dealing with false hits

FRA has on several occasions pointed to the risks of false hits as a consequence of low quality or inaccurate data. Carrying out queries based on alphanumeric data is likely to lead to more mistakes than searches based on fingerprints. The risk for mistakes is, therefore, considerable when queries are carried out against ETIAS (which does not contain fingerprints). Still, FRA research found that mistakes have happened in the context of VIS, for example, when the fingerprints belonging to another person were stored in the application file.[68]

Article 22b (7) recognises that querying the individual file against other EU IT systems may result in false hits. The querying authority must delete the false hit. This provision mirrors Article 9c (3-5) relating to short-term visas and which deals with the manual verification of hits in the application files by central visa authorities in the Member States. When an authority implements this task, it would need to receive guidance on how to identify false hits, particularly, if this is done by smaller authorities at the local or regional levels. One possibility would be that a central authority offers such support also in case of applications for residence permits processed within the territory.

FRA Opinion 9

The purpose of the automated VIS query for long-stay visa and residence permit holders is unclear. The term "hit" is not defined and data processed through automated queries are excessive. Sensitive Eurodac data that appear irrelevant for the query are consulted, and a safeguard is missing to prevent the sharing of information on beneficiaries of international protection whose data are stored in Interpol databases.

The EU legislator should:

- ***Better define the purpose of the automated VIS query for long-stay visa and residence permit holders in proposed Articles 22b (1) and Articles 22b (5) in a manner which complies with the necessity and proportionality of restriction to the right to protection of personal data. More specifically, this could mean:***
    - ***carrying out automated VIS queries only if the file is created by the consular authority, thus excluding automated queries on files created within the territory;***
    - ***amending proposed Article 22b (1) and Article 22b (5) stipulating that automated queries are solely carried out for the purpose of supporting border management authorities to assess whether the person poses a***

[67] For more information, see Interpol's legal materials on neutrality, available at: https://www.interpol.int/About-INTERPOL/Legal-materials/Neutrality-Article-3-of-the-Constitution.

[68] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 90.

threat to public policy or internal security (thus excluding public health considerations).

- ***Amend proposed Article 9a (3) to exclude from the automated checks applicants for international protection whose data are stored under Chapter II of the Eurodac Regulation.***
- ***Define the meaning of "hit" used in Article 9a, 9b and 9c as well as in Article 22b.***
- ***Insert a clause in Articles 9a and 22b to make clear that a VIS user can only see hits to IT systems he or she is authorised to consult according to the legal instruments regulating the individual IT systems. This limitation must also apply to the verifying authority under Article 9c (1) and 22b (7) of the proposal.***
- ***Define expressly which "relevant data" contained in Article 9 (4) will be used for automated checks in case of short-stay visa applications.***
- ***Reformulate proposed Article 9c (5) to limit the duty to inform other EU Member States to specific situations where this is justified.***
- ***Introduce a safeguard for preventing that hits against Interpol databases are shared with the owners of Interpol data, similar to Article 9 (5) of the interoperability proposals.***

3.5. Clarifying which personal data will be stored in the Common Identity Repository

With the IT systems becoming interoperable, certain biographical and biometric data of data subjects processed in VIS will be stored in the Common Identity Repository established by the proposed interoperability regulations. The data stored there will still 'belong' to VIS and include a reference to it.[69]

The proposed amendments to Article 5 (3) of the VIS Regulation follow the solutions envisaged in the amended interoperability proposal and do not introduce new data categories to be stored in the Common Identity Repository. However, there are some minor discrepancies between the data categories listed in proposed Article 5 (3) of the VIS Regulation and Article 7 (2) of the proposal, which introduces amendments to Article 18 (1) (b) of the Interoperability Regulation on borders and visa. First, proposed Article 5 (3) refers to a non-existing Article 22d (cc) of the VIS Regulation. Second, according to proposed Article 5 (3) [as per Article 9 (4) (aa) and (cc)] "the surname at birth (former surname(s)), place and country of birth, nationality at birth, the authority

[69] 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, Explanatory memorandum, p. 7 and Art. 18 (2).

issuing the travel document and the issuance date" should be stored in the Common Identity Repository, whereas this is not reflected in Article 7 (2) of the proposal.

FRA Opinion 10

The data referred to in Article 1 (5) and Article 7 (2) of the proposal are not fully aligned. Consistency in defining the data processed would help to ensure legal clarity and foreseeability of the proposed amendments.

The EU legislator should:

- ***clarify in the proposed amendments to Article 5 (3) of the VIS Regulation which data is meant with the reference to Article 22d (cc) of the VIS Regulation;***
- ***clarify in the proposed amendments to Article 5 (3) of the VIS Regulation and in Article 7 (2) of the European Commission proposal (which amends Article 18 (1) (b) of the proposed Interoperability Regulation on borders and visa) whether data referred to in Article 9 (4) (aa) and (cc) of the VIS Regulation should be stored in the Common Identity Repository or not.***

3.6. Protecting the rights of third-country national family members of persons enjoying the right of free movement

Recital (45) of the proposal stipulates that the VIS Regulation remains without prejudice to the application of Directive 2004/38/EC (Free Movement Directive).[70] However, Recital (48) adds that "specific provisions should apply to third-country nationals who are family members of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement under Union law and who do not hold a residence card referred to under Directive 2004/38/EC." Pursuant to this recital, third-country national family members of EU citizens as well those of nationals of the four Schengen Associated Countries and Switzerland (and the United Kingdom after Brexit) will continue to fall, to some extent, under the personal scope of the amended VIS Regulation if they are from a third-country which is subject to a visa requirement under Annex I of the Visa List Regulation (EC) No. 539/2001.[71]

At present, the VIS Regulation does not include any express rule governing the position of third-country national family members of EU citizens and of other persons enjoying the right to free movement under EU law. Implicitly, they are covered by the definition of 'applicant' as set out in Article 4 (5) of the Regulation. Therefore, their personal data submitted in the application for an entry visa are stored and processed in VIS.

It is to be noted that the amount of data which is collected on them under the VIS Regulation might raise issues under Article 7 (right to respect for private and family life), Article 8 (protection of personal data) and Article 52 (1) (necessity and proportionality test in case of limiting fundamental rights) of the Charter, following the

[70] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No. 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, OJ L 158/77.

[71] Council Regulation (EC) No. 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, OJ L 81/1, as amended (for the list of multiple amendments, see https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R0539).

CJEU's judgment in *Huber*. In this ruling, the CJEU confirmed that the personal data of EU citizens (and implicitly of their family members) who have moved within the EU can only be kept in central databases if this is necessary pursuant to the Free Movement Directive.[72]

In the operative part of the proposal, there is a specific provision in new Article 9b on how to perform queries, using the European Search Portal, to other large-scale IT systems for third-country national family members of EU citizens and those of non-EU nationals enjoying the right to free movement under EU law, when they apply for a short-stay visa. Proposed Article 9b (1), read in conjunction with proposed Article 9a (3), wishes to introduce automatic checks against large-scale databases for assessing "a risk to security or high epidemic risk" these individuals might pose in the EU Member States. This specific group of third-country nationals, enjoying a privileged status as having family ties with EU citizens, will be thus subject to automated checks via interoperability when applying for an entry visa.

Whereas interoperability can support the assessment of a risk to internal security (for example, if the individual is present under different names in the IT systems covered), as pointed out in Section 3.4, it is difficult to imagine how interoperability of various large-scale IT systems can help assessing public health risks. Automated checks via interoperability searching for factual indications on "high epidemic risk" are also discriminatory, compared to visa-free third-country national family members (e.g. in case of a spouse from Moldova, Ukraine or Venezuela). As a consequence, the indicator linked to "high epidemic risk" should be removed from the text.

In addition, the information obtained through interoperability needs to be assessed in line with Articles 5 (2) and 27 (2) of the Free Movement Directive. First, Article 5 (2) of this directive requires Member States to grant third-country national family members of EU citizens "every facility to obtain the necessary [entry] visa." This general wording encompasses all kinds of facilitations to comply with the object and purpose of the directive to ensure the unhindered exercise of free movement of family members of EU citizens, irrespective of nationality,[73] who join or accompany the latter. As the CJEU held, such family members have the right to obtain an entry visa,[74] which distinguishes them from other third-country nationals, who have no such right.[75] Using the personal data of this privileged group of third-country nationals to carry out further checks in multiple IT-databases raises compatibility concerns with the logic and purpose of the facilitations set out in Article 5 (2) of the Free Movement Directive.

Second, Article 27 of the Free Movement Directive sets out the limits on restricting the right to free movement on account of public policy, pubic security or public health. It prescribes in paragraph (2) that restrictive measures taken on grounds of public policy or public security (e.g. the non-issuance of an entry visa to a third-country national family member) must "comply with the principle of proportionality and [must] be based exclusively on the personal conduct of the individual concerned." This provision, codifying pre-existing CJEU case law,[76] further specifies the non-permitted grounds for

---

72 CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008, paras. 59-66.

73 See Recital (5) of Directive 2004/38/EC.

74 CJEU, C-503/03, *Commission of the European Communities v. Kingdom of Spain*, 31 January 2006, para. 42.

75 *Communication from the Commission to the European Parliament and the Council on guidance for better transposition and application of Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States*, COM(2009) 313 final, Brussels, 2 July 2009, point 2.2.1.

76 For example, CJEU, C-503/03, *Commission of the European Communities v. Kingdom of Spain*, 31 January 2006, paras. 46, 52-53 (see the earlier CJEU judgments mentioned therein).

resorting to such restrictive measures. For instance, previous criminal convictions must not in themselves constitute grounds to deny the issuance of an entry visa, given that the personal conduct of the individual concerned must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of the society. Justifications that are isolated from the particulars of the case or that rely on considerations of general prevention (e.g. due to public health risks) cannot be accepted.

Furthermore, as confirmed by the CJEU case law, the EU free movement law, notably Directive 2004/38/EC enjoys precedence over the Schengen acquis.[77] Recital (45) of the proposal and Article 1 (2) of the Visa Code formulating "without prejudice clauses" in respect of the Free Movement Directive also support this interpretation. Therefore, the substantive and procedural rules in the Free Movement Directive must take priority over the relevant provisions of the visa-related *acquis*, including the VIS Regulation, to the extent that the rules in Directive 2004/38/EC are more favourable to the persons concerned.[78] The requirements and facilitations in the Free Movement Directive related to the issuance of entry visas to the third-country national family members constitute such rules, which cannot be derogated from by newly introduced, interfering provisions of the VIS Regulation.

Finally, the operative provisions of the amendments are silent on the applicability of Chapter IIIa to this category of third-country nationals, for example, in case they are issued a long-stay visa to enter the EU. Although their exclusion from the scope of Chapter IIIa can be deducted indirectly from the text (using systemic and teleological interpretation) and from the Explanatory Memorandum of the proposal, clearer language to that effect would avoid doubts during implementation.[79]

FRA Opinion 11

Third-country nationals who are family members of a Union citizen, a national of the European Economic Area (EEA) or a Swiss national to whom Directive 2004/38/EC applies and who do not hold a residence card referred to under that directive fall within the personal scope of VIS. Adequate safeguards must be in place to protect their privileged status under EU law.

The EU legislator should build in a saving clause in proposed Article 9b emphasising that carrying out automated checks in other large-scale IT databases must not unduly and disproportionately affect the issuance of an entry visa. The absence of a safeguard clause could result in undue restrictions to the exercise of the right to free

---

[77] CJEU, C-459/99, *Mouvement contre le racisme, l'antisémitisme et la xénophobie ASBL (MRAX) v. Belgian State*, 25 July 2002, paras. 62, 80, 91 and 104; C-503/03, *Commission of the European Communities v. Kingdom of Spain*, 31 January 2006, paras. 30, 35.

[78] See by analogy, CJEU, C-503/03, *Commission of the European Communities v. Kingdom of Spain*, 31 January 2006. The Commission's 2009 guidance on the application of the Free Movement Directive implicitly confirms this position as well (COM(2009) 313 final, Brussels, 2 July 2009). In the legal literature, see, for example, Guild, E., Peers, S. and Tomkin, J. (2014), *The EU Citizenship Directive. A Commentary*, Oxford, Oxford University Press, 2014, p. 104; Peers, S. (2016), *EU Justice and Home Affairs Law. Volume I: EU Immigration and Asylum Law*, Oxford, Oxford University Press, fourth edition, 2016, pp. 181-182.

[79] Commission proposal, Explanatory Memorandum, p. 3 ("On 17 April 2018, the Commission presented a proposal on strengthening the security of residence cards of third country nationals who are family members of EU citizens. In view of this proposal, including such residence cards into the VIS is not necessary.") and p. 6 ("…information on residence cards issued to the family members of EU citizens with the right of free movement under Union law is not included in this proposal given the rights of these third country nationals stemming from their family relationship with an EU citizen".).

movement of those third-country nationals who are family members of EU citizens and of other non-EU nationals enjoying the right to free movement under EU law.

The EU legislator should remove the wording "high epidemic risks" from proposed Article 9b (1) as the checks carried out through the European Search Portal will not contribute to establish whether such risks exist and it raises issues in light of the object and purpose of Article 5 (2) of Directive 2004/38/EC. Public health risks should be assessed at the border based on epidemiological information provided by relevant official sources.

The EU legislator should also amend the relevant Recital to clarify that proposed Chapter IIIa does not apply to third-country national family members of EU citizens and of nationals of a third country enjoying the right to free movement under EU law.

3.7.Including safeguards for data transfer to third parties

Article 31 (1) of the current text of the VIS Regulation contains a general prohibition of sharing personal data stored in VIS with third countries and international organisations. Article 31 (2) derogates from the general prohibition allowing Member States to share specific VIS data under certain conditions. The proposal simplifies the wording of Article 31 removing the general prohibition to share data but requiring that any sharing of data continues to be subject to strict conditions:

- the data must be necessary in individual cases to prove the identity of a third-country national for return or resettlement purposes;
- the Member State which entered the data in VIS must agree to the data sharing;
- the data sharing must respect the General Data Protection Regulation (GDPR) requirements.

The proposed amendments would, however, broaden the possibility of data transfers. One important difference is that currently, only biographical and travel document data[80] may be communicated to the respective stakeholders. The proposal also includes the possibility of sharing fingerprints and a scan of the visa applicant's travel document's biographic data page. Another change concerns the reference to the EU data protection *acquis*.

Ensuring adequate safeguards

The proposal removes the protective provisions in Article 31 (2) (a) to (c) replacing these with the general wording "without prejudice to Regulating (EU) 2016/679". An explicit reference to the most relevant GDPR provisions would help to raise awareness on the specific requirements for data sharing with third parties flowing from the GDPR and promote adequate protection of persons who could be adversely affected by data transfers.

The VIS Regulation currently requires in Article 31 (2) (b) that the third country or international organisation must consent to use the transferred data "only for the purpose for which they were provided". The proposal envisages to delete this provision. While such an explicit safeguard is not included in Chapter V of the GDPR, the legal principle of purpose limitation is applicable throughout the GDPR's text.

[80] These are listed in Art. 9 (4) (a), (b), (c), (k) and (m) of the VIS Regulation: surname (family name), surname at birth (former family name(s)), first name(s) (given name(s)); date of birth, place of birth, country of birth, sex; current nationality and nationality at birth; type and number of the travel document, the authority which issued it and the date of issue and of expiry; the applicant's home address; in the case of minors, surname and first name(s) of the applicant's parental authority or legal guardian.

Nevertheless, a requirement to obtain the third countries' explicit consent could contribute to the effective protection of data subjects and help to prevent misunderstandings, in particular if data will be transferred for important reasons of public interest under the derogation provision in Article 49 of the GDPR, as per Recital (37) of the proposal. The European Data Protection Board noted that such transfers should never lead to fundamental rights breaches.[81] As illustrated in Table 2, a provision which requires to obtain the third country's consent is also included in other legal instruments on large-scale IT systems which allow the transfer of data for return purposes, with the exception of the SIS proposal on return.[82]

Table 2: Requirement to obtain third countries' explicit consent on purpose limitation when data is shared for return purposes

Legal instrument	TC's explicit consent on using the transferred data only for the purpose for which they were provided
VIS Regulation	Yes Art. 31 (2) (b)
Proposed amendments to the VIS Regulation	*No*
EES Regulation	Yes Art. 41 (3) (b)
ETIAS compromise text	*Yes* *Art. 65 (3)*
Eurodac proposal	*Yes* *Art. 38 (1) (b)*
SIS II proposal (return)	*No*

Note: Proposed changes and legislation in italics.
TC = third country
Source: FRA, 2018 (based on existing and proposed legislation)

Mitigating risks when sharing data concerning applicants for international protection

Individuals whose data are stored in VIS may also have international protection needs. In case residence permits holders are added to VIS, the system will store personal data of virtually all persons granted international protection in one of the EU Member States. In addition, a person entering the EU with a Schengen visa may subsequently apply for international protection.

Information that allows the country of origin to deduce – directly or indirectly – that a person has applied for international protection in another country is extremely sensitive. This was also confirmed by UNHCR, which stated that "confidentiality of data is particularly important for refugees and other people in need of international protection, as there is a danger that agents of persecution or rights violations may ultimately gain access to such information, potentially exposing a refugee to danger even in his/her asylum country".[83]

---

[81] European Data Protection Board (2018), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018, p. 3.

[82] Please note that the Eurodac Regulation, the SIS II Decision and police proposal, the SIS II Regulation and the borders proposal, the ECRIS-TCN proposal and the amended interoperability proposals generally don't allow for data sharing with third countries or international organisations, with some exceptions being possible. See also FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 78.

[83] UN High Commissioner for Refugees (UNHCR), UNHCR comments on the European Commission's Proposal for a recast of the 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 person ("Dublin II") (COM(2008) 820, 3 December 2008) and the European Commission's Proposal for a recast of the Regulation of the European

The current VIS Regulation includes in Article 31 (3) a safeguard clause according to which personal data transfers to third countries must "not prejudice the rights of refugees and persons requesting international protection, in particular as regards non-refoulement". As FRA noted in its ETIAS Opinion, this provision is a step in the right direction.[84]

This safeguard reduces the risk that data of asylum applicants or international protection beneficiaries are shared with third countries, unless required for resettlement purposes. However, the VIS Regulation does not make the data transfer to prove the identity for return purposes conditional to the existence of a final return decision, as required for data transfers under the EES and the ETIAS compromise text.[85] As underlined by FRA in its Eurodac Opinion, personal data of asylum applicants should not be shared with their country of origin to prepare their return as long as no final decision has been taken on the application for international protection.[86]

Cooperating with third countries on data protection matters

The GDPR requires the European Commission and supervisory authorities to take appropriate steps to ensure international cooperation on data protection matters. The same obligation addressing the Commission and Member States is included in the Police Directive.[87] The proposed changes to the VIS Regulation could build on this and include a provision encouraging data protection cooperation between the Member States transferring the data and third countries receiving it.

Cooperation between the Commission, the Member States' national supervisory authorities and data protection authorities of the third countries with which the data was shared could help to ensure compliance with the EU data protection requirements and consequently protection of the data subjects' rights.

Transfer of VIS data obtained for law enforcement purposes

The proposal does not envisage the transfer of VIS data to third countries or international organisations by law enforcement authorities. This prohibition is not explicitly included but stems from the wording of proposed Article 31 which limits data transfers "only for the purpose of return [...] or of resettlement". This approach avoids the risk that third parties may use the data they receive from law enforcement authorities to violate fundamental rights.

Should the EU legislator, nevertheless, envisage the possibility of data sharing in some situations, its necessity and proportionality must be demonstrated and adequate safeguards provided for. The other two relevant instruments in the area of borders and visa – EES and ETIAS – include specific safeguards for such data sharing.[88] These safeguards are similar in both instruments. For example, under the ETIAS compromise text, it will be generally prohibited to transfer or make available personal data, which was accessed by the Member States or Europol from the central system for preventing,

---

Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [the Dublin II Regulation] (COM(2008) 825, 3 December 2008), 18 March 2009, p. 19.

84 FRA (2017), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], Vienna, 30 June 2017, p. 39.

85 EES Regulation, Art. 41 (3) (c); ETIAS compromise text, Art. 65 (3). The enforcement of a return decision must not be suspended and no appeal, which could lead to the suspension, must be lodged.

86 FRA (2016), *The impact of the proposal for a revised Eurodac Regulation on fundamental rights*, p. 31.

87 GDPR, Art. 50; Police Directive, Art. 40.

88 EES Regulation, Art. 41 (5) and (6); ETIAS compromise text, Art. 65 (2) and (5).

detecting or investigating terrorist or other serious crime offences, to any third country, international organisation or third party. This applies also in situations where the data will be further processed at national level or between Member States.[89] In order to derogate from this prohibition, an exceptional case of urgency will have to exist, which could be subject to ex-post monitoring by the supervisory authorities established under Article 41 of the Police Directive. In addition, several requirements will have to be fulfilled:

- the transfer will have to be necessary for the prevention, detection or investigation of a terrorist or serious criminal offence;
- the designated authority will have to be authorised to access such data in line with the procedures and conditions regulating law enforcement access to the ETIAS Central System;
- the transfer will have to respect the requirements of the Police Directive;
- the third country will have to submit a duly motivated request; and
- data provision reciprocity will have to be in place between the Member States and the third country.[90]

Additional safeguards as included in the ETIAS compromise text and an explicit reference to the Police Directive would help to mitigate the risks connected to such data transfers, should they be envisaged.

FRA Opinion 12

The proposal introduces some relevant changes to Article 31 of the VIS Regulation on sharing VIS data with third parties. While the General Data Protection Regulation (GDPR) provides for general safeguards concerning data transfers, a more precise reference to these as well as inclusion of additional specific safeguards in the VIS Regulation would help to ensure the protection of the data subject's fundamental rights.

In regard to Article 31 of the VIS Regulation, the EU legislator should therefore:

- ***in Paragraph (1), replace the words "without prejudice to Regulation (EU) 2016/679" with an explicit reference to the relevant GDPR provisions by stating that "the data transfer shall comply with the relevant provisions of Union law, in particular Regulation (EU) 2016/679, including its Chapter V".***
- ***keep the legal safeguard in Article 31 (2) (b) pursuant to which "the third country or international organisation agrees to use the data only for the purpose for which they were provided";***
- ***explicitly exclude sharing personal data of applicants for international protection with their country of origin to prepare their return as long as no final decision has been taken on their application for international protection;***
- ***building upon Article 50 of the GDPR and Article 40 of the Police Directive, consider encouraging the European Commission and the national supervisory authorities to cooperate with the data protection authorities of the third countries with which VIS data is shared.***

[89] ETIAS compromise text, Art. 65 (2).

[90] ETIAS compromise text, Art. 65 (5).

For legal clarity, the EU legislator should include an explicit prohibition of transferring data to third parties for law enforcement purposes. Should the EU legislator envisage such transfer of VIS data to third parties for law enforcement purposes, such transfers should be subject to safeguards equivalent to those included in Article 65 (2) and (5) of the ETIAS compromise text.

4. Rights of data subjects

This chapter deals with the right to information, as well as with the right to access, correction and deletion of personal data.

4.1. Promoting effective provision of information

The provision of information is a transparency requirement under data protection law and a precondition to effectively exercise the right to access, correction and deletion of personal data. It also promotes respect for the dignity of the person, protected in Article 1 of the Charter. If a person understands the purpose of the data processing, it is easier to win their cooperation in the process.[91]

The right to information is guaranteed by the General Data Protection Regulation (GDPR) and the Police Directive,[92] both of which apply when data is processed under legal instruments covered by the proposal.[93]

Content of the information

According to the proposal, the content of the information provided to the data subjects will remain the same as currently provided under Article 37 of the VIS Regulation. The third-country nationals and their sponsors (for the short and long-stay visas as well as residence permits) will have to be informed about the identity of the data controller, the purposes of the data processing, categories of the data recipients, the retention period, the mandatory data collection and the right to access, correction and deletion of one's personal data. However, it is not envisaged that the information should cover the legal basis for the processing of personal data, the possibility to restrict the processing of personal data and, where applicable, the data transfer to third countries and international organisations, which generally have to be provided pursuant to the GDPR and/or the Police Directive.[94]

FRA research on biometrics shows that rights holders are often not fully informed of all aspects of the data processing.[95] For example, only 11 % of the approximately 570 interviewed visa applicants say that they have received information about how their data will be processed,[96] in spite of such information being included in the visa application form. The research confirms also past FRA findings that persons lack awareness of their data protection rights and consequently of what constitutes data protection violations and which remedies are available to them.[97] Therefore, although

---

91 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 30.

92 GDPR, Art. 12, 13 and 14; Police Directive, Art. 13. See also Art. 5 (1) of the GDPR, which requires that personal data are "processed lawfully, fairly and in a transparent manner in relation to the data subject".

93 Commission proposal, Recital (35). For the scope of the application of the respective legal instruments see GDPR, Art. 2 (material scope) and Art. 3 (territorial scope); Police Directive, Art. 2.

94 For the legal basis for processing see GDPR, Art. 13 (1) (c); Police Directive, Art. 13 (2) (a); for the restriction of processing see GDPR, Art. 13 (2) (b), Police Directive, Art. 13 (1) (e); for the data transfer to third countries or international organisations see GDPR, Art. 13 (1) (f).

95 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 9.

96 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 37, 38.

97 See FRA (2010), *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 (2012), *Access to justice in cases of discrimination – Steps to further equality*, Luxembourg, Publications Office, December 2012; FRA (2017), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II: field perspectives and legal update*, Luxembourg, Publications Office, October 2017.

information has to be provided in line with the EU data protection *acquis*, FRA considers it important to re-state some of the above mentioned missing aspects in the proposal to increase the awareness of what the duty to inform entails. Particularly, since the data subjects' fingerprints and facial images will be used for automated biometric matching, they should be made aware about it. Additionally, due to the sensitive nature of the data sharing with third countries (as explained in Section 3.7), individuals should be informed about this possibility.

Moreover, Article 37 (1) (c) of the current VIS Regulation covers the provision of information on law enforcement authorities' and Europol's access to the data when referring to them as "authorities referred to in Article 3". The proposal intends to delete Article 3 of the VIS Regulation. Therefore, the wording of Article 37 (1) (c) should be adjusted to ensure that information on law enforcement's access to data will also be provided in the future.

Manner of the information provision

As a general rule, the information has to be provided to the respective persons in writing at the time the data are collected (proposed Article 37 (2) of the VIS Regulation).

The proposal introduces some welcome amendments to Article 37 (2) of the VIS Regulation, which address the information gap identified in FRA's research on biometrics.[98] According to the proposal, information could be, if necessary, also provided orally to the data subjects. Moreover, the information will have to be provided in an understandable manner and language. Particular attention is payed to children, who will have to be informed in an age-appropriate manner. Different tools, such as leaflets and demonstrations, will have to be used to explain the fingerprinting procedure to them. This is particularly important since the proposal envisages to reduce the fingerprinting age from 12 to six years.

According to the GDPR and the Police Directive, which apply in the context of VIS, information has to be provided in a concise, intelligible and easily accessible form. Pursuant to the GDPR, information must also be provided in a transparent form.[99] The Article 29 Data Protection Working Party further defined the elements of transparency in its guidelines on transparency.[100] The proposed VIS Regulation, however, does not expressly stipulate these requirements; instead, it only entails an obligation to provide the information in an understandable manner.

Information about certain reasons for refusal

Under proposed Article 22d (h) files created upon rejection of the application for a long-stay visa or residence permit will contain "information indicating that the long-stay visa or residence permit has been refused because the applicant is considered to pose a threat to public policy, public security or to public health, or because the applicant presented documents which were fraudulently acquired, or falsified, or tampered with". Such data entries may affect future applications of the individual, thus negatively affecting his or her fundamental rights – for example, his/her right to

---

98 FRA's findings suggest that much information included in the Schengen visa application form passes unnoticed. For more information see FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 36-38.

99 GDPR, Art. 12 (1); Police Directive, Art. 12 (1).

100 Article 29 Data Protection Working Party (2017), *WP29 Guidelines on transparency under Regulation 2016/679*, WP 260.

respect for family life, if in future the person wishes to travel to join or visit a family member in the EU.

In case of a visa refusal or a refusal of entry at the border, EU law has established standardised ways to inform the individual about the reasons for refusal (see Annex VI to the Visa Code and Annex V, Part B to the Schengen Borders Code).

Article 37 of the VIS Regulation, which the proposal further strengthens, stipulates the right of applicants to be informed about the data processed in VIS. However, contrary to what EU law provides for visa refusals or refusals of entry, there is no standard format to inform individuals about the reasons for refusal of a residence permit, this being regulated in national law. Although national law must comply with the requirements of the EU data protection *acquis* there is no express provision which requires Member States to inform refused applicants of the data entered in VIS under proposed Article 22d (h). Without such information, the individual will not be in a position to exercise effectively his/her right to an effective remedy enshrined in Article 47 of the Charter.

FRA Opinion 13

It is important that the data subjects are informed about all relevant aspects of the data processing, also in light of the fact that adequate information is a pre-condition for access to an effective remedy against inaccurate or unlawfully stored data in VIS.

The EU legislator should consider the following measures to strengthen the right to information included in Article 37 of the VIS Regulation:

- ***expressly require that the information provided should also cover the legal basis for the processing of personal data, the possibility to restrict the processing of personal data and, where applicable, the data transfer to third countries and international organisation, in line with the GDPR and the Police Directive;***
- ***adjust the wording of Article 37 (1) (c) of the VIS Regulation to ensure the provision of explicit information on the fact that personal data may be accessed by law enforcement authorities, drawing upon the existing VIS Regulation as well as Article 50 of the EES Regulation and Article 30 of the Eurodac proposal;***
- ***expressly require that the information should be provided in a concise, intelligible and easily accessible form, and, where applicable, in a transparent form, pursuant to the GDPR and the Police Directive.***
- ***consider adopting a standardised form for notifying the reasons for the rejection which will be stored in VIS as per proposed Article 22d (h), so as to enable a refused applicant to exercise his/her right to an effective remedy. Such form could be similar to Annex VI of the Visa Code or Annex V of the Schengen Borders Code.***

4.2.Making the right to access, correction and deletion more effective

The right to access, correction and deletion of personal data processed is enshrined in Article 8 (2) of the Charter, as well as the GDPR, the Police Directive (with certain restrictions) and in Council of Europe Convention No. 108.[101] The possibility to exercise

[101] GDPR, Art. 15-17; Police Directive, Art. 14 and 16; Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981, Art. 8.

the right to access is part of the right to an effective remedy, as guaranteed under Article 13 of the ECHR and Article 47 of the Charter.

Both the data subject, as well as the authorities, have an interest in ensuring that the data stored in VIS are accurate. However, challenges with the data quality and the effective exercise of the right of access, correction and deletion of personal data exist in practice.

The 2016 VIS REFIT evaluation identified issues with the quality of data contained in VIS.[102] FRA's research on EU IT systems and biometrics confirms this finding. Interviewed diplomatic mission and consular staff, as well as external service providers, indicate that VIS sometimes generates wrong matches (43 % of the respondents) or contains inaccurate, incorrect or not updated data (53 % of the respondents).[103] Similar findings emerged from interviews with border guards, with 60 % of the 139 respondents replying that the data is "sometimes" inaccurate, incorrect or not updated and 9 % indicating that this is "often" the case.[104]

Next to data quality issues with alphanumeric data, processing biometric data is technically complex and, although rare, false biometric matches might occur, as FRA research showed. Moreover, national authorities and experts attach a high degree of credibility to such data. 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.[105]

The proposal addresses these challenges by introducing a number of important measures to improve the quality of the data stored in VIS. Pursuant to the amended Article 29 of the VIS Regulation, Member States will have to ensure that data will meet an adequate level of quality and completeness before the data is stored in VIS. The management authority (i.e. eu-LISA) will have to develop, together with the European Commission, automated data quality control mechanisms and quality check procedures and regularly report on them to the Member States. As explained in the proposed Article 29a, the data quality check will be performed on two levels. First, data will have to be checked by the national authorities prior sending them to VIS. Later, VIS will perform an additional quality check.

These newly introduced measures should also be complemented by a stronger role of the data subject to get inaccurate data corrected or deleted. As research shows, the number of requests for access, correction and deletion of personal data is low. According to the VIS REFIT evaluation, between September 2011 and December 2015,

---

[102] 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, pp. 9, 10; European Commission (2016), 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.

[103] The number of respondents varies for the replies, ranging from 39 to 53 persons. This is related to the fact that numbers of staff working with the databases at the actual DMCPs vary. See FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017, p. 30.

[104] FRA (2017), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, July 2017, p. 31.

[105] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 15, 16, 76.

data subjects made only a few dozen requests to access their data stored in the VIS. The number of requests for correction and deletion was even lower.[106] Lawyers and data protection officers interviewed for FRA's research on biometrics confirm that data processed in large scale IT systems are rarely challenged for being incorrect or unlawful.[107] While in the case of VIS the reasons for it could be also connected to the fact that its rollout finished only in 2015,[108] it should be born in mind that such issues were also observed in regard to the other two IT systems covered by the research, namely Eurodac and SIS, which had been operational for quite some time. This indicates that the issue is of a more general nature. In 2016, the Supervisory Group for VIS stressed that there is "great need to raise awareness" among visa applicants, in particular rejected ones, on data protection rights and how to exercise them.[109]

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.[110]

Despite all identified practical issues, the proposal introduces only a minor amendment to Article 38 of the VIS Regulation, which guarantees the right to access, correction and deletion of personal data.[111] The proposed wording does not seem sufficient to promote an effective exercise of the respective rights, also in the light of the technological and regulatory developments in the field of large scale IT systems as well as data protection since the adoption of the VIS Regulation in 2008. FRA considers it, therefore, extremely important to further strengthen the data subjects' rights by using this opportunity to include additional safeguards into the regulation.

Inserting a clear deadline for replying to requests

Under Article 38 (1) of the VIS Regulation, the data subject has the right to request access to his/her personal data stored and to information on the Member State which transmitted the data to VIS.

Under Article 38 (2) of the VIS Regulation, data subjects may request the correction of inaccurate data as well as deletion of unlawfully recorded data, which must be carried out *without delay* by the responsible Member State pursuant to its laws, regulations and procedures. If the request is forwarded by another Member State, it must be examined in one month.[112]

The VIS Regulation does not provide any deadline for Member States to reply to requests for access, correction or deletion. Pursuant to Article 38 (4) and (5), after

---

[106] European Commission (2016), 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, pp. 36, 90, 91.

[107] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 99.

[108] European Commission (2015), *Visa Information System now fully operational worldwide*, 2 December 2015.

[109] VIS Supervision Coordination Group (VIS SCG) (2016), *Report on access to the VIS and the exercise of data subjects' rights*, February 2016, p. 15.

[110] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 17, 101, 105.

[111] According to the proposal, only paragraph 3 of Article 38 should be amended, which regulates situations where a data subject submits the request to a Member State other than the one responsible. The period for the requested Member State to contact the responsible Member State will be reduced from 14 to seven days.

[112] Commission proposal, Art. 1 (31) [amending Art. 38 (3) of the VIS Regulation].

examining a request for correction or deletion, Member States must inform the data subject "without delay" about the decision. The VIS Supervision Coordination Group (VIS SCG) reported that deadlines for replying to access requests vary among the Member States: whereas in some the reply must be provided immediately, without delay or within a reasonable interval, in others a specific deadline of 30 days was set.[113] Moreover, according to data from a few Member States, the deletion requests during the initial period of implementation of VIS were answered within 30 to 60 days in practice.[114] Dealing with the first cases may have taken longer, as the rollout of VIS has been completed only in 2015.[115]

The GDPR requires the controller to inform the data subject on the action taken "without undue delay and in any event within one month". The period may be extended if necessary, however, the data subject has to be informed about it.[116] The Police Directive requires the controller to inform the data subject "without undue delay".[117] An explicit reference to the one month deadline in the VIS Regulation would help promoting timely responses to requests for access, correction and deletion in all Member States. This would be also beneficial to the data subjects who might find themselves in a precarious situation while their request is being examined. For example, if their data is stored also in other IT systems, incorrect data might create red links under the interoperability framework and the person could be suspected of committing identity fraud.

Handling requests submitted to a Member State other than the one responsible

In line with Article 39 of the VIS Regulation, Member States must cooperate to enforce the right to access, correction and deletion of personal data.

Article 38 (3) of the VIS Regulation regulates situations in which the request is submitted to the Member State which is not responsible to handle the request in substance. In these situations, the Member State who received the request must forward it to the responsible Member State within 14 days. The proposal suggests to reduce this deadline to seven days, thus diminishing the risk of procedural delays. However, the deadlines established by Article 38 (3) only concern requests for correction or deletion and do not apply to requests for access.

Furthermore, Article 38 (3) of the VIS Regulation does not include any requirement to inform the person concerned that his/her request has been forwarded to the responsible Member State. The data subject will therefore not be aware who is dealing with their request.

Restricting the data processing

Pursuant to Article 18 (1) (a) of the GDPR, the data subject can demand that the controller restricts processing contested data for a certain period, allowing the controller to verify the accuracy of the person's data. This means that the controller must refrain from using the data pending the verification, including further sharing of

[113] VIS Supervision Coordination Group (VIS SCG) (2016), *Report on access to the VIS and the exercise of data subjects' rights*, February 2016, p. 10.

[114] VIS Supervision Coordination Group (VIS SCG) (2016), *Report on access to the VIS and the exercise of data subjects' rights*, February 2016, p. 11.

[115] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, p. 104.

[116] GDPR, Art. 12 (3) and (4).

[117] Police Directive, Art. 12 (3).

the data, in order to ensure that possible false assumptions 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 – 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.[118]

The VIS Regulation does not include the right to restriction of processing. Since unlawful processing might have adverse consequences for the data subjects, it would be important to re-state this right, and consequently raise awareness, also in the VIS Regulation. Such a right is explicitly included also in the Eurodac proposal.[119]

FRA Opinion 14

The proposal only suggests one change to Article 38 of the VIS Regulation. In light of the significant obstacles adversely affecting the effectiveness of the right to access, correction and deletion of personal data more substantial changes to this provision would support data subjects in exercising their rights more effectively.

In order to increase the effectiveness of the access, correction and deletion procedure, the EU legislator should:

- ***include in Article 38 (1) of the VIS Regulation a deadline for the reply by adding the following sentence: "The Member State shall reply to such requests without delay and no later than within 30 days of receipt of the request", in line with Article 12 (3) and (4) of the GDPR;***
- ***include in Article 38 (2) of the VIS Regulation a deadline for the correction or deletion of personal data by indicating that the "correction and deletion shall be carried out without delay and no later than in 30 days of receipt of the request", in line with Article 12 (3) and (4) of the GDPR;***
- ***cover in Article 38 (3) also requests for access to personal data;***
- ***include in Article 38 (3) a duty to inform in writing any person who has approached a Member State other than the one responsible to review the request, indicating to whom the request has been forwarded;***
- ***include in the VIS Regulation the right to restriction of data processing.***

[118] The right to the restriction of processing is included, in a more restrictive manner, also in Art. 16 of the Police Directive.

[119] Eurodac proposal, Art. 31 (8).

5. Access by airlines and other carriers

This chapter deals with the fundamental rights challenges raised by providing access to VIS data to carriers, meaning companies that transport passengers across the border. Carriers will have the duty to check the passport of passengers against EU IT systems. This raises a number of fundamental rights issues.

5.1. Dealing with false matches

Article 26 (1) (b) and (3) of the Convention implementing the Schengen Agreement requires signatories to oblige carriers transporting foreigners by land, air or sea to take all the necessary measures to ensure that they are "in possession of the travel documents required for entry into the territories of the Contracting Parties".[120]

To fulfil their obligations, proposed Article 45b of the VIS Regulation requires carriers to verify the passenger's data contained in the machine readable zone of the travel document prior to boarding against the data stored in VIS. Furthermore, Article 13 (3) of the Entry/Exit System Regulation requires carriers to use a dedicated "web service to verify whether third-country nationals holding a short-stay visa issued for one or two entries have already used the number of entries authorised by their visa".

Pursuant to Article 13 (5) of the Entry/Exit System Regulation, carriers will not directly consult the EU IT system, but a separate read-only database updated on a daily basis via a one-way extraction of the minimum necessary subset of EES and VIS data. Proposed Article 45b (2) of the VIS Regulation further clarifies that a dedicated "carrier gateway" will be established for this purpose. Thus, carriers will not be entitled to query VIS itself, but only a copy of it which stores the data carriers need for their check. This approach is preferable to giving private actors direct access to the IT system itself. As FRA points out in its report on interoperability, it is important to keep a clear separation between the data carriers are entitled to access and those data they are not entitled to see.[121]

According to proposed Article 45b (4), carriers will receive a response from VIS saying "OK/NOT OK" to board. The reply is generated automatically, but airlines will have the duty to manually review it, in line with Article 22 of the GDPR which gives the data subject the right not to be subject to a decision based solely on automated processing.

One of the main findings of FRA's report on the use of biometric data in large-scale IT systems is the significant amount of inaccurate data stored therein.[122] Although measures are being taken to progressively improve data quality, data contained in the IT systems that carriers will be obliged to consult will continue to have inaccuracies, at least as long as data is entered manually in VIS. It can, therefore, be expected that passengers will be refused boarding because data in the machine readable zone of the passport will not match with those stored in VIS.

In some cases – for example, when all data are the same but there is a mistake in one of the letters/numbers of the passport or in the spelling of the name – the mismatch

---

[120] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239/19. Regarding land carriers, this applies to "international carriers transporting groups overland by coach, with the exception of border traffic" (Art. 26 (3)).

[121] FRA (2017), *Fundamental Rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office of the European Union, see for instance Chapters 1 and 2; especially p. 26.

[122] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, Chapter 5.

between the data sent by the airline and the one stored in the IT system is clearly caused by a data entry error. A mechanism should be envisaged to sort out automatically minor inconsistences that are clearly the result of inaccurate data entry.

Decisions to refuse to board based on inaccurate data may affect various fundamental rights, depending on the circumstances, such as freedom to conduct a business set out in Article 16 of the Charter (in case a person travelling for work), right to respect for family and private life, right to asylum, right to an effective remedy (for a person who travels to testify in a court in the EU), etc.

FRA Opinion 15

Small inaccuracies between the data sent by the airline and the one stored in the IT system may result in a significant number of "NOT OK" to board, even when the mismatch is clearly caused by a data entry error. Steps should be taken to mitigate this risk.

The Commission implementing act setting up the authentication scheme in proposed Article 45b (5) should design the carrier gateway in such a way that mismatches that are clearly the result of data entry mistakes are not flagged as "NOT OK".

5.2. Informing passengers

Data subjects have the right to information when their data is being collected for VIS (see Section 4.1). Although the EU data protection *acquis* does not confer a right to information when authorities or other stakeholders, including carriers, are consulting already stored data, such information is crucial to ensure the effective exercise of the data's subject right to access, correction and deletion of personal data.

Under the proposal, the carriers are not obliged to inform the passengers about the "NOT OK" message. The refusal of boarding might have adverse effects on the person concerned. Since FRA research showed that large-scale IT systems contain a significant amount of inaccurate alphanumeric data (see Section 4.2),[123] it is crucial that the data subjects are adequately informed about the possibility to exercise their right to access, correction and deletion of personal data. Moreover, the carriers should give the passengers the opportunity to provide explanations for the "NOT OK" reply before refusing the boarding. There might be valid reasons behind the negative reply which should be taken into account, for example, the passenger could be holding two passports.

FRA Opinion 16

The right to information is a precondition to effectively exercise the right to access, correction and deletion of personal data. Therefore, it is crucial that the person concerned receives appropriate information if refused boarding due to a "NOT OK" message.

The EU legislator should include a specific provision in proposed Article 45b obliging the carriers to provide information to passengers refused boarding due to a "NOT OK" response from VIS, indicating also how to exercise their right to access, correction and deletion of personal data stored in VIS.

[123] FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, Chapter 5.

5.3. Handling "NOT OK" to board notices

According to proposed Article 45b (4), read together with Article 13 of the Entry/Exit System Regulation, carriers will receive a response from VIS saying "OK/NOT OK" to board. A similar arrangement is envisaged for visa free passengers through Article 45 (2) of the ETIAS compromise text.

While in light of Article 22 of the GDPR the airline will need to review each case manually, without real-time and effective assistance by the authorities in charge of border control, carriers will find themselves in a difficult position. Considering the flow of passengers and the considerable amount of inaccurate data stored in IT systems it is likely that the number of passengers which will be flagged as "NOT OK" will be significant. Airlines will be, therefore, confronted with the choice of risking a fine for carrying "NOT OK to board" passengers or risking legal proceedings for disallowing somebody to board.

This may lead to discrepancies in the policies among airlines, as they may tend to be more lenient towards passengers who are more likely to sue them. Moreover, larger airlines might afford to be stricter as they can often offer a later flight in case the person misses the original flight but is later cleared. Smaller airlines will be under more pressure. If the procedure to clarify any discrepancies takes place only at the airport, it will probably also affect passenger flows, as people would turn up earlier for their flight. People flying from their 'domestic' airport will also have a natural advantage as they can likely clarify any issue easier and faster than people flying from an airport where they do not speak the local language or English. In practice, this may result in discriminatory approaches based on social origin or property, with wealthier people being more likely to be allowed to travel even in case of a "NOT OK" to board.

In the interpretative guidelines[124] in relation to Regulation (EC) No. 261/2004,[125] the European Commission encourages airlines to, among others, verify travel documents and visas by consulting the public authorities (embassies and Ministries of Foreign Affairs) of the countries concerned in order to prevent incorrect denials of boarding. A similar consultation would be necessary in case of "NOT OK" to board.

As a derogation from the general rule set forth in proposed Article 45b (4), transit passengers by air, who have their final destination in a third country, should not be subject to this verification by carriers, unless they are required to hold an airport transit visa according to Annex IV of the Visa Code. Their data would not be stored in VIS and, therefore, they should also not be subject to the query by carriers. The ETIAS compromise text of July 2018 establishes a similar exception for visa-free travellers (last sentence of Article 45 (2)), with which the VIS Regulation should align, also with a view to avoiding discriminatory treatment of two groups of third-country nationals in a comparable situation.

---

[124] *Interpretative Guidelines on Regulation (EC) No. 261/2004 of the European Parliament and of the Council establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights and on Council Regulation (EC) No. 2027/97 on air carrier liability in the event of accidents as amended by Regulation (EC) No. 889/2002 of the European Parliament and of the Council*, point 3.1.1.

[125] Regulation (EC) No. 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No. 295/91 (text with EEA relevance), OJ L 046, 17 February 2004, pp. 1-8.

FRA Opinion 17

Carriers should be able to contact a functioning support centre where they can receive a reply within minutes when they have queries on a "NOT OK" to board reply. This will limit the number of cases in which genuine passengers are not allowed to board as a result of a wrong match based on inaccurate data stored in the system.

The EU legislator should consider establishing a support centre within each Member State and/or within Frontex as may be appropriate which is sufficiently staffed to provide real time response to all queries carriers have in relation to passengers for whom they received a "NOT OK" to board. Such a call centre would require significant resources, so that in most cases a decision on whether or not to board can still be taken before boarding is closed.

In addition, the EU legislator should establish that in the case of airport transit, the airline should not be obliged to verify whether the passenger is in possession of a valid short-stay visa (except for those third-country nationals who are required to hold an airport transit visa according to Annex IV of the Visa Code).

5.4. Avoiding excessive burden on land carriers

Article 26 (1) (b) and (3) of the Convention implementing the Schengen Agreement (CISA), to which also Article 13 of the Entry/Exit System Regulation refers, requires states to oblige carriers transporting foreigners by land, air or sea to take all the necessary measures to ensure that they are "in possession of the travel documents required for entry into the territories of the Contracting Parties".[126] Pursuant to the proposal, carriers will be asked to implement this requirement by consulting VIS. Article 45b of the Commission proposal imposes a duty on carriers to query VIS for the purposes of CISA.

Whereas airlines and international ferry operators are usually large companies with the necessary infrastructure enabling them, though with some additional costs, to query the relevant IT systems, bus operators are more diverse, including companies operating only few busses across the Schengen area. These can be connections from a third country subject to visa requirements (for example, the Russian Federation) to the Schengen area. More frequently, it will be companies operating busses starting from visa-free countries, for example, in the Balkans. However, also in this second scenario, the bus company may carry nationals from a third-country national to visa (e.g. a bus from Sarajevo to Vienna carrying a Turkish national).

The imposition of additional burdens to service providers in the transport sector can raise issues under the freedom to conduct a business laid down in Article 16 of the Charter. This right is not an absolute right. However, limitations have to conform to Article 52 (1) of the Charter. Article 16 of the Charter is particularly relevant for small businesses, as infringements of the freedom to conduct a business are likely to have a relatively larger negative impact on them, compared to larger enterprises.[127]

Imposing an obligation on all carriers at land and sea irrespective of their size, capacity and experience to check the passport data before transporting a person may have a disproportionate impact on small carriers, as they may not be able to absorb the

---

[126] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239/19.

[127] See FRA (2015), *Freedom to conduct a business: exploring the dimensions of a fundamental right*, Luxembourg, p. 11.

additional costs ensuing from the infrastructure necessary to consult the carriers' gateway and to build up the expertise to be able to handle adequately a "NOT OK" when travellers present plausible arguments showing that they do have a valid visa to enter the Schengen area. This may result in an unjustified restriction of their freedom to conduct a business.

FRA Opinion 18

The obligation to verify the passport details of each passenger against VIS disproportionately affects the freedom to conduct a business of small carriers who operate bus connections or small ferry connections over the Schengen border. In such cases, the person could be checked when he or she reaches the border, where border guards have access to the relevant IT systems.

The EU legislator should revise the wording of Article 45c of the proposed amendments to the VIS Regulation to allow the European Commission to exempt small carriers from the duty of querying VIS by implementing acts.

6. Access by law enforcement authorities (LEA)

This chapter deals with access to VIS data by law enforcement authorities (LEA), following the specific request by the European Parliament to cover this subject.

6.1. Regulating access by LEA for suspects of serious crime

One of the original purposes of VIS is reinforcing the internal security of the Schengen area, as manifested in Article 2 (g) of the current VIS Regulation and in Decision 2008/633/JHA.[128] The proposal aims at reinforcing the security-related objective in two ways: first, more generally, by facilitating the exchange of information among Member States on third-country nationals who applied for short-stay visas and who are holders of long-stay visas and residence permits; and second, by making data of these people processed in VIS available to national law enforcement authorities and Europol for combating terrorism and other serious crimes.[129] This section focuses on the latter, i.e. on provisions that allow law enforcement authorities to access the data to combat terrorism and other serious crimes.

Access by law enforcement to VIS has already been possible under the current rules, after this EU database has become operational (this access was put into effect as of 1 September 2013[130]). The original legal basis (Decision 2008/633/JHA) was adopted pre-Lisbon, under the former third (intergovernmental) pillar of the EU (police and judicial cooperation in criminal matters). Decision 2008/633/JHA will be repealed according to Article 8 of the proposal. The procedures and conditions on law enforcement access to VIS will be incorporated in the VIS Regulation itself, under new Chapter IIIb.

VIS has been referred to as an example for the usefulness of law enforcement access to large-scale EU databases. However, as per the practical functioning of law enforcement access thus far (since 1 September 2013), the European Commission admitted, in its assessment of VIS, that the conclusions about the usefulness of law enforcement's access to VIS are based on sources of "limited analytical value" (e.g. due to the low quantity and quality of replies to the relevant questionnaire). By the end of 2015 – the period used to assess the functioning of law enforcement access to VIS – such access was still recent and very fragmented; only a minority of the Member States' law enforcement agencies used the system regularly, with a number of Member States actually making less use of it over time.[131] The number of queries was thus limited: as of the end of September 2015, 11 Member States reported that their law enforcement authorities had performed

[128] 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 L 218/129.

[129] Commission proposal, Explanatory Memorandum, pp. 3-4.

[130] See Council Decision 2013/392/EU of 22 July 2013 fixing the date of effect of Decision 2008/633/JHA 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 L 198/45, which was then replaced, as a result of an action for annulment before the CJEU, by Council Implementing Decision (EU) 2015/1956 of 26 October 2015 fixing the date of effect of Decision 2008/633/JHA 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 L 284/146.

[131] European Commission (2016), *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 visa (VIS Regulation) / REFIT Evaluation*, SWD(2016) 328 final, Brussels, 14 October 2016, pp. 98-99.

a total of 9,474 searches in VIS.[132] Between 1 October 2015 and 30 September 2017, close to 28,000 such searches were performed by eight EU Member States.[133]

The proposal will expand the material scope of data which law enforcement authorities will also be allowed to access: personal data of long-stay visas and residence permits holders which are stored in VIS can also be consulted in future by law enforcement agencies. In addition, as a result of lowering the age limit for fingerprinting in the case of children from 12 to six years of age, law enforcement authorities will get access to a larger pool of biometric data related to children. It is also necessary to assess the impact of the access by law enforcement authorities to a considerably extended amount of information in light of the planned interoperability of IT systems (see especially Articles 20 and 22 of the interoperability proposals). Such interconnectedness of large-scale databases will also facilitate law enforcement access to personal data stored in all interoperable EU IT-systems, including VIS. The necessity and proportionality of law enforcement access should be thus examined in the overall framework of the architecture of existing or planned EU information systems in the field of freedom, security and justice, including the ongoing legislative discussions on the interoperability of these databases.

Given that further information is to become accessible for law enforcement due to being included in VIS (data on long-stay visas and residence permits holders), the EU legislator should assess the consequences of granting such access to law enforcement in this respect and demonstrate the necessity and proportionality of the such extension. In this regard, the proposal should examine in particular detail the impact of the requirement stemming from CJEU jurisprudence[134] under which a distinction must be made between the different categories of data in terms of conditions of access and the length of retention based on their law enforcement relevance.

Extent of access

Under the proposal, national law enforcement authorities and Europol would continue to have access to all information stored in VIS, as is the case under the current legal framework. Requests for certain types of information (related to occupation, the employer or education) would require specific justification and further approval, but are otherwise subject to the same access conditions (proposed Articles 22n and 22p).

Access to personal data by law enforcement authorities 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 principles 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

[132] 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, p. 24 for information on the Czech Republic, Estonia, Finland, Germany, Greece, Hungary, the Netherlands, Poland, Slovenia, Spain and Switzerland.

[133] eu-LISA (2018), *Technical reports on the functioning of VIS as per Article 50(3) of the VIS Regulation and Article 17(3) of the VIS Decision,* May 2018, p. 26 for information on Finland, France, Germany, Greece, Hungary, the Netherlands, Spain and Switzerland.

[134] 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* [GC], 21 December 2016.

freedoms of others.[135] Similar requirements are also imposed by the ECHR. Pursuant to Article 8 (2) of the ECHR, any interference with the right to respect for private life has to pursue a legitimate aim, be in accordance with the law as well as necessary in a democratic society (proportionality test).[136]

The usefulness of a measure (in this case, the effectiveness and usefulness of VIS for law enforcement purposes) is not in itself sufficient to comply with these requirements. 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 in itself mean that the measure would be considered necessary for the purpose.[137] Based on these principles, FRA has repeatedly emphasised that facilitating access to large-scale EU databases should not be at the expense of existing safeguards and should not undermine the principle of purpose limitation which is in place for accessing each EU database.[138]

As highlighted in the FRA opinions on the recast Eurodac proposal and on interoperability,[139] large-scale EU databases contain an increasingly comprehensive set of data on third-country nationals that is not available to Member States' law enforcement agencies and Europol for nationals of an EU Member State. This is in particular the case for biometric identifiers. Comprehensive biometric datasets exist at a national level only in regard to persons convicted or suspected of a crime. Hence, a logical connection between the nature of the data and law enforcement exists. Such logical link is not clearly identifiable in case of law enforcement access to VIS. Although specific individuals included in VIS may be connected to organised crime or even terrorism, these persons represent a small segment of the overall number of people whose data are stored in VIS. This holds particularly true for long-stay visas and residence permits holders who have been previously subject to more thorough security checks than visa applicants. Among third-country nationals having a residence permit, long-term or permanent residents have already been thoroughly vetted, to a degree that they should not be considered a threat to internal security. The characteristics of those residing and living in the EU is generally speaking closer to EU citizens than tourists or business travellers who come only for a short-stay visit. The vetting they have undergone and their stable status in the EU may question the necessity and proportionality of providing access to their personal data stored in VIS to law enforcement agencies combatting serious crime. Such access to residence permits holders data needs thus to be better justified, at least in the recitals of the proposal.

---

[135] CJEU, C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, 17 December 2015, paras. 69 and 80-82.

[136] ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 95-104.

[137] CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General* and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, 8 April 2014, para. 51.

[138] FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the* impact on fundamental rights of the proposal for a revised Eurodac Regulation, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, p. 42; FRA (2017), *Fundamental Rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office of the European Union, see for instance Chapters 1 and 2; FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018, p. 30.

[139] FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, p. 41; FRA (2018), *Opinion of the European Union Agency for Fundamental Rights on interoperability and fundamental rights implications*, FRA Opinion – 1/2018 [Interoperability], Vienna, 11 April 2018, p. 33.

The lack of an even indirect or remote connection between the data retained and the purpose of their retention – serious crime – was among the arguments used by the CJEU in the *Digital Rights Ireland* case to conclude that the quashed Data Retention Directive (Directive 2006/24/EC) was not in line with the Charter.[140] Given that the data are primarily collected in VIS for a number of specific visa policy and border management objectives,[141] the ancillary law enforcement purpose necessarily implies the need to take into account the principles outlined in the CJEU jurisprudence.

The above argument is particularly strong in the case of children. The age limit for the inclusion of their fingerprints in VIS will be lowered to six years (proposed Article 13 (7) (a) of the Visa Code), i.e. much below the age of criminal responsibility in the overwhelming majority of EU Member States (14 years or more).[142] As a consequence, the same dataset would become available to law enforcement authorities in relation to adults and children aged between six and 18 years. When addressing the issue of blanket retention of biometric data by law enforcement authorities of persons not convicted of a crime, in the case of *S. and Marper*, the European Court of Human Rights (ECtHR) emphasised that this may be especially harmful in the case of children, given their special situation and the importance of their development and integration in society.[143] As FRA emphasised in relation to the proposed revision of the Eurodac Regulation and the planned ETIAS, these arguments are also applicable where law enforcement agencies access data that were originally collected for other purposes.[144]

There is insufficient evidence of the need to process personal data of children to prevent, detect and investigate terrorism and serious crime, particularly for children below the age of criminal responsibility. At the same time, in some cases, VIS could possibly help protect children who have gone missing, been abducted or are victims of trafficking in human beings. This is a newly introduced ancillary objective of the VIS Regulation (see Recital (28) and proposed Articles 2 (1) (f) and 22o). If a child who was previously recorded in SIS II as missing or as a victim of human trafficking applies for a short-stay visa to re-enter the EU, alerted law enforcement authorities could develop a targeted response.

Conditions for access

In addition to the question on the extent to which law enforcement authorities should be entitled to consult VIS data (including data of long-stay visa and residence permits holders), the conditions for such access pursuant to proposed Article 22n also need to be examined. The conditions are similar for national law enforcement authorities and Europol. Access continues to be subject to a set of cumulative conditions which require that such access is:

---

140 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General* and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, 8 April 2014, paras. 58-59.

141 See Commission proposal, Explanatory Memorandum, p. 3.

142 See the overview at http://www.childreninjudicialproceedings.eu/Criminal/ComparativeData/default.aspx#Theme_2_Child_offenders.

143 ECtHR, *S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 124-125.

144 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, pp. 22-23; FRA (2017), *Opinion of the European Union Agency for Fundamental Rights on The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], Vienna, 30 June 2017, p. 32.

a) necessary and proportionate for the purpose of the prevention, detection and investigation of terrorist offences or other serious crime;

b) necessary and proportionate in a specific case (ruling out systematic comparisons); and

c) information contained in VIS to which access requested is considered to substantially contribute to the objective of addressing terrorist or other serious criminal offences. This is in particular the case when there is a substantiated suspicion that the person falls in a category covered by this database.

Law enforcement access will remain indirect, based on submitting a reasoned request for access to VIS data to a central access point, and only receiving further information if there is a match with the data contained in the VIS ('hit/no-hit system').[145] However, contrary to the EES (Article 32 (2)), there is no further requirement of prior consultation of national databases and the automated fingerprint identification systems (AFIS) of other Member States under Council Decision 2008/615/JHA (Prüm Decision), before requesting access to VIS by law enforcement authorities (cascade system). Nevertheless, such a cascade system would be a key safeguard to ensure that VIS data is only consulted where the information cannot be obtained from dedicated databases, i.e. those set up at a national level. With the future interoperability of large-scale databases, law enforcement access to all EU IT-systems will become more streamlined, which is one of the explicit objectives of the interoperability proposals (Recital (10) and Article 2 (2) (f)). Hence, it is legitimate to align the minimum access conditions, while keeping a higher level of safeguards for IT-systems holding the most sensitive categories of data, e.g. Eurodac on asylum seekers.

The proposed new Article 22m of the VIS Regulation, places greater emphasis on an independent verification of law enforcement requests (with the possibility of an ex post verification in exceptional cases of urgency). The proposal keeps the current rules on national verifying authorities (central access points), which examine if the request by law enforcement authorities comply with the access conditions. Compared to Decision 2008/633/JHA, which did not contain the requirement of independence, further safeguards are proposed to be added reflecting the approach taken in recent proposals on migration-related EU databases: the central access points may, in practice, be part of the same organisational structure as the designated authorities submitting requests for law enforcement access, but they need to be separate from the operating units and act fully independently, i.e. must not receive instructions from the designated authorities (proposed Article 22k (3)). These criteria aim at responding to the standards set out by the CJEU in the *Digital Rights Ireland* judgment, namely that verification is to be conducted "by a court or by an independent administrative body whose decision seeks to limit access to the data."[146] The practical difference from the existing verification mechanism will nevertheless depend on the interpretation of the term 'fully independently', in combination with the requirement of 'separateness', by the Member States, and ultimately by the CJEU. Proposed Articled 22l (2) uses a slightly different wording of the safeguards in case of Europol's designated central access point and the reason for the different formulation is not clear.

---

[145] Proposed Articles 22m and 22n (4).

[146] CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* Ltd (C-293/12) *v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General* and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12*), 8 April 2014, para. 62.

FRA Opinion 19

The principle of proportionality enshrined in Article 52 (1) of the Charter, as interpreted by the Court of Justice of the EU, requires that access to personal data for law enforcement purposes is subject to adequate safeguards and that the retention of the data reflects its law enforcement relevance.

The EU legislator should ensure that any solution for allowing access to EU IT systems by law enforcement for the purposes of fighting terrorism and serious crime requires the authorities to first consult databases more directly linked to criminal investigations, similarly to the mechanism in place for the Entry/Exit System. More specifically, this would mean:

- ***conduct a prior search in relevant national databases, and***
- ***in case of searches with fingerprints, at least launching a prior search in the automated fingerprint identification system of the other EU Member States under Council Decision 2008/615/JHA (Prüm Decision).***

The EU legislator should allow law enforcement access to children's data, particularly those below the age of criminal responsibility, only to protect missing children or children who are victims of serious crimes (e.g. trafficking in human beings);

The EU legislator should align the slightly different wording of the safeguards in case of Europol's designated central access point (proposed Article 22l (2)) with the set of criteria applicable to national central access points (proposed Article 22k (3)), except for the requirement of separateness. This would mean inserting the word "fully" into the phrase "shall act independently", and adding the following half-sentence at the end of Article 22l (2): "which it shall perform independently".

6.2.Regulating access by LEA to data on victims or missing persons

FRA field research shows that large-scale EU IT systems are important to help identify missing persons and victims of crime.[147] For instance, SIS II allows for registering alerts for missing persons,[148] which could include victims of crime. FRA also recommends in its opinion on the fundamental rights impact of the recast Eurodac Regulation to include an additional objective in this instrument to protect child victims of trafficking and support the identification and protection of missing children.[149] Specific situations may occur where persons covered by the VIS Regulation need to be identified in their own interest – because they have gone missing, been abducted or identified as victims of trafficking in human beings. It is laudable that the proposal pursues a new, explicit and separate objective to make it easier to identify missing persons (new Article 2 (1) (f) of the VIS Regulation).

Proposed Article 22o of the VIS Regulation seeks to provide quick and "barrier-free" access for law enforcement authorities to VIS data to enable a fast and reliable identification of such persons, without the need to fulfil all the preconditions and additional safeguards for law enforcement access. This specific scenario complements access for law enforcement purposes by national authorities under the general rules

147 FRA (2018), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, March 2018, pp. 70-72.

148 SIS II Decision, Art. 32 (2) (a) (i); SIS II proposal (police and judicial cooperation), Art. 32 (2) (a) (i).

149 FRA (2016), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposal for a revised Eurodac Regulation*, FRA Opinion – 6/2016 [Eurodac], Vienna, 22 December 2016, Opinion 4.

(proposed Articles 22k – 22n of the VIS Regulation), as it deals with persons in need of assistance who have been encountered directly by the police and other law enforcement agencies. In this case, there is a need for swift and simplified access to the database to protect the legitimate interests of the person concerned. This is different from the situation where the police wishes to consult VIS to prevent, detect and investigate terrorist offences or other serious crimes.

This newly inserted Article 22o of the VIS Regulation covers three categories of vulnerable persons:

- missing persons;
- persons who have been abducted;
- victims of trafficking in human beings.

All three categories of people are covered without any age limitation, so not only children but adults also fall under the personal scope of this protection-oriented regime.

The "barrier-free" access provided to law enforcement authorities under proposed Article 22o should be read in light of the new objective set out in proposed Article 2 (1) (f) and implicitly in Article 2 (2) (d) and (f) of the VIS Regulation. Such provisions, which seem to apply to all persons covered in VIS, refer solely to the identification of 'missing persons', without mentioning abducted persons and victims of trafficking. For the sake of consistency and legal certainty, the wording of this specific objective should be aligned with the broader list of persons covered in proposed Article 22o.

An additional precondition in proposed Article 22o to trigger this protection-driven and simplified law enforcement access to VIS is that in respect of the persons concerned, the "consultation of VIS data will support their identification, and/or contribute in investigating specific cases of human trafficking". The language in the second half-sentence is very vague: it is unclear on who exactly is targeted under this category related to investigations in trafficking. This goes beyond mere identification of victims and concerns "investigating specific cases of human trafficking". Given the exceptional character of removing all preconditions and additional safeguards for law enforcement access, which is essentially justified by a protection-driven objective, the implementation of this option can lead to circumventing the general access conditions for fighting serious crime. Trafficking in human beings is one of the serious criminal offences under Council Framework Decision 2002/584/JHA, to which crime the general regime of law enforcement access applies (see also the definition of 'serious criminal offences' in newly added paragraph (22) of Article 4 of the VIS Regulation). Hence, to be lawful, obtaining information on perpetrators of, accomplices to, and other people involved in this crime must always be processed in application of the general rules.

FRA Opinion 20

Enabling law enforcement access to VIS to identify persons who have gone missing, been abducted or are victims of trafficking in human beings has beneficial effects to protect the legitimate interests of such vulnerable people. However, the modalities of such a "barrier-free" and simplified access for law enforcement authorities to VIS data need to be sufficiently detailed and contain built-in safeguards. These are needed to prevent that such simplified access is used to circumvent the requirements which need to be fulfilled

when VIS is accessed to prevent, detect and investigate terrorist offences or other serious crimes.

Therefore, the EU legislator should

- ***align the formulation of the new objective in proposed Article 2 (1) (f) of the VIS Regulation with the persons covered by proposed Article 22o and complement Article 2 (2) with a new specific objective of identifying this group of vulnerable people;***
- ***remove the wording "and/or contribute in investigating specific cases of human trafficking" from proposed Article 22o, as it conflicts with the general rules of law enforcement access to investigate terrorism and other serious crimes (proposed Articles 22m-22n).***

7. Reporting, statistics and evaluation

The proposed changes to the VIS Regulation will provide EU Member States, as well as relevant EU actors, including Frontex, with a significant amount of anonymised data to be used for analytical purposes. This chapter deals with the use of VIS data to produce statistics and reports, as well as with the evaluation of the VIS Regulation.

7.1. Ensuring anonymity when producing report and statistics

The proposal introduces a specific provision (new Article 45a of the VIS Regulation) concerning the use of VIS data for reporting and statistics. For these purposes, the relevant VIS data will be stored in the Central Repository for Reporting and Statistics (CRRS),[150] established under Article 39 of the interoperability proposals, pursuant to which the CRSS will "generate *cross-system* statistical data and analytical reporting" [emphasise added].

The production of reliable statistics supports evidence-based policy decisions. Statistics have also the potential to identify fundamental rights challenges and, consequently, help to strengthen adherence to Charter rights during the implementation of the regulation. According to Article 45a (7), the European Commission may request eu-LISA to prepare tailor made statistics on the implementation of the common visa or migration policy. Such reports present a good opportunity to produce statistics on various fundamental rights aspects relating to the implementation of the VIS Regulation. For example, the data stored in the CRRS pursuant to proposed Article 45a (o), (p) and (q) on factual and legal impossibility to provide fingerprints can be correlated with visa refusals to analyse whether persons who are unable to provide their fingerprints are discriminated against. Similarly, data on factual impossibility to provide fingerprints can be correlated with age, thus contributing to assessing the quality of biometric data of children and older people.

However, the processing of data for reporting and statistic purposes create also fundamental rights risks which need to be adequately addressed. The main challenge concerns anonymisation. According to Article 39 (2) of the interoperability proposals, the CRRS will only contain data which do not enable the identification of individuals. The anonymisation will be done automatically by eu-LISA (Article 39 (3) of the interoperability proposals). Article 89 (1) of the GDPR requires adequate technical and organisational safeguards for the anonymisation to be achieved effectively. In this context, solutions must be applied which prevent also an indirect identification through the combination of different data elements. The VIS data stored in the CRRS pursuant to proposed Article 45a will be much more detailed than the data submitted to the CRRS by the other two related large scale IT systems in the area of visas and borders – the EES and the ETIAS (see Annex 2). While the EES and ETIAS will submit information on the year of birth (which can be already seen as problematic from an indirect identification point of view) VIS goes further by submitting information on the "date" of birth. This seems excessive as it might lead to indirect identification. For example, in case of data subjects from small island states, even where the name and the passport number is removed from the repository, an individual may still be identified through a combination of nationality, sex and date (or even the year) of birth. Furthermore, Article 45a (1) (i) and Article 45a (1) (j) envisage also storing the geographic location of the competent authority processing the case. This might also

[150] Commission proposal, Art. 1 (34) [introducing Art. 45a (2) in the VIS Regulation].

lead to individual identification in combination with other data, in particular when data is connected to a smaller location with a lower number of applications.

Furthermore, in some instances unclear wording used in the proposal may lead to inconsistent implementation of the VIS Regulation, affecting data subject's rights:

- Proposed Article 45a (1) refers in lit (h) and (l) to a "document" without defining what document is meant.
- VIS data which will be stored in the CRRS is listed in proposed Article 45a (1) of the VIS Regulation. A cross-reference to the respective article is however missing in Article 39 (2) of the interoperability proposal on borders and visa, which defines which data from the underlying systems will be stored in the CRRS.[151]

FRA Opinion 21

The production of reliable statistics supports evidence-based policy decisions. The data used to produce reports and statistics, however, must not allow direct or indirect identification of the data subjects. Data categories to include in the Central Repository for Reporting and Statistics (CRRS) must be defined in a clear manner.

The EU legislator should consider enhancing safeguards to Article 45 (a) to prevent that data stored in the CRRS may lead to identification of data subjects. The safeguards should include:

- ***in Article 45a (1) (c), replacing the reference to "data of birth" with "year of birth" and complementing this provision with a safeguard according to which "this should not lead to the identification of the person concerned";***
- ***in Article 45a (1) (i) and Article 45a (1) (j), replacing "the location" of the competent authority with "the country" of the competent authority.***

For reasons of legal clarity, the EU legislator should also:

- ***clarify the term "document" in Article 45 (1) (h) and (l) or replace it with more specific wording;***
- ***include in Article 7 of the proposal an amendment to Article 39 (2) of the interoperability proposal (borders and visa) clarifying that data listed in proposed Article 45a (1) of the VIS Regulation should be contained in the CRRS.***

7.2. Evaluating the impact of VIS on fundamental rights

Pursuant to proposed Article 50 (5), the European Commission will prepare an overall evaluation of the VIS every four years and submit it to the European Parliament and Council.[152] According to the Explanatory Memorandum, the evaluation of the VIS should include also "its direct and indirect impacts and practical implementation on fundamental rights".[153] However, such an explicit reference to fundamental rights

[151] Art. 39 (2) of the interoperability proposal on borders and visa contains a reference to "Article 17 of Regulation (EC) No. 767/2008", which will be deleted with the Commission proposal. Art. 7 of the Commission proposal, which amends the interoperability proposal on borders and visa, does not include any amendment of Art. 39 (2).

[152] The proposed Art. 50 (5) corresponds to a large extent to the current Art. 50 (4) of the VIS Regulation.

[153] Commission proposal, Explanatory memorandum, p. 15.

is missing in the proposed amendments to Article 50 of the VIS Regulations. As FRA pointed out in its Interoperability Opinion, it would be also useful to specify on which fundamental rights the evaluation should focus on.

The proposal suggests to amend Article 50 of the VIS Regulation on monitoring and evaluation. As a novelty, under the proposed Article 50 (4) the Member States and Europol will have to prepare annual reports on the effectiveness of law enforcement's access to the VIS.[154] The information and statistics included in this provision are relevant and essential to evaluate the necessity and proportionality of using the data to prevent or combat serious crimes and terrorism. The provision does, however, not cover the collection of statistics on the central access points' ex-post verifications of law enforcement authorities' access in case of exceptional urgencies as per Article 22m of the VIS Regulation. By obtaining statistics on the frequency and the number of *ex-post* approved requests as well as cases where that urgency was not approved, the necessity of the access to VIS could be better assessed. Such information will be collected also in the framework of other large scale IT systems and interoperability.[155]

Moreover, as children will be fingerprinted as of six years of age (see Section 3.3), information included in Article 50 (4) would be useful to determine the proportionality of processing data on children to illustrate how it helps to fight abuses against children, including child trafficking.

Finally, one of the challenges is the risk of the indirect discrimination of persons whose data are stored in VIS. The possibility to undertake law enforcement checks against visa applicants or holders of long stay visas or residence permits – but not against others whose personal data are not stored in EU-wide systems, may result in an artificial increase of crime detection rate of crimes committed by third-country nationals, compared to EU nationals. This may stigmatise third-country nationals as potentially more criminal than EU nationals. For this reason, it is suggested to complement the draft provisions on the overall evaluation of the VIS Regulation in proposed Article 50 (5)) with examining possible indirect discrimination against persons covered by the VIS Regulation.

FRA Opinion 22

Article 50 regulates the monitoring and evaluation of the VIS Regulation but does not include an express duty to evaluate also how the implementation of the regulation will affect fundamental rights, in spite of the fact that this is announced in the Explanatory Memorandum. Moreover, the indicators listed in Article 50 (4) could be further developed so that these could be used more effectively to evaluate the impact of law enforcement access on fundamental rights.

The EU legislator should add in Article 50 (5) of the VIS Regulation an explicit reference to "the impact on fundamental rights". Such reference could expressly mention that the evaluation should "in particular cover the right to protection of personal data, the right to non-discrimination, the rights of the child and the right to an effective remedy". Moreover, the evaluation should also examine whether law enforcement access to VIS has led to indirect discrimination against persons covered by the regulation.

[154] European Commission proposal, Art. 1 (38) [introducing Art. 50 (4) in the VIS Regulation].

[155] EES Regulation, Art. 72 (8) (f), ETIAS compromise text, Art. 92 (8) (e), Eurodac Regulation, Art. 40 (7); Eurodac proposal, Art. 42 (8); Amended Interoperability proposals, Art. 68 (8) (e).

In Article 50 (4), the EU legislator should:

- *include a reference similar to the wording in Article 72 (8) (f) of the EES Regulation to "the number and type of cases in which the urgency procedures referred to in Article 22m (2) were used, including those cases where that urgency was not accepted by the ex post verification carried out by the central access point";*
- *consider requesting EU Member States and Europol to present separate statistics on child trafficking under Article 50 (4) (a) and to specify under Article 50 (4) (b) and (c) how many of the cases concern persons below 18 years of age. Under Article 50 (4) (c), the EU legislator should furthermore consider adding the words "with a breakdown of granted and rejected requests".*

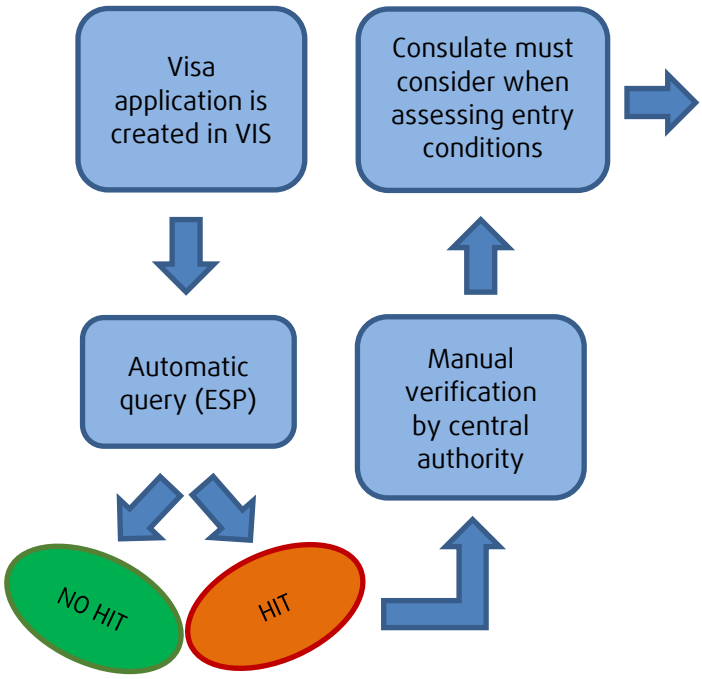
8. Risk indicators

This last chapter reviews the changes proposed to the Visa Code (Regulation (EC) No. 810/2009) to support visa authorities in assessing in an objective manner whether or not an applicant fulfils the entry conditions.

8.1. Using only relevant data to verify entry conditions

Pursuant to Article 21 of the Visa Code, consulates must verify whether the applicant fulfils the entry conditions and conduct a risk assessment. For this purpose, national authorities must consult also VIS. The proposal amends Article 21 (2) of the Visa Code which regulates such consultation: in future the consultation will be carried out automatically, pursuant to proposed Article 9a of the VIS Regulation. Under this provision, when a visa application is created, VIS automatically queries other VIS entries as well as entries in SIS, EES, ETIAS, Eurodac, ECRIS-TCN, the Europol databases and two Interpol databases. VIS will automatically query the different systems using the European Search Portal (proposed Article 9a (3) of the VIS Regulation). Figure 3 illustrates the procedure.

Figure 3: Procedure for queries under Articles 9a and 9c of the VIS Regulation and Article 21 of the Visa Code



IT system	To check if...
SIS, SLTD, TDAWN	travel document recorded
ETIAS	refused/revoked/annulled application for travel authorisation
VIS	another visa application; refused/ revoked/annulled SSV
EES	overstaying/ed; refused entry
Eurodac	application for int. protection withdrawn/rejected
Europol	data recorded
ECRIS-TCN	data recorded for terrorist or other serious criminal offences
SIS	EAW alert for surrender purposes; wanted for arrest for extradition purposes

Source: FRA, 2018

Under proposed Article 9c of the VIS Regulation, all hits obtained through the automated query will have to be manually verified by the respective Member State's central authority. The VIS Regulation does not include any time limit for the manual verification, as opposed to the ETIAS Regulation (compromise text) which foresees that it will have to be carried out within 12 hours from the receipt of the application file.[156] Such a time limit can help to ensure speedy application procedures.

Under proposed Article 21 (3a) of the Visa Code, visa authorities must take the results of such manual verification into account when assessing whether the applicant fulfils the

[156] ETIAS compromise text, Art. 22 (6).

entry conditions listed in Article 21 (3) of the Visa Code. The specific results which the visa authorities must assess are listed in proposed Article 21 (3a). While most factors to consider seem reasonable, certain provisions entail some fundamental rights concerns or would need to be further clarified.

According to proposed Article 21 (3a) (e) of the Visa Code, the consulates will have to check Eurodac to see whether the visa applicant also applied for international protection in the past and the application was withdrawn or rejected. It is difficult to see how this information could be necessary to assess the fulfilment of entry conditions contained in Article 21 (3). First, Eurodac contains and will in future only contain information on the date when an asylum applicant left the Member State after the asylum application was rejected or withdrawn, meaning it will in practice probably not contain information on all rejected or withdrawn asylum applications.[157] Second, using past rejections or withdrawal of asylum claims as an indicator for assessing a visa application would result in attaching negative consequences to a decision to apply for asylum, which could indirectly undermine the right to asylum set forth in Article 18 of the Charter. Information on the rejection or withdrawal of an asylum application should therefore not be treated in the same manner as an entry ban stored in SIS, which in many cases indicates that the third-country national has not complied with the obligation to return.

Furthermore, the proposed Article 9a (3) of the VIS Regulation envisages that ECRIS-TCN will have to be queried "as far as convictions related to terrorist offences and other forms of serious criminal offences are concerned". Consulates will have to check whether the applicant is recorded for terrorist offences or other serious crime, in line with the proposed Article 21 (3a) (g) of the Visa Code. ECRIS-TCN will, however, not include such information, since it will not store information on the type or severity of the committed crime.[158] According to the European Commission's ECRIS-TCN Analytical Supporting Document, a proposal to include the full conviction data and thereby avoid the "two-step-approach" (i.e. EU Member States sending a normal request for conviction data to the relevant Member State after a hit in ECRIS-TCN) was not supported by Member States and would not be in line with the principle of data minimisation.[159] The central authority and consulates could obtain such information only if they would request it from the Member State issuing the conviction and the reply could still be subject to limitations, since the information is not required for the purposes of criminal proceedings.[160] It should also be noted that ECRIS-TCN will contain information on offences of different severity, ranging from terrorist offences to misdemeanours.[161] If a consulate would only know that a hit in the system exists, without knowing to which crime it refers, this could consciously or unconsciously affect their decision-making and increase the likelihood of an unjustified visa refusal.

---

157 See Eurodac Regulation, Art. 11 and 14 (2); Eurodac proposal, Art. 12 and 13 (2).

158 ECRIS-TCN will hold only information on the convicted person and the code of the convicting Member State, provided the conviction is entered also in the national criminal records register (Art. 5 of the ECRIS-TCN proposal).

159 European Commission (2017), *Analytical Supporting Document Accompanying the document 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 people (TCN) to supplement and support the European Criminal Records Information System (ECRISTCN system) and amending Regulation (EU) No. 1077/2011*, COM(2017) 344 final, Brussels, 29 June 2017, p. 6.

160 Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93/23, Art. 7.

161 ECRIS-TCN proposal, Art. 2, Art. 3 (1) (a) and (c).

FRA Opinion 23

The manual verification of hits obtained after the automatic European Search Portal query is a welcome step to avoid automated decision making. The current provision does, however, not provide for any time limit for the manual verification. An appropriate time limit could help to ensure speedy procedures across EU Member States.

When assessing entry conditions, consulates will have to take into account the results from the manual verification and consider specific information contained in the connected IT databases. Regarding Eurodac, the information is not relevant to assess the entry conditions and could undermine the right to asylum enshrined in Article 18 of the Charter. The information requested from ECRIS-TCN will not be available in the IT system itself.

The EU legislator should include a time limit for the manual verification procedure in Article 9c of the VIS Regulation to ensure speedy processing of visa applications.

The EU legislator should amend proposed Article 21 (3a) of the Visa Code by:

- ***deleting proposed point (e) relating to Eurodac,***
- ***finding an appropriate solution so as to ensure that the relevant authorities examining a visa application can only see ECRIS-TCN hits which concern a terrorist offence or another serious crime and not entries which concern less serious crimes.***

8.2. Designing specific risk profiles

Articles 20 and 21 of the Charter guarantee equality before the law and protects individuals from discrimination. Both principles are protected also in various international and European law instruments, including secondary EU legislation.[162] Non-discrimination law prohibits direct as well as indirect discrimination.

Proposed Article 21a of the Visa Code introduces specific risk indicators, similar to those foreseen in ETIAS.[163] Visa authorities will use these indicators to assess in a more objective manner whether or not the applicant presents an irregular immigration, security or high epidemic risk. Proposed Article 21a (1) lists six data sources on which the risk assessment must be based, and which can be summarised as follows:

- statistics from the Entry-Exit System and Member States' information on overstayers and refusals of entry for a specific group of travellers;

---

[162] For UN instruments see, for example, United Nations (UN), Universal Declaration of Human Rights, 10 December 1948, Art. 2, Art. 7; International Covenant on Civil and Political Rights, 16 December 1966, Art. 2, Art. 26; International Covenant on Economic, Social and Cultural Rights, 16 December 1966, Art. 2 (2); UN Convention on the Rights of the Child, 20 November 1989, Art. 2. For Council of Europe instruments see, for example, Council of Europe, European Convention on Human Rights, Art. 14; Protocol No. 12 to the ECHR, ETS No.177, 2000; European Social Charter (revised), ETS No.163, 1996, Art. E. For secondary EU legislation see Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180/22 , Art. 1; Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), OJ L 204/23, Art. 1; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303/16, Art. 1; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373/37, Art. 1.

[163] ETIAS compromise text, Art. 33.

- VIS statistics on refusals of visa applications due to an irregular migration, security or public health risk associated with a specific group of travellers;
- VIS and EES statistics on the correlation between the information obtained through the application form and overstay or refusals of entry;
- Member States' information on specific security risk indicators or threats;
- Member States' information on specific high epidemic risks as well as the European Centre for Diseases Prevention and Control's (ECDC) epidemiological surveillance information and risk assessments and the WHO's reports on disease outbreaks.[164]

Based on these data sources, the European Commission is tasked to develop specific risk indicators. Under proposed Article 21a (4), these indicators will be based on a combination of data, including age range, sex, nationality, place of residence and current occupation. Table 3 lists the categories of data which will be used in the Visa Code and compares them to those used in ETIAS.

Table 3: Risk indicators under proposed Article 21a of the Visa Code and under Article 33 of the ETIAS compromise text

Risk indicators	Visa Code	ETIAS *
Age range, sex, nationality	X	X
Country and city of residence	X	X
Member State(s) of destination	X	
Member State of first entry	X	
Purpose of travel	X	
Level of education (primary, secondary, higher or none)		X
Current occupation	X	X**

Notes: * *ETIAS compromise text.*

** *ETIAS includes a more detailed reference to the "current occupation (job group)".*

Source: FRA, 2018

The proposal includes safeguards by explicitly stating that the risk indicators will have to be targeted and proportional. They must not be based *solely* on the person's sex or age. In line with Article 21 of the Charter, the proposal re-affirms that information must not reveal the race, colour, ethnic or social origin, genetic features, language, political or any other opinions, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation of the persons.[165] In spite of these safeguards, there is, nevertheless, still a risk that the indicators could be based *predominantly* on these characteristics.

Moreover, using the "current occupation" as a risk indicator is not justified as it entails a high risk of discrimination based on prohibited grounds. For example, members of a national or ethnic minority or people of certain nationalities in a specific location could be primarily involved in a certain profession (e.g. farming, fishing, berry-picking), as opposed to the majority of people living in this location. This could lead to people being

[164] Commission proposal, Art. 3 (4) [introducing Art. 21a in the Visa Code].

[165] See also Recitals (18) and (23).

unintentionally discriminated based on their social origin, membership of a national minority, or nationality.

The visa authorities will use these risk profiles when examining an individual visa application. They will compare whether the applicant falls under one of the higher risk groups. The proposal does not define the concept of "specific groups of travellers". While many of the sources listed in Article 21a (1) of the Visa Code are justified, there is nevertheless still a risk for discriminating groups of travellers. This is particularly the case when using VIS statistics indicating abnormal rates of visa refusals due to an irregular migration, security or public health risk. For example, an applicant would be more likely refused a short-term visa simply because he/she meets some characteristics of other refused applicants even though there are no *individual* reasons for such conclusions.

According to Article 8 (4) of the VIS Regulation, the individual files of groups and family members will be linked in VIS. The authority deciding on a visa application will see also the hits relating to other members of the group or family. Under Article 24 (3) of the EES Regulation which regulates the use of the Entry Exit System for examining and deciding on visa applications, visa authorities have also access to refusals of entry which in EES are linked to the applicant. The information on past decisions concerning members of the same groups and family members may also lead to a bias in the assessment of the person's application.

To avoid that officers give excessive weight to risk profiles or to past negative decisions or refusals of entry concerning members of the family or of the same group who are linked with the individual in VIS, a safeguard could remind relevant authorities to examine each application individually and on the basis of all available information.

FRA Opinion 24

Proposed Article 21a of the Visa Code introduces specific risk indicators that visa authorities should use when assessing whether or not the applicant presents an irregular immigration, security or high epidemic risk. Although safeguards will have to be applied when using these specific risk indicators, certain risks for discrimination or unequal treatment, both prohibited by the Charter, exist.

To comply with Articles 20 and 21 of the Charter guaranteeing equality before the law and non-discrimination, the EU legislator should add the word "predominantly" in proposed Article 21a (4) of the Visa Code.

The EU legislator should delete point (f) in proposed Article 21a (3) of the Visa Code and thereby remove "current occupation" from the specific risk indicators due to the high risk it might lead to indirect discrimination.

The EU legislator should include a new provision in Article 21 of the Visa Code, expressly stating that every application must always be subject to an individual assessment based on all available information.

Annex 1: Data automatically queried under proposed changes to VIS and the amended interoperability proposals

		SSV holders[a]		LSV/RP holders[b]		Interop.
Data queried		**VIS Reg., Art. 9a (3)[c]**	**VIS Reg., Art. 9a (5)[d] (supporting SIS objectives)**	**VIS Reg., Art. 22b (2)[e]**	**VIS Reg., Art. 22b (4)[f] (supporting SIS objectives)**	**Amended interop. proposals, Art. 27[g]**
Personal data of the applicant	Surname (family name)	Art. 9 (4) (a)	Art. 15 (2) (b)	Art. 22c (2) (a)	Art. 22c (2) (a)	Art. 27 (3) (b)
	First name/s (given names)	Art. 9 (4) (a)	Art. 15 (2) (b)	Art. 22c (2) (a)	Art. 22c (2) (a)	Art. 27 (3) (b)
	Date of birth	Art. 9 (4) (a)	Art. 15 (2) (b)	Art. 22c (2) (a)	Art. 22c (2) (a)	Art. 27 (3) (b)
	Nationality/ nationalities	Art. 9 (4) (a)	Art. 15 (2) (b)	Art. 22c (2) (a)	Art. 22c (2) (a)	Art. 27 (3) (b)
	Sex	Art. 9 (4) (a)	Art. 15 (2) (b)	Art. 22c (2) (a)	Art. 22c (2) (a)	Art. 27 (3) (b)
	Surname at birth (former surname(s))	Art. 9 (4) (aa)				
	Place and country of birth	Art. 9 (4) (aa)		Art. 22c (2) (a)	Art. 22c (2) (a)	
	Nationality at birth	Art. 9 (4) (aa)				
	Home address	Art. 9 (4) (k)				
Other personal data	Current occupation & employer	Art. 9 (4) (l)				
	If students: name of educational establishment	Art. 9 (4) (l)				
	If minors: name of parents/ guardian	Art. 9 (4) (m)			Art. 22c (2) (d)	
Travel document (TD) data	TD(s) type & No.	Art. 9 (4) (b)	Art. 15 (2) (c)	Art. 22c (2) (b)	Art. 22c (2) (b)	
	3-letter code of the TD's issuing country	Art. 9 (4) (b)	Art. 15 (2) (c)	Art. 22c (2) (b)	Art. 22c (2) (b)	
	Expiry date	Art. 9 (4) (c)	Art. 15 (2) (c)	Art. 22c (2) (c)	Art. 22c (2) (c)	
	Issuing authority	Art. 9 (4) (cc)			Art. 22c (2) (cc)	
	Date of issue	Art. 9 (4) (cc)				
	Application place & date	Art. 9 (4) (d)				
	Application No..		Art. 15 (2) (a)			
Sponsor's details	Sponsor's surname and first name (if natural person)	Art. 9 (4) (f) (i)	Art. 15 (2) (d)		Art. 22c (2) (e)	
	Sponsor's address (if natural person)	Art. 9 (4) (f) (i)	Art. 15 (2) (d)		Art. 22c (2) (e)	
	Name of company/other organisation (if applicable)	Art. 9 (4) (f) (ii)	Art. 15 (2) (d)		Art. 22c (2) (e)	
	Company's/ other organisation's address (if applicable)	Art. 9 (4) (f) (ii)	Art. 15 (2) (d)		Art. 22c (2) (e)	
	Surname and first name of the company's/ organisation's	Art. 9 (4) (f) (ii)				

	contact person (if applicable)					
Travel information	Destination MS	Art. 9 (4) (g)				
	Intended stay's/ transit's duration	Art. 9 (4) (g)				
	Main purpose(s) of the journey	Art. 9 (4) (h)				
	Intended arrival date in the Schengen area	Art. 9 (4) (i)				
	Intended departure date from the Schengen area	Art. 9 (4) (i)				
	MS of first entry	Art. 9 (4) (j)				
	Fingerprints		Art. 15 (2) (e)	Art. 22c (2) (g)	Art. 22c (2) (g)	Art. 27 (2)
	Facial image		Art. 15 (2) (ea)	Art. 22c (2) (f)	Art. 22c (2) (f)	Art. 27 (2)
Visa info.	Visa sticker No.		Art. 15 (2) (f)			
	Issue date of previous visa		Art. 15 (2) (f)			

Notes: [a] *= SSV - short stay visa*

VIS will store the following data on short stay visa holders: data referred to Art. 9(1) to (6) and Art. 10 to 14; hits referred to in Art. 9a; results of verification pursuant to Art. 9c (6); links to other applications referred to in Art. 8(3) and (4)

[b] *= LSV – long stay visa; RP – residence permit*

VIS will store the following data on long stay visa or residence permit holders: data referred to in Art. 22c, 22d, 22e and 22f; hits referred to in Art. 22b; results of verification referred to in Art. 9c (6); links to other applications referred to in Article 22a (3)

[c] *= purpose → to check if: entry conditions fulfilled, risk for irregular migration/security, intention to leave (Visa Code, Art. 21 (1)); TD genuine (Visa Code, Art. 21 (3) (a)), entry ban in SIS (Visa Code, Art. 21 (3) (c)); threat to public policy, internal security or public health or int. relations (Visa Code, Art. 21 (3) (d))*

[d] *= purpose → Supporting the SIS objectives (VIS Regulation, Art. 2(1)(k))*

[e] *= purpose → Assessing whether the person could pose a threat to public policy, or internal security or public health, with limitations regarding the consultation of EES, ETIAS and VIS (VIS Regulation, Art. 22b (2) and (5))*

[f] *= purpose → Supporting the SIS objectives (VIS Regulation, Art. 2(2)(f))*

[g] *= purpose → MID is facilitating identity checks and combating identity fraud, supporting the functioning of the CIR and the objectives of the underlying systems (amended interoperability proposal, Art. 25 (1))*

Source: FRA, 2018

Annex 2: EES, ETIAS and VIS data stored in the Central Repository for Reporting and Statistics*

Data category		EES	ETIAS[a]	VIS
Data stored under more legal instruments				
	Status information	Art. 63 (1) (a)	Art. 84 (1) (a)[b]	Art. 45a (1) (a)
Personal data	Sex	Art. 63 (1) (b)	Art. 84 (1) (b)	Art. 45a (1) (c)
	Date of birth			Art. 45a (1) (c)
	Year of birth	Art. 63 (1) (b)	Art. 84 (1) (b)	
	Nationality/current nationality/nationalities	Art. 63 (1) (b)	Art. 84 (1) (b)	Art. 45a (1) (c)
Travel document info.	Type of travel document	Art. 63 (1) (d)	Art. 84 (1) (f)	Art. 45a (1) (g) (only SSV)
	3 letter code of the issuing country	Art. 63 (1) (d)	Art. 84 (1) (f)	Art. 45a (1) (g) (only SSV)
	Number of persons exempt from fingerprinting	Art. 63 (1) (h)		Art. 45a (1) (n)
	Specific data			
	3 letter code of the MS issuing the visa, if applicable	Art. 63 (1) (g)		
	Competent authority, including its location			Art. 45a (1) (b)
Personal data	Country of residence		Art. 84 (1) (c)	
	Education (primary, secondary, higher or none)		Art. 84 (1) (d)	
	Current occupation (job group)		Art. 84 (1) (e)	
Data on entry/exit	MS of first entry			Art. 45a (1) (d) (only SSV)
	Date and BCP of entry and exit	Art. 63 (1) (c)		
	No. of TCN refused entry, their nationalities, type of border (land, air or sea) of the BCP & reasons for refusal	Art. 63 (1) (i)		
D at	Application date and place, and decision (issued/refused)			Art. 45a (1) (e)
	Type of document issued (ATV, uniform/LTV, LSV/RP)			Art. 45a (1) (f)
	Grounds for any decision on the document/application			Art. 45a (1) (h) (only SSV)
	Decision concerning the application (issued/refused and on which ground);			Art. 45a (1) (h) (LSV, RP)
	If refusal: competent authority, including its location & date			Art. 45a (1) (i) (only SSV)
	More SSV applications with more visa authorities (which visa authorities, their location and dates of refusals)			Art. 45a (1) (j) (only SSV)
	Main purpose(s) of the journey			Art. 45a (1) (k) (only SSV)
	Purpose of the application			Art. 45a (1) (k) (LSV/RP)
Document data	Data entered on any withdrawn/ annulled/revoked/ extended document, as applicable			Art. 45a (1) (l)
	Expiry date of the LSV/RP, if applicable			Art. 45a (1) (m)
Fingerprinting	Cases where fingerprints could factually not be provided			Art. 45a (1) (o)
	Cases where fingerprints were not required to be provided for legal reasons			Art. 45a (1) (p)
	Cases where a person who could factually not provide the fingerprints was refused a visa			Art. 45a (1) (q)
Stay	No. of persons identified as overstayers, their nationalities and BCP of entry	Art. 63 (1) (e)		

	Data entered on revoked/extended stay	Art. 63 (1) (f)		
Travel authorisation (TA) info	Type of TA; for a TA with limited territorial validity, a reference to the MS(s) issuing it		Art. 84 (1) (g)	
	TA's validity period		Art. 84 (1) (h)	
	Grounds for TA refusal/revocation/ annullment		Art. 84 (1) (i)	

Notes: *EES = Entry-Exit system; ETIAS = European Travel Information and Authorisation System; VIS = Visa information system*

MS = Member State

** The table presents the data stored in the Central Repository for Reporting and Statistics by three large scale IT systems in the area of borders and visa (EES, ETIAS and VIS). The SIS proposal on border checks does not define which data will be stored in the Central Repository for Reporting and Statistics (Article 54).*

[a] = ETIAS compromise text, Art. 84, which covers the use of data for reporting in statistics.

[b] = Application status information

Source: FRA, 2018

TK-03-18-243-EN-N

Publications Office

ISBN: 978-92-9474-238-4
doi: 10.2811/560520

FRA – European Union Agency for Fundamental Rights

Schwarzenbergplatz 11 ▪ 1040 Vienna ▪ Austria ▪
Tel +43 158030-0 ▪ Fax +43 158030-699
fra.europa.eu ▪ info@fra.europa.eu ▪ facebook.com/fundamentalrights
▪ linkedin.com/company/eu-fundamental-rights-agency ▪
twitter.com/EURightsAgency