The European Commission package of ETIAS consequential amendments

Substitute impact assessment

STUDY

EPRS | European Parliamentary Research Service

Ex-Ante Impact Assessment Unit
PE 642.808 – December 2019

EN

The European Commission package of ETIAS consequential amendments

Substitute impact assessment

On 7 January 2019, the European Commission presented two proposals for amendments to the legal instruments of the EU information systems following the adoption of Regulation 2018/1240 on the establishment of a European Travel Information and Authorisation System (ETIAS). The ETIAS Regulation requires all visa-exempt non-EU nationals to apply online for travel authorisation prior to the date of their departure. Neither the original Commission proposal for ETIAS, nor the two subsequent proposals ('the Commission package') were accompanied by Commission impact assessments.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) therefore requested a targeted substitute impact assessment of the expected fundamental rights impacts of specific elements of the Commission package.

This assessment concludes, inter alia, that the Commission package expands the scope of the European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN) beyond the purposes stated in the ECRIS-TCN Regulation. This expansion constitutes a serious interference with the rights to respect for private life and to protection of personal data. The necessity of this interference is called into question due to the potential overlap between the Schengen Information System (SIS) and ECRIS-TCN. The assessment moreover finds that the provisions on the automated processing of ETIAS application files also entail interference with the rights to respect for private life and protection of personal data. It also highlights the existence of data quality issues and calls into question the relevance of certain data stored in EU information systems. That said, it finds the provisions on access by the ETIAS Central Unit and the ETIAS National Units relatively well balanced and recommends certain clarifications.

EPRS | European Parliamentary Research Service

AUTHOR

This study has been written by Dr Niovi Vavoula from Queen Mary University of London at the request of the Ex-ante Impact Assessment Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

ADMINISTRATOR RESPONSIBLE

Dr Katharina Eisele, Ex-Ante Impact Assessment Unit, EPRS.

To contact the publisher, please e-mail: EPRS-impactassessment@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in December 2019.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Brussels © European Union, 2019.

PE 642.808
ISBN: 978-92-846-6080-3
DOI: 10.2861/156127
CAT: QA-02-19-968-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

In September 2018, the EU legislator adopted Regulation (EU) 2018/1240 concerning the establishment of a European Travel Information and Authorisation System (ETIAS). The ETIAS Regulation requires all visa-exempt non-EU nationals to apply online for travel authorisation prior to the date of their departure. Article 11 of this Regulation also stipulates that ETIAS applications will be initially processed automatically through comparisons of the ETIAS data with data present in a series of EU and international information systems and databases.

This includes six EU information systems, three of which are currently operational, namely:

1. the Schengen Information System (SIS);
2. the Visa Information System System (VIS); and
3. the Eurodac.

The other three remain on paper (but their respective legal instruments have been adopted), namely:

4. the Entry Exit System (EES);
5. the European Travel Information and Authorisation System (ETIAS); and
6. the European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN).

These information systems have been developed independently, but the Interoperability Regulations 2019/817 and 2019/818 prescribe four interoperability components to enable interaction with one another: a European Search Portal (ESP), a shared Biometric Matching Service (BMS); a Common Identity Repository (CIR) and a Multiple Identity Detector (MID). Interoperability between EES and ETIAS is also envisaged in the EES and ETIAS Regulations.

On 7 January 2019, the European Commission published two proposals to establish interoperability between ETIAS and other EU information systems ('the Commission package'):

> 1. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN]) (COM(2019) 3 final);
>
> 2. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No. 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861 (COM(2019) 4 final).

The need for the Commission package emerged as follows: At the time of the adoption of the ETIAS Regulation, Regulation (EU) 2019/816 on the establishment of ECRIS-TCN had not yet been formally adopted. However, Recital 58 of the ETIAS Regulation states that if a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons is established at EU level, ETIAS should be able to query it. Furthermore, the revised legal framework on SIS had not been formally adopted. Importantly, Article 11(2) of the ETIAS Regulation requires amendments to the legal acts establishing the EU information systems so as to establish interoperability with ETIAS.

The first proposal concerns amendments to the law enforcement branch of SIS (Regulation 2018/1862) and ECRIS-TCN, whereas the second proposal concerns amendments to the immigration branch of SIS, VIS, EES and ETIAS. Amendments to Eurodac are not foreseen as a recast of the Eurodac Regulation is currently negotiated.

The Commission package was not accompanied by an impact assessment, neither was the original Commission proposal for ETIAS.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) is currently considering the proposals (rapporteur Jeroen Lenaers, EPP, the Netherlands). Being of the view that an impact assessment is necessary, on 4 October 2019, the LIBE Committee requested the European Parliamentary Research Service (EPRS) to conduct a targeted substitute impact assessment. This targeted impact assessment examines the following two main research questions:

- Does the Commission package expand the scope of ECRIS-TCN in comparison to the one laid down in the ECRIS-TCN Regulation, and if so, what are the implications of such extension with respect to the protection of fundamental rights, particularly the right to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and to the protection of personal data (Article 8 of the EU Charter)? This question primarily concerns the first Commission proposal.
- What are the privacy and personal data protection implications of the provisions concerning the automated processing of ETIAS applications through comparison of the ETIAS data against data already stored in EU information systems? This question primarily concerns the second Commission proposal.

The targeted substitute impact assessment is based on an external study, which was outsourced by the Ex-Ante Impact Assessment Unit of EPRS. The impact assessment is primarily based on desk research, but the input of stakeholders has also been taken into account through four semi-structured interviews with experts from the European Commission, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Union Agency for Fundamental Rights (FRA) and the European Data Protection Supervisor (EDPS). The study is limited in scope and was conducted within a specific limited time frame. Any information on Member States' practices is based on publicly available sources.

The first research question:

With regards to the first question, the study finds that ECRIS-TCN is deeply rooted in criminal justice cooperation, as evidenced by its link to the European Criminal Record Information System (ECRIS), a de-centralised tool that assists national authorities in identifying which Member State holds information on previous convictions in respect of an individual. The purpose of ECRIS-TCN is to assist in identifying such Member States when the individual in question is a third-country national. **The use of ECRIS-TCN data for examining ETIAS application files is not foreseen in the ECRIS-TCN Regulation**. Furthermore**, though the use of ECRIS-TCN for ETIAS-related purposes is provided for in Recital 58 of the ETIAS Regulation, that expansion has evaded scrutiny at the level of an impact assessment, both when the ETIAS Regulation was adopted, and when ECRIS-TCN was negotiated.**

The impact assessment gap is threefold, at the time: 1) when the ETIAS Regulation was proposed; 2) when the ECRIS-TCN was proposed and negotiated; and 3) when the Commission package was proposed.

Moreover, the study finds that **the expansion of the scope of ECRIS-TCN constitutes a serious interference with the rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter)**. **ECRIS-TCN will be used for purposes in addition to those that were originally foreseen, and** two new types of authorities will have access to ECRIS-TCN data: the ETIAS Central Unit and the ETIAS National Units.

The study notes that both fundamental rights are not absolute and interferences may be justified provided that the requirements of Article 8(2) ECHR and Article 52(1) of the EU Charter are met. Central in that respect is the assessment of whether the interference with the aforementioned rights complies with the principles of necessity and proportionality.

From the perspective of EU secondary law on the protection of personal data, **the expansion of the ECRIS-TCN scope is difficult to reconcile with the purpose-limitation principle, which is a key principle of EU data protection law**. It is testament to the **growing trend to blur the boundaries between immigration law and law enforcement, and the emergence of function creep**, which means that the use of a system or a database is gradually widened beyond the purpose for which it was originally conceived.

In the present case, **instead of expanding the purpose of information systems established for immigration control to assist in law enforcement, a criminal justice cooperation mechanism is proposed to be used for border management purposes.** The principle of purpose limitation is enshrined in Article 5(2)(1) of the GDPR and requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The principle of purpose limitation in the law enforcement context allows for exceptions under Article 4(2) of the Data Protection Directive for Law Enforcement Purposes, when the use for other purposes is necessary and proportionate.

As a result, both from the perspectives of EU primary law (in line with the ECHR) and EU secondary law on protection of personal data, the study must assess whether the exception to the purpose limitation principle is justified and examine whether the expansion of the scope of ECRIS-TCN is necessary and proportionate.

On the one hand, the expansion of the scope of ECRIS-TCN may be seen as consistent with the potential use of ECRIS-TCN data at the national level for purposes related to immigration procedures, if these are provided for under national law. Furthermore, the purpose of ETIAS is to produce a risk assessment of visa-free travellers and all other EU information systems, certain Interpol databases and Europol data shall also be automatically consulted to identify potential hits. Furthermore, the use of ECRIS-TCN data for ETIAS-related purposes is consistent with the approach taken by the United States, where a system similar to ETIAS, the Electronic System for Travel Authorization (ESTA), is operational. In turn, the Australian Electronic Travel Authorisation system (ETA) does not foresee consultation of criminal records.

On the other hand, the study takes note that SIS registers alerts on convicted third-country nationals for the purpose of refusing entry or stay in the Schengen area (Article 24(1)(a) and 24(2)(a) of Regulation 2018/1861). **Alerts in connection to third-country nationals convicted of terrorist offences are mandatorily entered in SIS (Article 21(2) of Regulation 2018/1861). However, alerts related to third-country nationals convicted of other offences are entered following an individual assessment in accordance with the principle of proportionality** (Article 21(2) of Regulation 2018/1861). **Consequently, the study concludes that once ECRIS-TCN becomes operational, there will be complete overlap between SIS and ECRIS-TCN with regards to convictions on terrorist offences**. The overlap between SIS and ECRIS-TCN with regards to other offences listed in the Annex of the ETIAS Regulation is opaque due to the discretion enjoyed by Member States. Further information is required to determine the full extent of that overlap, as publicly available information is inconclusive on national practices.

Be that as it may, **the scope of SIS alerts is wider than the one for ECRIS-TCN**. This is because SIS alerts may be registered in relation to a criminal offence carrying a custodial sentence of more than a year. This threshold is lower than that of the ETIAS Regulation. Furthermore, suspected individuals

may also be registered in SIS. In addition, **there is no publically available information concerning the inadequacy of the SIS alerts in preventing the entry or stay of third-country nationals due to the lack of registering alerts on convicted third-country nationals. Given that their purpose is precisely to prevent the entry of unwelcome third-county nationals, there is no indication that these alerts are not sufficient for the purposes of examining ETIAS applications**. **A hit in ECRIS-TCN without an alert in SIS may even complicate a decision on an ETIAS application**.

The study further considers that **comparing ETIAS applications against records of dual nationals is not necessary** – as dual nationals will benefit from free movement rights – and therefore their records should be excluded from automated processing.

With respect to proportionality considerations, the study concludes that should the co-legislators decide to extend the scope of ECRIS-TCN, the flagging of records concerning offences in the Annex of the ETIAS Regulation is a welcome approach. The flagging of records takes into account that criminal convictions constitute a special category of personal data in accordance with the GDPR. The keeping of logs is also a welcome requirement. The study recommends that any statistical information created by eu-LISA on the basis of logs should be circulated to the EU institutions and the EDPS with a view to evaluating whether the extension of ECRIS-TCN was unnecessary. As for the categories of personal data processed, this study notes that the interoperability between ECRIS-TCN and ETIAS should not lead to requiring Member States to collect and store in ECRIS-TCN information which may only be inserted if it is available to the central authority.

Finally, the study warns that **the expansion of ECRIS-TCN to assist ETIAS-related purposes must not be used as a precedent to make ECRIS-TCN available for future consultation by other EU information systems, thus eliminating the boundaries between immigration law and law enforcement**. It may also legitimise the routine consultation of criminal records in the course of immigration procedures at the national level.

The second research question:

With regards to the second research question, the study finds that automated processing of ETIAS applications through **consultation of EU information systems constitutes an interference with the rights to respect for private life (Article 7 EU Charter and Article 8 ECHR) and to the protection of personal data**. This is because new forms of processing of personal data are foreseen and new authorities will have access to stored data.

The study assessed the necessity and proportionality of this interference in light of case law of the Court of Justice of the EU (CJEU).

In the case of the Commission package**, the study finds that no additional data will be collected by any of the systems and no discrepancies are evident when comparing the tables of correspondences and the proposed Article 11 of the ETIAS Regulation. However, the study stresses that EU information systems suffer from data quality issues** (spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names, etc.). If the stored information is not of sufficient quality, any automated processing may lead to incorrect processing and irregularities, with significant repercussions for third-country nationals. **Besides, the greater the number of information systems consulted and the more data contained therein, the greater the possibility of a false hit.**

Furthermore, the study underlines that depending on national practices, some SIS alerts on 'discreet checks', 'inquiry checks' or 'specific checks' – which will be consulted when ETIAS becomes operational – may not be relevant for ETIAS-related purposes. This is because **SIS has been criticised for storing alerts on discreet checks of doubtful lawfulness, because national**

authorities in certain Member States assess differently each individual case under different proportionality assessments.. **The relevance of VIS data is also uncertain**. VIS stores personal data on visa applicants, whereas ETIAS concerns visa-free travellers. As a result, the automated processing of ETIAS applications against personal data on third-country nationals coming from countries whose nationals do not require a short-stay visa to enter the Schengen area may not generate a hit, due to the different scope between the two EU information systems. VIS will be of interest in relation to dual nationals (with nationalities of both countries whose nationals need a short-stay visa and visa-free countries). It will also be relevant when the revised EU legal framework on VIS will be adopted, which will expand its scope. Under this expanded scope VIS will store records on long-stay visa applicants and holders of residence permits and residence cards.

With respect to access by the ETIAS Central Unit, the study considers that temporary access by the ETIAS Central Unit is proportionate to the purpose of manually processing the hits produced by the ETIAS Central System. The study finds that it may be useful to add that the ETIAS Central Unit's right to search and access the relevant data is on a read-only basis and merely involves the data that generated a hit.

In relation to the addition of ETIAS National Units among the competent national authorities having read-only access to the EU information systems, the study concludes that this is proportionate. The amendments to the SIS Regulations do not make a reference to the fact that access by the ETIAS National Units is on a read-only basis.

The keeping of logs is a welcome development, as it will allow supervision of the data processing activities.

As for comparison of ETIAS application files against the new category of SIS alerts on 'inquiry checks' that was inserted in 2018 after the adoption of the ETIAS Regulation. **The study finds that this amendment is proportionate to the aims pursued by SIS, as long as the registration of these alerts is lawful.** This is because 'inquiry checks' constitute an intermediate step in between 'discreet checks' and 'specific checks'. Under the ETIAS Regulation, both these alerts will be consulted when examining an ETIAS application.

In light of the difficult negotiations between the EU and Interpol so as to enable the consultation of certain Interpol databases for ETIAS-related purposes, the study considers that the requirement to conclude an international cooperation agreement with Interpol is a welcome addition to the ETIAS Regulation. The EU co-legislators may wish to consider the addition of some safeguards in the ETIAS Regulation (keeping of logs, prohibition of onward transfers to other international entities, etc.).

Given the importance of the right to effective remedies, as enshrined in Article 47 of the EU Charter and Article 13 ECHR, for the enjoyment of the rights to private life and protection of personal data the study scrutinises the impact of the Commission package on that right. **The study finds that the right to effective remedies requires informing the ETIAS applicant about the information system which has generated a hit that resulted in the refusal of the travel authorisation. However, this provision of information should be without prejudice to any limitations in the exercise of the right to information as laid down in the legal instruments of the information systems** (e.g. SIS).

Finally, with regards to the automated processing of ETIAS data through direct importing in EES, **the study notes that the Commission package requires the importing of additional categories of personal data which go beyond the categories of personal data to be collected by EES pursuant to the EES Regulation (details on family members and minors). The study finds that the justification for the insertion of these additional categories in EES is not sufficient.**

Table of contents

List of abbreviations

AFSJ	Area of Freedom, Security and Justice
ATS	Automated Targeting System
BMS	Biometric Matching Service
CEAS	Common European Asylum System
EU Charter	Charter of Fundamental Rights of the European Union
CIR	Central Identity Repository
CISA	Convention implementing the Schengen Agreement
CJEU	Court of Justice of the European Union
CMAL	Central Movement Alert List
DPIA	Data Protection Impact Assessment
EBCG	European Border and Coast Guard
ECHR	European Convention on Human Rights
ECRIS	European Criminal Record Information System
ECRIS-TCN	European Criminal Record Information System – Third-Country Nationals
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EMN	European Migration Network
EPPO	European Public Prosecutor's Office
ESP	European Search Portal
ESTA	United States Electronic System for Travel Authorisation
ETA	Australian Electronic Travel Authority
ETIAS	European Travel Information and Authorisation System
EU	European Union
Eurodac	European Dactyloscopy
Europol	European Union Agency for Law Enforcement Cooperation
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation

MID	Multiple Identity Detector
PNR	Passenger Name Record
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Document Database
TDAWN	Interpol Documents Associated with Notices Database
TECS	Treasury Enforcement Communications System
TFEU	Treaty on the Functioning of the European Union
TSDB	Terrorist Screening Database
VIS	Visa Information System

1. Introduction

1.1. Background in a nutshell

In September 2018, the EU legislator adopted Regulation (EU) 2018/1240 concerning the establishment of a European Travel Information and Authorisation System (ETIAS).[1] The ETIAS Regulation requires that all visa-exempt non-EU nationals need to apply online for travel authorisation prior to the date of their departure. Article 11 of this Regulation also stipulates that ETIAS applications will be initially processed automatically through comparisons of the ETIAS data with data present in a series of EU and international information systems and databases.

On 7 January 2019, the European Commission published two proposals to establish interoperability between ETIAS and other EU information systems ('the European Commission package'):

1. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN]) (COM(2019) 3 final);

2. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No. 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861 (COM(2019) 4 final).

The Commission package was not accompanied by an impact assessment, neither was the original Commission proposal for ETIAS.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) is currently considering the proposals (rapporteur Jeroen Lenaers, EPP, the Netherlands). Being of the view that an impact assessment is necessary, on 4 October 2019, the LIBE Committee requested a targeted substitute impact assessment.

1.2. Objective and scope of the study

The objective of this targeted impact assessment is to assess the main expected legal impacts of the most important provisions of the Commission package on ETIAS consequential amendments, with emphasis on fundamental rights protection, particularly on the rights to respect for private life (Article 7 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights) and protection of personal data (Article 8 of the EU Charter).

In particular, the study aims at evaluating whether the Commission package:

- Extends the scope of ECRIS-TCN and if so, what are the consequences of such expansion particularly with regards to access rights; and
- Poses privacy and data protection challenges with regards to the automated processing of ETIAS application files by comparing them against personal data stored in EU information systems.

[1] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (ETIAS Regulation) [2018] OJ L236/1.

The basis for comparison (status quo) is the current regulatory framework. The targeted nature of the study translates into a focus on the main changes that the Commission package introduces with respect to the Regulations currently in force.

1.3. Overview of the legal context

1.3.1. The ETIAS Regulation

On 12 September 2018, the European Parliament and the Council of the European Union adopted two Regulations concerning the setting up of an EU-wide information system, namely the European Travel Information and Authorisation System (ETIAS):

1. Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS Regulation);
2. Regulation (EU) 2018/1241 amending the Europol Regulation for the purpose of establishing this new system.[2]

ETIAS will allegedly fill in the 'information gap'[3] created by the lack of available personal data on third-country nationals who are exempt from the requirement to be in possession of a Schengen visa when crossing the external borders of the EU.[4] The ETIAS Regulation applies to this particular group of third-country nationals[5] with the purpose of identifying whether their presence in the territory of the Member States would pose a security, irregular migration or high epidemic risk.[6] In order to assess these risks, the ETIAS Regulation prescribes that all visa-exempt third-country nationals will be required to apply online for travel authorisation prior to the date of their departure. In processing each application, According to Article 20 of the ETIAS Regulation, ETIAS will automatically compare the personal data submitted by the applicants with the data already stored in records, files or alerts registered in EU information systems.[7]

- the Schengen Information System (SIS) (operational);
- the Visa Information System (VIS) (operational);
- the Eurodac (operational);
- the Entry/Exit System (EES) (under development) and;

---

2 Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) [2018] OJ L236/72.

3 European Commission, 'Feasibility Study for a European Travel Information and Authorisation System (ETIAS)' (16.11.2016) 9.

4 For an analysis of the fundamental rights implications of ETIAS see Julien Jeandesboz, Susie Alegre and Niovi Vavoula, 'European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection' (European Parliament Study for the LIBE Committee, PE 583.148, 2017).

5 On the scope *ratione personae* of ETIAS see Article 2 of the ETIAS Regulation.

6 Article 1 of the ETIAS Regulation.

7 For reasons of simplicity and coherence, reference is made to EU information systems though Member States may not have access to some of these systems (e.g. non Schengen States), whereas non-EU Member States that are Schengen Associated States have access. In 2018, 26 EU Member States and 4 Associated Countries (Iceland, Liechtenstein, Norway and Switzerland) had access to SIS. The authorities of Cyprus and Ireland are preparing their technical connection to SIS. Eurodac is used in 32 countries: 28 EU Member States and 4 Associated Countries (Iceland, Liechtenstein, Norway and Switzerland). VIS is used by all Schengen States, including Denmark that has decided to implement it.

- ETIAS itself (under development).[8]

The personal data in ETIAS applications shall also be automatically compared against Europol data,[9] certain Interpol databases, namely the Stolen and Lost Travel Document database (SLTD) and the Interpol Documents Associated with Notices databases (TDAWN),[10] and cross-checked against a dedicated ETIAS watchlist[11] and ETIAS screening rules.[12] Automatic processing aims to identify whether the applicant's personal data are listed in any of the aforementioned information systems or databases for a reason that merits further attention and may justify the refusal of the travel authorisation (e.g. whether the applicant has been refused a short-stay visa, or is reported to SIS as subject to refusal of entry or stay). If automated processing reveals a hit, then Articles 21 and 22 of the ETIAS Regulation provide that a dedicated ETIAS Central Unit, established within the European Border and Coast Guard (EBCG), shall be consulted to verify the hit. If the hit is verified then the application will be processed manually by an ETIAS National Unit.[13] If the hit proves to be a false one, then the applicant shall be issued with a travel authorisation.[14]

As mentioned above, ETIAS is not operational yet. Eu-LISA, the EU Agency responsible for the management of large-scale IT systems in the area of freedom, security and justice (AFSJ), is responsible for its development with aim that the system will be operational by 2020. According to Article 11 of the ETIAS Regulation, in order for automated processing to take place, interoperability of ETIAS with other EU information systems must be established.

1.3.2. The legal landscape of EU information systems in the area of freedom, security and justice (AFSJ)

Given that the rules on automated processing require consultation of the other EU information systems, as outlined above, ETIAS must be viewed in the broader context of an elaborate network of EU information systems, some of which are currently operational (SIS, VIS, Eurodac), whereas others are still in the development stage (EES, ECRIS-TCN).[15]

Schengen Information System (SIS)

Operational since 1995, the overarching purpose of SIS is to ensure a high level of security in the Schengen area by facilitating both border control and police investigations.[16] To these ends, SIS

8 Article 20 of the ETIAS Regulation.

9 Article 20(2)(j) of the ETIAS Regulation.

10 Article 20(2)(b) and (l) of the ETIAS Regulation.

11 Article 34 of the ETIAS Regulation. The watchlist will consist of data on persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offences, or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment, to believe that they will commit a terrorist offence or other serious criminal offences.

12 Article 33 of the ETIAS Regulation. The screening rules shall be an algorithm enabling profiling through the comparison of the data recorded in the ETIAS application file with specific risk indicators. The European Commission will adopt a delegated act to further define the risks related to security or illegal immigration or a high epidemic risk.

13 Article 26 of the ETIAS Regulation.

14 Article 22(4) of the ETIAS Regulation. A false hit would be where the data do not correspond.

15 For an overview see Niovi Vavoula, 'The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Data Protection', *European Law Review* (forthcoming 2020) https://www.academia.edu/40601618/The_Puzzle_of_EU_Large-Scale_Information_Systems accessed 18 November 2019.

16 At its early days, the specific objective of SIS was twofold; a) to maintain public order and security, including State security and b) to enable the Contracting parties to automatically search the information on persons and objects

registers alerts on various categories of persons and objects. In connection with each alert, the SIS initially stored basic alphanumeric information – such as name, nationality, the type of alert and any specific objective physical characteristics.[17] However, the pressing need to develop a second generation SIS (SIS II) so as to accommodate the expanded EU family after the 2004 enlargement was seen as an opportunity to insert new functionalities into the system.[18] One major shift has been the possibility of interlinking alerts involving different individuals or events that are inserted under different legal bases.[19] Another change involved the possibility of including biometric identifiers (photographs and fingerprints) within the system.[20] In 2018, the SIS legal framework underwent another revision primarily with a view to adding certain categories of alerts.[21] According to the current rules, SIS stores alerts on persons wanted for arrest and extradition,[22] missing persons, or vulnerable persons who need to be prevented from travelling,[23] persons sought to assist with a judicial procedure,[24] persons or objects subject to discreet, inquiry or specific checks,[25] objects sought for the purpose of seizure or their use as evidence in criminal proceedings,[26] and unknown wanted persons.[27] In addition, the SIS stores alerts on third-country nationals subject to return procedures, which is also a new category of alerts,[28] or to be refused entry or stay in the Schengen area. In practice, alerts on third-country nationals dominate the system.[29] The variety of possible

registered therein for the purposes of border control and police investigations, control and other searches. See Article 93 of the 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 [2000] OJ L239/19 (CISA).

17 Article 94 of CISA.

18 Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63.

19 Article 37 of Regulation 1986/2006 and Article 52 of Decision 2007/533/JHA.

20 Article 22 of Regulation 1986/2006 and Article 22 of Decision 2007/533/JHA.

21 Regulation 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1; Regulation 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14; Regulation 2018/1862 of the European Parliament and of the Council of 28 November 2018 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 and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56.

22 Articles 26-31 of Regulation 2018/1862.

23 Articles 32-33 of Regulation 2018/1862.

24 Articles 34-35 of Regulation 2018/1862.

25 Articles 36-37 of Regulation 2018/1862. Inquiry checks' is a new category of alerts.

26 Articles 38-39 of Regulation 2018/1862.

27 Articles 40-41 of Regulation 2018/1862. This is also a new category of alerts.

28 Article 3 of Regulation 2018/1860.

29 Article 24 of Regulation 2018/1861. For a detailed overview of SIS see Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008). For a more recent analysis see Evelien Brouwer, 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders - Citizens, Migrants, Humans: Liber Amicorum in honour of prof.dr. Elspeth Guild* (Wolf Legal Publishers 2019).

alerts reflect the system's overall purpose, which the European Commission has acknowledged that it is not unitary.[30]

Visa Information System (VIS)

A post 9/11 initiative, VIS is an information system that stores a wide range of personal data (both biographical and biometric) on individuals applying for short-stay (Schengen) visas. The VIS was set up by a series of instruments: Decision 2004/512/EC,[31] Regulation 767/2008[32] governing the use of the system for border control purposes, and Council Decision 2008/633/JHA[33] prescribing the modalities by which visa data are consulted by law enforcement authorities and Europol. The VIS is also a multi-purpose tool aimed at improving the implementation of the common visa policy, but seven sub-purposes are envisaged, including the fight against fraud and visa shopping and the contribution to the prevention of threats to Member States' internal security.[34] At the timing of writing, VIS is under revision; the VIS proposal[35] extends the system to long-term visa holders as well as holders of residence permits and residence cards, and it also lowers the threshold age for fingerprinting (six years).

Eurodac

Eurodac processes the fingerprints of asylum seekers and certain categories of irregular migrants (irregular migrants apprehended in connection with the irregular crossing of an external border or found illegally staying in a Member State)[36] with the purpose of assisting in the implementation of the Dublin rules on the allocation of the Member State responsible to examine an application for international protection.[37] Eurodac may also be accessed by national law enforcement authorities and Europol for the purposes of preventing, detecting and investigating terrorist offences and

---

30 European Commission, 'Overview of information management in the area of freedom, security and justice' (Communication) COM(2010) 385final, 22.

31 Council Decision 2004/512/EC establishing the Visa Information System (VIS) [2004] OJ L213/5.

32 Regulation (EC) 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas [2008] OJ L218/60, as amended by Regulation (EC) 810/2009 [2009] OJ L243/1 (VIS Regulation).

33 Council 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 [2008] OJ L218/129.

34 For a critical examination of the VIS purposes, see Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Databases* (Brill Nijhoff forthcoming 2020) Chapter 3. The ranking of the purposes has been litigated before the CJEU. See C-482/08 *UK v Council* ECLI:EU:C:2010:631.

35 European Commission, COM(2018) 302final.

36 Regulation 603/2013 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [2013] OJ L180/1.

37 Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013] OJ L180/31 (Dublin III Regulation).

serious crimes.[38] A recast proposal[39] tabled since May 2016 is currently negotiated as part of the revised Common European Asylum System (CEAS), with the aim of expanding the purpose, scope and categories of personal data stored in the system.[40]

Entry/Exit System (EES)

Adopted in 2017, Regulation 2017/2226 provides for the establishment of EES that will register the border crossings, both at entry and exit, of all third-country nationals admitted for a short stay, irrespective of whether they are required to obtain a Schengen visa or not.[41] EES is a multi-purpose tool: it aims to enhance the efficiency and automation of border checks, assist in the identification of irregular migrants and overstayers, combat identity fraud and misuse of travel documents and strengthen internal security and the fight against terrorism by allowing law enforcement authorities access to travel history records.[42]

European Criminal Record Information System – Third-Country Nationals (ECRIS-TCN)

The latest addition to the EU information system family is the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).[43] The latter emerged as a necessity in the law enforcement context, because in order to obtain complete information on previous convictions of third-country nationals, the requesting Member States were obliged to send 'blanket requests' to all Member States, thus creating a heavy administrative burden.[44] The ECRIS-TCN will be a centralised system for the exchange of criminal records on convicted third-country nationals and stateless persons. The ECRIS-TCN is meant to complement the already existing, decentralised ECRIS system through which information on the criminal records of EU nationals is exchanged among Member States.[45]

---

38 Articles 19-22 of Regulation 603/2013. For a critical analysis see Niovi Vavoula, 'The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015).

39 European Commission, COM(2016) 272final. Agreement has been reached, but due to complications in relation to other asylum-related files, formal adoption is still pending.

40 Given that the Commission package does not lay down amendments to the Eurodac Regulation, the implications of expanding Eurodac to assist ETIAS are not be assessed in depth. It suffices here to mention the following: the wording of the purposes of Eurodac (e.g. if Eurodac is transformed from an asylum database to an immigration control) will be crucial; as the EU Fundamental Rights Agency (FRA) has noted, Eurodac is not database that is accessed at the external borders. Therefore, the necessity of such expansion may be questioned. See FRA, 'The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS) – Opinion of the European Union Agency for Fundamental Rights' (2017) 22-24. Also it may be questioned whether there will be any hit against Eurodac and whether the hits will involve persons who may already be subject to an alert in SIS as irregular migrants. If the irregular migrant is already reported in SIS, then cross-checking against Eurodac is not necessary. There is no information to question the sufficiency of SIS alerts for examining ETIAS application files.

41 Subject to certain exceptions. See Article 2(3) of the EES Regulation.

42 Article 6(1) of the EES Regulation. For a critical analysis, see Mark Cole and Teresa Quintel, 'Data Retention under the Proposal for an EU Entry/Exit System (EES) Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union' (Legal Opinion for the Greens, 2017).

43 Regulation (EU) 2019/816 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135/1 (ECRIS-TCN Regulation); Directive 2019/884 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA [2019] OJ L151/143.

44 Recital 6 of the ECRIS-TCN Regulation.

45 Recital 7 of the ECRIS-TCN Regulation. The existing ECRIS framework will be used to request the criminal records information from the convicting Member State(s) in accordance with Council Framework Decision 2009/315/JHA of

Interoperability of EU information systems

SIS, VIS and Eurodac were originally envisaged to operate independently, without the possibility of interacting with one another. Progressively, the need has emerged to provide technical and legal solutions that would enable EU information systems to complement each other. To that end, the Interoperability Regulations 2019/817 and 2019/818 adopted on 20 May 2019 prescribe four main components to be implemented: a European Search Portal (ESP), a shared Biometric Matching Service (BMS), a Common Identity Repository (CIR) and a Multiple Identity Detector (MID).[46]

The ESP will enable competent authorities to simultaneously query the underlying systems and the combined results will be displayed on a single screen. Even though the screen will indicate in which EU information systems the information is held, access rights should remain unaltered.

The BMS will generate and store templates from all biometric data recorded in the underlying systems, thus effectively becoming a new information system that compiles biometrics from the SIS II, VIS, Eurodac, EES and ECRIS-TCN.

The CIR will store an individual file for each person registered in the systems, containing both biometric and biographical data, as well as a reference indicating the system from which the data were retrieved. CIR's main objectives are to facilitate identity checks of third-country nationals,[47] assist in the detection of individuals with multiple identities and streamline law enforcement access. With respect to law enforcement, a new two-step process is foreseen: law enforcement authorities will first consult the underlying EU information systems (VIS, Eurodac, EES, ETIAS, ECRIS-TCN) to check whether records on an individual exist in any of the databases without obtaining prior authorisation by a verifying authority. In the event of a hit, the second step is to obtain access to each individual system that contains the matching data through the procedure prescribed in the legal basis of each database.

The MID will use the alphanumeric data stored in the CIR and the SIS II to detect multiple identities; it will create links between identical data to indicate whether the individual is lawfully registered in more than one system or whether identity fraud is suspected. The purpose of these components is

26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States [2009] OJ L93/23.

[46] Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L135/27; Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L135/85 (Interoperability Regulations). For an analysis see Teresa Quintel, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (University of Luxembourg Law Working Paper No. 002-2018) https://orbilu.uni.lu/bitstream/10993/35318/1/Teresa%20Quintel%20Interoperability%20of%20EU%20Databases.pdf accessed 18 November 2019; Niovi Vavoula, 'Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?' (*EU Immigration and Asylum Law and Policy*, 08.07.2019) https://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/ accessed 18 November 2019.

[47] Article 20 of the Interoperability Regulations. For an analysis see Teresa Quintel, 'Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals' (2018) 4 *European Data Protection Law Review* 470.

to allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat irregular migration.[48]

Finally, interoperability between EES and VIS – as both systems will record data on visa applicants – is already envisaged in the EES and ETIAS Regulations.[49]

1.4. The Commission package

In light of the above, and in order to implement the provisions of the ETIAS Regulation regarding automated processing of ETIAS applications, on 7 January 2019, the European Commission adopted a package of two proposals to establish interoperability between ETIAS and other information systems:

> 1. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN]);[50]
>
> 2. Proposal for a Regulation of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No. 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861.[51]

The proposals follow on from Article 11(2) of the ETIAS Regulation, which prescribes that:

> 'amendments to the legal acts establishing the EU information systems that are necessary for establishing their interoperability with ETIAS as well as the addition of corresponding provisions shall be subject of a separate legal instrument.'

Similarly, reference should also be made to Article 88 of the ETIAS Regulation on the start of operations of ETIAS. Article 88(1)(a) requires that the legal acts of the EU information systems are amended in order to ensure interoperability with ETIAS. Without amendments to the legal instruments of EU information systems, automated processing of ETIAS applications (thus the full establishment of the database) will not be possible and ETIAS cannot start its operations.

Furthermore, it must be recalled that when the ETIAS Regulation was adopted in September 2018, the SIS legal framework was under revision, with the final text being adopted by the European Parliament and the Council in November 2018. Therefore, the SIS legal framework is not adapted to the new ETIAS rules. ECRIS-TCN was negotiated and the corresponding legal instruments were adopted in June 2019. In addition, as mentioned earlier, at the time of writing the recast of the Eurodac Regulation has not yet been adopted, whereas a recast of the VIS Regulation is also under negotiations.

As a result, the Commission package includes amendments to the currently applicable VIS Regulation (Regulation 2008/767), but makes no amendments in relation to Eurodac and these shall be included in a separate legislative proposal.

---

48 Article 2(1) of the Interoperability Regulations.

49 Article 8 of the EES Regulation and Article 11 of the ETIAS Regulation.

50 European Commission, COM(2019) 3final.

51 European Commission, COM(2019) 4final.

1.4.1. Consolidation of the ETIAS consequential amendments

Since not all EU information systems are accessed by the same EU Member States,[52] the first proposal in the Commission package concerns amendments to the law enforcement branch of SIS (Regulation 2018/1862) and ECRIS-TCN, whereas the second proposal concerns amendments to the immigration branch of SIS, VIS, EES and ETIAS. A consolidation and categorisation of the proposed amendments is as follows:

- **Addition of ECRIS-TCN among the EU information systems, which are consulted for the automated processing of ETIAS applications:** The purpose of ECRIS-TCN will be expanded to include border management and contributing to facilitating and assisting in the correct identification of persons. As a result, conviction information in relation to terrorist offences and other serious crimes will be consulted when processing ETIAS applications and such information shall only be used for verifying the identity of the third-country national concerned, and may be used for making specific requests (Annex II and Amendments 1, 7, 11 and 13 of Annex III).

- **Interoperability of SIS, ECRIS-TCN, VIS, EES with ETIAS to enable automated processing:** For the purpose of ensuring the automated processing of ETIAS applications, a tool interconnecting ETIAS with the rest of the EU information systems is envisaged. Furthermore, the Commission package lays down which specific categories of personal data will be compared during the automated process (Amendment 3 of Annex I, Amendment 4 of Annex III, Amendment 2 of Annex IV, Amendment 2 of Annex V, Amendment 3 of Annex VI);

- **Table of correspondences between ETIAS data and data stored in other EU information systems**: Due to discrepancies in the categories of personal data processed in each information system, the tables lay down the categories of personal data in the ETIAS applications which shall be processed and how these correspond to categories of personal data stored in each EU information system. As it is explained in Section 3.2.3. this is a positive development (Amendment 11 of Annex II, Amendment 4 of Annex IV, Amendment 8 of Table V).

- **Addition of the ETIAS Central Unit among the authorities that shall have access to SIS, VIS, ECRIS-TCN and EES for the purpose of performing its tasks pursuant to the ETIAS Regulation**: The ETIAS Central Unit, established within the European Border and Coast Guard (EBCG), is granted access to the EU information systems for the purpose of verifying the hits (Amendment 3 of Annex I, Amendment 2 of Annex IV, Amendment 5 of Annex V, Amendment 3 of Annex VI).

- **Addition of ETIAS National Units among the competent authorities that shall have access to SIS, VIS and EES in order to manually process ETIAS applications following a hit:** Pursuant to Article 26 of the ETIAS Regulation, ETIAS National Units shall have access to the application file and any linked application files, as well as any hits triggered during the automated process (Amendment 2 of Annex I, Amendment 10 of Annex III, Amendments 1 and 2 of Annex IV, Amendments 3 and 5b of Annex V, Amendment 2 of Annex VI).

[52] See n 7.

- **Keeping of logs for the purpose of interoperability with ETIAS:** Logs shall be kept in relation to each data processing operation carried out within SIS, VIS, EES and ETIAS[53] (Amendment 1 of Annex 1, Amendment 10 of Annex II, Amendments 8 and 9 of Annex III, Amendment 3 of Annex IV, Amendment 7 of Annex V, Amendment 1 of Annex VI).
- **Requirement for an agreement between the EU and Interpol that regulates querying the Interpol databases** (Amendment 6 of Annex III).
- **Amendments in the categories of SIS alerts consulted during the automated processing**: Inclusion of the new category of SIS alert 'inquiry checks' among the alerts which will be cross-checked (Amendment 9 of Annex III).
- **Revocation of a travel authorisation due to a SIS alert:** It will not be necessary for SIS to hold a new alert in respect of a third-country national to revoke the travel authorisation issued to him/her. This means that a revocation may be based on the fact that a third-country national was issued with an alert for the first time after the issuance of an ETIAS authorisation. (Amendment 12 of Annex III).
- **Interoperability of ETIAS and EES:** According to the European Commission Communication on 'Smarter Information Systems for borders and security', ETIAS will be built based on a re-use of hardware and software components developed for the EES.[54] The technical development of the CIR and the ESP will be based on EES/ETIAS components. Consequently, a series of amendments involve the relationship of ETIAS and EES for the purpose of interoperability. As mentioned above, relevant rules on the interoperability between EES and ETIAS are already present in the EES and ETIAS Regulations. This has resulted in:
  - **Amendments with regards to the technical architecture of ETIAS:** ETIAS and EES shall be built as a shared identity repository which shall form the basis for the CIR (Amendment 3 of Annex III);
  - The support of the objectives of ETIAS is added among the objectives of EES (Amendment 1 of Annex V);
  - The support of the objectives of EES is added among the objectives of EES (Amendments 2 and 5 of Annex III);
  - **Automated processing of data between EES and ETIAS:** Importation of data from ETIAS into the EES entry/exit or refusal of entry records (Amendment 5 of Annex III, Amendments 2 and 4 of Annex V); and
  - **Keeping of EES data in ETIAS application files:** Such keeping must be done only where necessary in an individual case (Amendment 6 of Annex V).

[53] A log is an electronic record of data processing operation, e.g. that a file has been accessed by a national authority on a particular date and time.

[54] European Commission, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205final.

The Commission did not conduct an impact assessment of the proposed ETIAS consequential amendments, since it regards the amendments as technical adjustments that implement Article 11 of the ETIAS Regulation without going further than the provisions of the ETIAS Regulation.[55] The Commission notes that separate stakeholder consultations have not taken place.[56]

However, the European Parliament's LIBE Committee considers that a targeted impact assessment is necessary to assess the legal impact of the most important provisions of the Commission package, with a focus on their implications for the fundamental rights to private life and protection of personal data.[57]

1.5. Methodological approach

In light of the targeted scope and the limited time frame given by the LIBE Committee to prepare the present study, the methodology used is based upon desk research and four semi-structured interviews. It must be further stressed that the study takes the existing legal framework as a baseline and is based on available public data that may be obtained through research. The operation of EU information systems may reveal sensitive information about Member States' practices. Therefore, though such information may be available to the EU institutions and agencies, it is not publicly accessible.

The inherently technical nature of the subject means that the first step is to discern the legal implications of the Commission package, if any. In that respect, dedicated tables, whereby the current legal framework has been placed next to the proposed amendments, are included so as to clarify how each legal instrument will be modified. This is because the Commission package only includes the proposed amendments, or newly inserted provisions, without reference to the current legal framework.

These tables are included in the present study in Annexes I-VI, with each Annex concerning a specific information system/branch of an information system. Given that a series of amendments are common to all EU information systems, a codification of the amendments is also provided.[58]

In examining the impact of the amendments, relevant sources were taken into consideration, including:

- EU primary and secondary law on information systems and fundamental rights;
- Case law of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR) – So far, however, EU information systems have not generated any case law. Inspiration is drawn from judgments concerning the interpretation of legal instruments in the light of the rights to private life and protection of personal data. In that respect, it must be noted that although the author takes the approach of the CJEU with regard to the relationship between the two rights into consideration,[59] the relevance of key data protection principles has also been taken into account;

---

55 Explanatory Memorandum attached to the Commission package foe ETIAS consequential amendments (n 51-52) 6.

56 Ibid.

57 This view was also shared by the European Data Protection Supervisor (EDPS). See EDPS, 'Formal comments of the EDPS on two proposals to establish the conditions for accessing other EU information systems for ETIAS purposes' (13.03.2019) 4-5.

58 See above, Section 1.3.1.

59 See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238, paras 24-30; Case C-362/14

- European Commission feasibility study for ETIAS and policy study for an EU ESTA;
- European Commission impact assessments for EES, ECRIS-TCN and Interoperability Regulations;
- Studies commissioned by the European Parliament, particularly in relation to the ETIAS and Interoperability Regulations;
- Reports by the EU Agency on Fundamental Rights (FRA);
- Opinions by the European Data Protection Supervisor (EDPS);
- Council of the EU position, as found in Council document 11300/19 (16.07.2019);
- Relevant studies and reports in relation to SIS, VIS, EES and ETIAS; and
- Relevant academic research.

The full references of the above sources can be found in the last section.

The study is informed by the input of some stakeholders from the EU institutions and agencies. Semi-structured interviews were organised with: one expert from the European Commission; two experts from eu-LISA; two experts from the EDPS; one expert from FRA. The limited time frame, in which the study had to be conducted, did not allow for more extensive stakeholder consultations. The main findings of the impact assessment were discussed with the stakeholders with the aim of gaining their insight. Where necessary, their input is explicitly indicated.

The two research questions (as outlined in Section 1.1 above) are approached as follows in this study: the first question is specifically concerned with the addition of ECRIS-TCN among the EU information systems, the data of which will be compared against those in ETIAS applications. The author will explain the rationale and origins of ECRIS-TCN and then underline how the Commission package will alter the purpose and functions of ECRIS-TCN. Identifying this extension in the scope as a serious interference with the rights to private life and personal data protection, as well as a violation of the purpose limitation principle, the author will then assess whether the reform complies with the principles of necessity and proportionality.

The second question concerning the automated processing of ETIAS applications involves the assessment of a series of inter-related consequential amendments, each of which will be examined from a privacy and personal data protection perspective, emphasising on their necessity and proportionality. The existence of data quality issues as well as the relevance of data stored in EU information systems and the rules on manual processing by the ETIAS Central and National Units will be scrutinised.

Issues related to the right to effective remedies (as enshrined in Article 47 of the EU Charter) are also examined, as they are a necessary precondition of the effective protection of the rights to privacy and data protection. Amendments related to specific databases (e.g. interoperability between ETIAS and EES) are also evaluated in terms of their compliance with the principles of necessity and proportionality.

Maximilian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, para 39; Joined Cases C-203/15 and C-698/15 T*ele2 Sverige AB v Post-och Telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970, paras 93-94; Opinion 1/15, ECLI:EU:C:2017:592, paras 121-26; Case C-207/16 *Ministerio Fiscal,* ECLI:EU:C:2018:788, para 51.

2. The use of ECRIS-TCN for ETIAS-related purposes

One of the key amendments of the Commission package involves the addition of ECRIS-TCN among the list of EU information systems which shall be consulted in the course of automated processing of ETIAS application files.

As a result, a series of provisions in the ECRIS-TCN Regulation have been amended in relation to the purpose of, and access to, ECRIS-TCN so as to reflect that ECRIS-TCN shall support ETIAS-related purposes. This section examines the substance and legal implications of these amendments with a view to answering the first research question posed. In particular, this section assesses whether the amendments in the Commission package concerning the use of ECRIS-TCN data for ETIAS-related purposes go beyond the scope of the ECRIS-TCN Regulation. Furthermore, this section examines whether such extension constitutes a proportionate interference with the fundamental rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter).

2.1. The ECRIS-TCN Regulation

2.1.1. The criminal justice origins of ECRIS-TCN

The need to establish ECRIS-TCN emerged in the aftermath of the terrorist attacks in Paris and Brussels in 2015, when calls for boosting exchange of information extracted from criminal records of convicted persons proliferated. The Commission had already stressed in April 2015, in its European Agenda on Security, that the de-centralised European Criminal Record Information System (ECRIS)[60] that was operational since 2012 'does not work effectively for non-EU nationals convicted in the EU'.[61] This was because although the ECRIS legal framework allowed for the exchange of information on convictions concerning third-country nationals, there was no mechanism or procedure in place to do so efficiently, due to the emphasis placed on the EU nationality of the convicted person.

As third-country nationals do not have the nationality of an EU Member State, the national authorities are obliged to send 'blanket requests' in order to obtain information, a procedure that is costly and lengthy.[62] The original Commission proposal provided for a decentralised ECRIS-TCN,[63] whereby an index-filter of identification data on convicted third-country nationals would be created and transmitted to the other Member States in an anonymised way.

However, it soon became clear that a de-centralised structure would be administratively burdensome.[64] Therefore, in June 2017, the Commission published a proposal to establish a centralised information system that would store records of convicted third-country nationals, with

60 See n 43.

61 European Commission, 'The European Agenda on Security' (Communication), COM(2015) 185final, 7-8.

62 European Commission, COM(2017) 344final, 2.

63 European Commission, COM(2016) 7final. Two reports have also been released in that respect. See UNiSYS, 'Feasibility Study: Establishing a European Index of Convicted Third Country Nationals' (11.06.2010). Also see ICT, 'ICT Final Report - Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN)' (4.12.2015).

64 Council, Document 9376/16 (30.05.2016).

the aim of identifying the Member State that holds conviction information on third-country nationals and stateless persons.[65]

After lengthy negotiations,[66] ECRIS-TCN became the sixth centralised information system and was formally adopted in June 2019.[67] Its legal basis is Article 82(1)(d) TFEU that involves measures to 'facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions'. As evidenced by the link between ECRIS-TCN and ECRIS, as stressed above, and the legal basis of the ECRIS-TCN Regulation, the system is deeply rooted in criminal justice cooperation.

2.1.2. The purpose and functions of ECRIS-TCN

Pursuant to Articles 1 and 7 of the ECRIS-TCN Regulation, the purpose of the system is to identify the Member State(s) holding criminal record information on a third-country national in order to obtain information on previous convictions through the de-centralised ECRIS.

ECRIS-TCN may be used when criminal record information on that person is requested in the Member State concerned for the purposes of criminal proceedings against that person, or for any of the following objectives, provided that processing of criminal record data is enshrined under national law and subject to domestic rules.[68] These purposes are: checking a person's own record at his or her request; security clearance; obtaining a licence or permit; employment vetting; vetting for voluntary activities involving direct and regular contact with children or vulnerable persons; visa, acquisition of citizenship and migration procedures, including asylum procedures; and checks in relation to public contracts and public examinations.[69]

However, a Member State may decide to use ECRIS-TCN for purposes other than those set out above if prescribed under, and in accordance with, national law. In that regard, a notification to the European Commission by the start of operations (or soon afterwards) is required, which will be published in the Official Journal of the EU.[70] Consequently, the purposes for which ECRIS-TCN data may be processed are primarily determined under national law and may pertain to different types of procedures and contexts.

According to Recital 35 of the ECRIS-TCN Regulation, depending on the type and context of processing activity, different data protection rules will apply: if the processing involves the purposes of the prevention, investigation, detection or prosecution of criminal offices or the execution of criminal penalties, Directive (EU) 2016/680 (Data Protection Directive for Law Enforcement Purposes)[71] applies, whereas in other cases Regulation 2016/679, the General Data Protection

---

65 European Commission (n 62).

66 The difficulties in the negotiations stemmed from the fact that within the European Parliament some groups took note of the risk that ECRIS-TCN could be used for other objectives than those mentioned in the Commission proposal. The inclusion of dual nationals in the personal scope of ECRIS-TCN was also criticised. For concerns on dual nationals' data see below Section 2.3.4.

67 See n 43.

68 Article 7(1) of the ECRIS-TCN Regulation.

69 Ibid.

70 Article 7(2) of the ECRIS-TCN Regulation.

71 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Data Protection Directive for Law Enforcement Purposes).

Regulation (GDPR), is applicable.[72] In addition, EU agencies, namely Eurojust, Europol and the European Public Prosecutor's Office (EPPO), are entitled to query ECRIS-TCN to identify the Member States holding criminal records information on a third-country national, in accordance with Articles 14-18 of the Regulation. Consequently, the current ECRIS-TCN Regulation does not provide for use of the system for purposes other than those which exist under national law, or for specific law enforcement purposes by EU agencies.

2.1.3. ECRIS-TCN in other EU instruments

Interoperability Regulations

ECRIS-TCN constitutes one of the EU information systems which will form part of the interoperable information exchange environment. All four interoperability components mentioned earlier shall process personal data collected in the context of ECRIS-TCN. In particular:

> a) through the ESP, national authorities shall be able to query simultaneously ECRIS-TCN alongside the other EU information systems (SIS, VIS, Eurodac, EES and ETIAS) and Europol data, subject to existing access entitlements;[73]
>
> b) biometric templates of the ECRIS-TCN biometric data shall be stored in the BMS so as to enable querying with biometric data across several EU information systems;[74]
>
> c) individual files for persons in ECRIS-TCN shall be created and stored in the CIR for the purpose of facilitating and assisting in the correct identification of persons. Such identification is stipulated in Article 20 of the Interoperability Regulations.[75] Other purposes include the functioning of the MID and the streamlining of the access conditions by law enforcement authorities;[76] and
>
> d) Identity confirmation files containing links between different records, files or alerts, including data from ECRIS-TCN, shall be created and stored in MID.[77]

ETIAS Regulation

In addition to the synergies between ECRIS-TCN and other information systems in the interoperability framework, Recital 58 of the ETIAS Regulation stipulates that:

> 'If a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons is established at Union level, ETIAS should be able to query it'.

Therefore, **the ETIAS Regulation already provides for the possibility of accessing ECRIS-TCN during the automated processing of ETIAS application files**, without stipulating further specifications or rules in that respect. Three remarks must be made in that respect.

---

72 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 [2016] OJ L119/1 (General Data Protection Regulation).

73 Articles 6-11 of the Interoperability Regulations.

74 Articles 12-16 of the Interoperability Regulations.

75 See above Section 1.2.2.

76 Articles 17-24 of the Interoperability Regulations.

77 Articles 25-36 of the Interoperability Regulations.

Firstly, at the time when the Commission proposal for establishing ETIAS was released, a centralised ECRIS-TCN had not been conceptualised yet; however, **the ETIAS proposal envisaged consultation of ECRIS data during the processing of ETIAS applications and interoperability of ETIAS with ECRIS**.[78]

Be that as it may, the ETIAS proposal was not accompanied by an impact assessment,[79] but merely by a 2016 Feasibility Study. In that Study it was pointed out that ECRIS only contained convictions of EU citizens and therefore was not relevant for ETIAS. However, in the future 'ECRIS could also contain convictions (in the EU Member States) of third-country nationals, thus becoming a source of valuable information for ETIAS'.[80] It was also stressed that the assessment of ECRIS was based on the current situation and that 'it should be revised should the system evolve and contain convictions of third-country nationals'.[81] A pre-existing 2011 Policy Study on an EU electronic system for travel authorisation (EU ESTA)[82] considered that at that time the conditions were not met for justifying such a system, because VIS had just started its roll out worldwide, Eurodac had – and still has – no capacity of automatically comparing biographical data, and EES was not yet proposed and adopted. The de-centralised ECRIS was not considered as well, because though it had been formally adopted, it was not operational yet.

Secondly, although the ETIAS proposal referred to ECRIS as one of the systems to be queried when processing ETIAS applications, the 2016 impact assessment accompanying the Commission proposal for a de-centralised ECRIS with regards to the exchange of information on third-country nationals is silent on that issue.[83]

Thirdly, when the ETIAS Regulation was adopted, ECRIS-TCN was still in the negotiation phase and remained under negotiation after the proposals were published in January 2019. Indeed, as noted in the Explanatory Memorandum of the Commission package, at that time, 'agreement in principle was found by the co-legislators'. However, ECRIS-TCN does not make any reference to its future use for the purpose of supporting ETIAS purposes in border management, although it was still negotiated for months after the ETIAS Regulation was adopted in September 2018. In light of the above, the lack of any impact assessment on the implications of interoperability between ETIAS and ECRIS-TCN at all stages in the adoption of the respective legal instruments is noteworthy. In light of the above, it is evident that **the Commission package extends the scope of ECRIS-TCN beyond the agreement between the co-legislators and the wording of the ECRIS-TCN Regulation. Such expansion has evaded scrutiny at the level of an impact assessment, both when the ETIAS Regulation was adopted and when ECRIS-TCN was negotiated.**

The impact assessment gap is thus threefold, at the time: 1) when the ETIAS Regulation was proposed; 2) when the ECRIS-TCN was proposed and negotiated; and 3) when the Commission

---

78 European Commission, COM(2016) 731final.

79 For a critical assessment, see EDPS 'Opinion 3/2017 - Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)' (06.03.2017); Jeandesboz, Alegre and Vavoula (n 4).

80 European Commission, 'Feasibility Study for a European Travel Information and Authorisation System (ETIAS) (16.11.2016) 21.

81 bid. Elsewhere, it is noted that it might be interesting to reassess it if the system evolves and include data on third-country nationals. See n 80, 84.

82 European Commission, 'Policy study on an EU Electronic System for Travel Authorization (EU ESTA)' (2011).

83 Commission, 'Staff Working Document – Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA' SWD(2016) 5final.

package was proposed. This approach obscures, and further complicates, an already complex legal landscape burdened by the existence of numerous legal instruments, which can be accessed by different Member States, and the inherent technical nature of EU information systems. This approach also undermines the significance of scrutinising potential legal implications. It rather sustains an understanding that once the legal instrument concerning an EU information system has been formally adopted, any amendments may not be properly scrutinised in advance, from the perspective of their legal implications.

Furthermore, it must be stressed that the reference to ECRIS-TCN in Recital 58 of the ETIAS Regulation cannot be considered as sufficient to justify an expansion of the ECRIS-TCN scope.[84] **In accordance with the case law of the CJEU, recitals do not have independent legal value and they are not binding on their own, but are used to assist in the interpretation of the scope of ambiguous provisions.[85] The role of recitals is to provide the reasons behind the adoption of the legal act to which they are attached and cannot function as the legal basis for a legal instrument.[86]** As a result, Recital 58 in the ETIAS Regulation cannot on its own be the reason for the adoption of another legal act, as in the present case.

2.2. The proposed amendments

Against this backdrop, and in order for ECRIS-TCN to become interoperable with ETIAS, the Commission package extends the subject matter and scope of ECRIS-TCN to include 'border management' within the purposes of the system.[87] The Council replaced the term 'border management purposes' with 'support the ETIAS objectives of identifying whether the presence of ETIAS applicants in the territory of the Member States will pose security risks'.[88]

In order for the present study to remain relevant this and other relevant changes are taken into account in the assessment. Of importance in this respect is also the fact that the amendments to ECRIS-TCN have been separated from those related to SIS (law enforcement branch). The second purpose of ECRIS-TCN will be its contribution to 'facilitating and assisting in the correct identification of persons'. This purpose is meant to reflect the current legislative framework in the aftermath of the adoption of the Interoperability Regulations.[89] It is recalled that under Article 20 of the Interoperability Regulations, the CIR shall be used by national police authorities to identify third-country nationals.

---

84 Interview with experts from the EDPS (03.12.2019).

85 Tadas Klimas and Jūratė Vaičiukaitė, 'The Law of Recitals in European Community Legislation' (2008) 15(1) *ILSA Journal of International and Comparative Law* 63, 76-81. See Case C-162/97 *Nilsson and Others* ECLI:EU:C:1998:554. Its para 54 reads: ''[…] the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question'. See also General Secretariat of the Council of the European Union, 'Manual of precedents for acts established within the Council of the European Communities' (2009) https://op.europa.eu/en/publication-detail/-/publication/d451bf6b-1889-4551-a102-48bfda08340f/language-en accessed 18 November 2019.

86 In accordance with Article 296 of the Treaty on the Functioning of the European Union (TFEU) that states that '(l)egal acts shall state the reasons on which they are based and shall refer to any proposals, initiatives, recommendations, requests or opinions required by the Treaties'.

87 Amendments 1-2 of Annex II.

88 Council of the EU, Document 11300/19 (16.07.2019) 26.

89 As mentioned earlier, ECRIS-TCN data shall form part of all four interoperability components including CIR. As a result, given that the study is targeted and must take as a baseline scenario the existing legal framework this amendment will not be further assessed.

Querying ECRIS-TCN data may only take place in relation to specific offences, in respect of which a flag shall be created.[90] The Commission package refers to terrorist offences and serious crimes – definitions of which are provided in the proposed text.[91] The definitions replicate those included in other EU legal instruments governing the operation of EU information systems to ensure consistency.[92] However, the Council position has deleted the reference to terrorism and serious crimes, as well as the respective definitions, and specifies that the ECRIS-TCN records that will be flagged will relate to the offences listed in the Annex of the ETIAS Regulation, if these are punishable under national law by a custodial sentence or a detention order of a maximum period of at least three years.[93] This is a welcome amendment that delimits which criminal records will be consulted for ETIAS-related purposes.

The expansion of ECRIS-TCN to support ETIAS further signifies that the ETIAS Central Unit is included among the competent authorities so as to verify a hit against ECRIS-TCN and shall be provided with information as to which Member State(s) holds criminal record information on the third-country national, along with the reference number and any corresponding identity information.[94] The record on the criminal conviction will be acquired following a request through the de-centralised ECRIS. This is because ECRIS-TCN does not hold all information on the criminal conviction, but merely enables the identification of the Member State(s) that has such information. The ETIAS Central Unit shall have access to flagged files only, and the data may only be used for the purpose of the verification of a hit by the ETIAS Central Unit or for the purpose of consultation of the national criminal records by the ETIAS National Unit when manually processing the ETIAS application.[95]

2.3. Fundamental Rights Assessment

2.3.1. Interference with the rights to respect for private life and protection of personal data

The Commission package considers that the co-legislators expressed the intention to include ECRIS-TCN among their EU information systems that would be automatically consulted when examining ETIAS applications, as encapsulated in Recital 58 of the ETIAS Regulation. Therefore, it was not necessary to further justify the necessity and proportionality of the extension of the scope of ECRIS-TCN.[96] The amendments have been viewed as technical adjustments, merely reflecting the provisions already established in the ETIAS Regulation.

However, the use of ECRIS-TCN for ETIAS-related purposes inevitably **allows processing of the data stored for purposes different than those initially laid down in the ECRIS-TCN Regulation and for which the data were initially intended.** The risk of opening up ECRIS-TCN to immigration law

90 Amendment 4 of Annex II.

91 Amendment 3 of Annex II.

92 With the exception of VIS that provides a different definition of serious offences. See Article 2(1)(d) of Decision 2008/633/JHA.

93 Council of the EU, Document 11300/19 of 16.07.2019 (n 88) 28.

94 Amendment 6 of Annex II.

95 Amendment 5 of Annex II.

96 See Commission package on ETIAS consequential amendments (n 50-51) 2, 6. The Commission considers that the proposals are 'in line with the intention expressed by the co-legislators' in the ETIAS Regulation'.

was highlighted by FRA, which in 2015 had already called for 'express prohibition to use ECRIS-TCN for immigration law enforcement purposes outside of criminal proceedings'.[97]

As the EDPS correctly pointed out, by expanding the scope of ECRIS-TCN to assist ETIAS, **the group of authorities which will be entitled to have access to ECRIS-TCN will be enlarged** in two ways: firstly, to include the ETIAS Central Unit, which shall verify a hit pursuant to Article 20 of the ETIAS Regulation, in cases where an ETIAS applicant corresponds to a person whose personal data is recorded in ECRIS-TCN for offences listed in the Annex; and secondly, to allow ETIAS National Units to manually process the applications pursuant to Article 26 of the ETIAS Regulation.

In a series of cases, the ECtHR has held that access of the competent national authorities to personal data stored in centralised systems constitutes an interference with the right to private life, as enshrined in Article 8 ECHR.

In particular, in *Leander v. Sweden*, the ECtHR found such interference in relation to a secret police register,[98] whereas in *Rotaru v. Romania* it concerned files including information about his alleged membership of a legionnaire movement and on publication of two anti-government pamphlets, which were accessed by the Romanian Intelligence Service.[99] In *Weber and Saravia v. Germany*, the ECtHR further held that the transmission of data to other authorities and the subsequent use by them, enlarges the group of individuals with knowledge of the personal data intercepted and can therefore lead to investigations being instituted against the persons concerned.[100] In the court's view, this danger amounts an interference with the right to private life.[101]

In a similar vein, in *Digital Rights Ireland*,[102] the Grand Chamber of the CJEU found interferences with both the right to respect for private life, as enshrined in Article 7 of the EU Charter, – reiterating the ECtHR's findings[103] – and with the right to the protection of personal data, as encompassed in Article 8 of the EU Charter, because the contested legislation provided for the processing of personal data.[104] In *Schrems*, concerning the transfer to the US of personal data under the 'Safe Harbor' Agreement, the CJEU referred to the hybrid right to 'privacy with regard to the processing of personal data'.[105] In *Tele2 and Watson*, a case that followed the release of *Digital Rights Ireland*, the obligation imposed on providers of electronic communications services to retain traffic data in order to make that data available to the competent national authorities was found to raise questions relating to compatibility with Articles 7 and 8 of the EU Charter.[106]

---

97 FRA, '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' (2015) 3.

98 *Leander v. Sweden* (1987) 9 EHRR 433, para 48.

99 *Rotaru v. Romania* (2000) 8 BHRC 449, para 46.

100 *Weber and Saravia v. Germany* (2008) 46 EHRR SE5, para 79.

101 Ibid.

102 *Digital Rights Ireland* (n 59).

103 Ibid, para 35.

104 Ibid, para 36. In comparison to previous judgments of the CJEU, in *Digital Rights Ireland* the Grand Chamber did not endorse a combined reading of the two rights as was the case in *Schwarz* (Case C-291/12 *Michael Schwarz v Stadt Bochum*, ECLI:EU:C:2013:670) or in Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662. However, in the proportionality assessment its analysis eventually followed the same analytical pattern.

105 *Schrems* (n 59) para 39.

106 *Tele2 and Watson* (n 59) para 92.

In Opinion 1/15 concerning the draft EU-Canada Agreement on the transfer of Passenger Name Record (PNR) data from the EU to Canada, the Grand Chamber found that the various forms of processing to which PNR data may be subject, namely its transfer, access, use or retention, affect the right to private life.[107] Furthermore, the processing of the PNR data covered by the envisaged agreement also falls within the scope of Article 8 of the EU Charter, because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article.[108]

In *Ministerio Fiscal*, the CJEU found that the access of public authorities to electronic data retained by telecommunication providers constitutes an interference with the fundamental right to respect for private life, even in the absence of circumstances which would allow that interference to be defined as 'serious'.[109] The Court further found that it was not relevant whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way. In addition, such access was also found to constitute interference with the right to the protection of personal data, as it constitutes processing of personal data.[110]

In light of the above, **adding the ETIAS Central Unit and ETIAS National Units among the authorities allowed to process ECRIS-TCN data for ETIAS-related purposes constitutes an interference with both the rights of private life and protection of personal data, as enshrined in Articles 7 and 8 of the EU Charter respectively**. The Commission package proposes new forms of processing the personal data included in ECRIS-TCN.

As mentioned above, ECRIS-TCN was meant to assist Member States and certain EU agencies in the field of criminal justice cooperation in identifying the Member State that holds a criminal record on a third-country national. The addition of supporting ETIAS was not included among its aims. The interference with the rights to private life and protection of personal data could be considered as a serious one because the Commission package proposes that a system created in the law enforcement context will be routinely consulted for border management purposes. As it will be explained below, these fields remain separate with divergent objectives.[111] Furthermore, ECRIS-TCN was established in order to assist national authorities in accordance with national law, but by assisting the processing of ETIAS application files the system will acquie an EU purpose.

Be that as it may, **both rights are not absolute and interferences may be justified provided that specific requirements are met**. On the one hand, Article 8(2) ECHR stipulates that an interference with the right to private life may be justified if it is 'in accordance with the law' and it is 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. On the other hand, interferences with the fundamental rights encompassed in the EU Charter may be justified, provided that the requirements in Article 52(1) of the EU Charter are met; namely that the interference must be provided for by law, respect the essence of the rights and, subject to the principle of proportionality, limitations may be

[107] Opinion 1/15 (n 59) para 122.

[108] Ibid, para 123.

[109] *Ministerio Fiscal* (n 59) para 51.

[110] Ibid.

[111] See Section 2.3.2.

made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[112]

The provisions of the ETIAS Regulation and the amended provisions are clear and foreseeable enough to justify the legality requirement. Furthermore, the identification of whether an ETIAS applicant poses a security risk because he or she has been convicted of a serious criminal offence is a legitimate purpose of the EU that is aimed at maintaining an EU AFSJ. Thus, the final step in assessing the amended scope of ECRIS-TCN is by reference to the **principles of necessity and proportionality in order to determine whether the interferences with the aforementioned are justified**. As it will be shown below, a necessity and proportionality assessment is also necessary from the perspective of secondary EU data protection law. The next section will explain the relevance of EU secondary law on the protection of personal data.

2.3.2. The relevance of the purpose limitation principle - Function creep

According to the EDPS, the addition of the support for the ETIAS objectives in the list of purposes that ECRIS-TCN will serve constitutes a 'major change'[113] in the functioning of ECRIS-TCN. This is by no means an isolated phenomenon. This amendment is yet another example of a **'function creep'**, namely **the gradual widening of the use of a system or database beyond the purpose for which it was originally conceived**. According to this trend, personal data and records which have been collected, stored and further processed in an information system are casually repurposed for additional purposes other than those for which they were initially collected, without explicit justification or transparent debate.[114] This trend has been fleshed out in two ways:

1. By conceptualising multi-purpose information systems from the outset; though the personal data are collected for purposes related to immigration control, these may be further used for law enforcement purposes.[115] Examples of that trend are VIS, EES and ETIAS, which though their primary objectives relate to border management, the personal data stored are accessed under specific conditions by national law enforcement authorities and Europol in the course of criminal investigations with the aim of preventing, detecting and investigating terrorist offences and other serious crimes; and

2. Through the gradual opening up of purposes of EU information systems after adopting the respective legal instruments. The prime example in that respect is Eurodac, which was recasted in

---

[112] Despite some differences between Article 8(2) ECHR and Article 52(1) of the EU Charter (e.g. the lack of reference to the essence of the right), the approach of the EU Charter mirrors a strong strand of case law by the ECtHR. See *Rotaru v. Romania* (n 99), *Weber and Saravia v. Germany* (n 100).

[113] EDPS, 'Formal comments' (n 57) 3.

[114] The EDPS has repeatedly referred to the risk of function creep. See EDPS, 'Opinion of the European Data Protection Supervisor on the amended 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 […/…] (Recast version)' [2013] OJ C28/3; 'Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)' (18.07.2013) pt 68; 'Opinion 06/2016 on th Second EU Smart Borders Package' (21.09.2016) pt 76. For an analysis see Benedita Menezes Queiroz, *Illegally Staying in the EU - An Analysis of Illegality in EU Migration Law* (Hart 2018) Chapter 4 III.

[115] To that effect see Niovi Vavoula, *Immigration and Privacy in the Law of the EU* (n 34); 'Consultation of Immigration Databases for Law Enforcement Purposes: A Necessary and Proportionate Interference with Privacy and Data Protection Rights?' *European Journal of Migration and Law* (forthcoming 2020). A working version of this article may be found here: https://www.academia.edu/41195137/_Consultation_of_Immigration_Databases_for_Law_Enforcement_Purposes_A_Necessary_and_Proportionate_Interference_with_Privacy_and_Data_Protection_Rights accessed 18 November 2019.

2013 with the purpose of regulating law enforcement access to fingerprint data.[116] In that case, which resembles the present case of ECRIS-TCN, Eurodac was also amended without the prior conduct of a European Commission impact assessment.[117]

In both cases, the result has been the progressive transformation of all EU information systems into multi-purpose tools.[118] In addition, it is notable that EU information systems are accessed not only by national competent authorities, but by EU bodies and agencies as well (such as Europol, Eurojust, European Border and Coast Guard – EBCG – and the EPPO). However, the trend so far has been one whereby immigration-related files, alerts and records have been repurposed for law enforcement purposes - not the other way round, as is the present case.[119] This reverse 'function creep', makes the amendment of ECRIS-TCN unique in nature and it is testament of the **almost complete blurring of the boundaries between immigration and criminal law**.[120]

Despite their synergies, the fields of border management and law enforcement remain distinct, with separate objectives. The fact that personal data have already been collected and centrally stored does not automatically mean that the data may also be consulted for purposes, which are unrelated to those that justified their collection without proper justification. Regrettably, there is no relevant case law concerning the expansion of the use of personal data for purposes other than those for which they were initially collected. In *A, B and P*, a question concerning the proportionality of processing certain biometric data collected by residence permit applicants for law enforcement purposes under specific conditions was found inadmissible by the CJEU.[121]

It is also noteworthy that the proposal does not make a distinction between primary and secondary (ancillary) purposes. All EU information systems have both primary and secondary objectives (e.g. contribution in preventing, detecting and inviestigating terrorist offences or other serious crimes is an ancillary objective).[122] However, in the case of ECRIS-TCN, it is unclear whether the support of ETIAS purposes is an ancillary or a primary purpose of ECRIS-TCN, further sustaining the blurred boundaries between law enforcement and border management. The fact that support of ETIAS purposes is subject to specific rules and conditions seems to suggest that the expanded scope is an ancillary one.

Thus, the proposed amended scope of ECRIS-TCN **is difficult to reconcile with the purpose-limitation principle, which is a key principle of EU data protection law**. The GDPR lays down this

---

116 Vavoula, 'The Recast Eurodac Regulation' (n 38).

117 Four proposals were submitted to recast Eurodac, one of which concerned law enforcement access to Eurodac data. That proposal of 2009 was accompanied by an impact assessment, but was blocked by the European Parliament. The fourth revised proposal of 2012, however, which was negotiated leading to the adoption of Regulation 2013/603 was not paired with an impact assessment.

118 Both in the cases of Eurodac and ECRIS-TCN no impact assessments were conducted, whereas VIS and EES were accompanied. Therefore, ironically it may be preferable to conceptualise multi-purpose databases from the outset, so that the Impact Assessment covers all possible uses of the system, rather than amending existing legal instruments. Possible amendments may even result in lowering the level of privacy and personal data protection, because the discussions may not be fully informed on the legal implications by impact assessments.

119 This analysis excludes Europol data which are also collected for law enforcement purposes and will be used for ETIAS-related purposes. This is because of the lack of standardised categories of personal data and purposes for which Europol processes its records.

120 In his formal comments on the Commission package, the EDPS took note of the trend. See EDPS, 'Formal comments' (n 57) 4. The function creep is described as reverse, because in the previous years the information system was primarily established for border management purposes and assistance in law enforcement was an add-on. In the present case, the starting point of ECRIS-TCN was law enforcement and the added purpose is one related to border management.

121 Case C-70/18 *Staatssecretaris van Justitie en Veiligheid v A and Others*, ECLI:EU:C:2019:823.

122 See Section 1.2.2. For an analysis see European Commission, 'Overview of information management' (n 30).

principle in Article 5(1)(b) which stipulates that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This article also states that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

As explained above, ECRIS-TCN aims at enhancing judicial cooperation in criminal matters by improving the exchange of information on criminal records of third-country nationals throughout the EU. Given the criminal justice origins of ECRIS-TCN, the relevant framework providing the general principles of personal data processing in the law enforcement context is the Data Protection Directive for Law Enforcement Purposes, which is the counterpart of the GDPR in the law enforcement context. Article 4 of this Directive also provides for the purpose limitation principle. However, the content of this principle is different than that prescribed under the GDPR, In particular, personal data must be 'collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes'.

However, Article 4(2) stipulates the exceptions to the principle of purpose limitation in the law enforcement context:

> '[p]rocessing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
>
> a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
>
> b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law'.

Therefore, taking into account EU secondary data protection law relevant to the present study, the analysis concerning the purpose limitation principle requires an examination of the amendments in light of the principles of necessity and proportionality.

Overall, the analyses of Sections 2.3.1 and 2.3.2 demonstrate that the expansion of the ECRIS-TCN scope both from the perspective of the EU Charter and ECHR and EU data protection law entail a proportionality assessment. According to the CJEU, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[123]

2.3.3. Necessity of interoperability between ECRIS-TCN and ETIAS: Consistency with policies of the EU and worldwide

Consistency with EU policies

The expansion of the ECRIS-TCN purpose to support the processing of ETIAS applications may be viewed as not significantly deviating from the objectives for which conviction data may be used. Article 7 of the ECRIS-TCN Regulation allows Member States to use the information on criminal convictions in different types of procedures, which may include immigration law ones.[124] Indeed,

[123] For example see *Volker und Markus Schecke and Eifert* (n 104) para 74; *Digital Rights Ireland* (n 59) para 46; Opinion 1/15 (n 59) paras 152, 154.

[124] See Section 2.1.1.

visa, acquisition of citizenship and migration procedures, including asylum procedures, may require criminal conviction information depending on, and in accordance with, national law. From this perspective, it is argued that the expansion of ECRIS-TCN to assist ETIAS is implicitly embedded in the ECRIS-TCN Regulation. That interpretation was provided by one of the experts from eu-LISA.[125]

Furthermore, it is recalled that in accordance with Article 17(4)(a) of the ETIAS Regulation, ETIAS applicants will be asked to reply to questions as to whether they have been convicted in the past 10 years for committing an offence listed in the Annex attached to the ETIAS Regulation. Consequently, querying ECRIS-TCN will enable the verification of the accuracy of information that an ETIAS applicant has provided.

In addition, this approach is consistent with the fact that the purpose of ETIAS is to produce a risk assessment of visa-free applicants and all other EU information systems, certain Interpol databases and Europol data shall also be automatically consulted to identify potential hits. Besides, the dedicated ETIAS watchlist shall register data on persons suspected of having committed or taken part in a terrosit offence or other serious criminal offence or persons regarding who there are factual indications or reasonable grounds to believe that they will commit such offences.[126] By applying an argumentation *a minore ad maius,* it may be considered as reasonable that data on convicted third-country nationals should also be cross-checked.

Consistency with policies in other countries operating systems comparable to ETIAS

As regards the extent to which similar travel authorisation systems worldwide perform checks against criminal records, the European Commission Policy Study of 2011 on EU ESTA provides for insights from the United States and Australia.[127] On the one hand, the Electronic System for Travel Authorization (ESTA) in the Unites States is interoperable with a series of national immigration and law enforcement databases: the Automated Targeting System (ATS); the Treasury Enforcement Communications System (TECS); the Terrorist Screening Database (TSDB); the Interpol Lost or Stolen Passports Records; and the Department of State lost or stolen passport records.[128] On the other hand, the Australian Electronic Travel Authorisation (ETA) processes applications by cross-checking data stored in the Central Movement Alert List (CMAL), which registers alerts on individuals who have been convicted of serious offences. However, there is no automated processing of files on convicted foreigners .[129]

Appropriateness of consulting ECRIS-TCN data for ETIAS-related purposes

The appropriateness of consulting information on criminal conviction when examining ETIAS applications is also not to be called into question; prior convictions may be a valuable tool to indicate whether an ETIAS application may constitute a security risk to the Schengen area.

2.3.4. Necessity of interoperability between ECRIS-TCN and ETIAS: Overlap with SIS

In order to justify the additional interference with the rights to private life and protection of personal data, querying ECRIS-TCN data must be necessary for the objectives pursued.

---

[125] Interview with experts from eu-LISA (21.11.2019). The author takes the current legal framework as a baseline, therefore any concerns regarding the use of ECRIS-TCN at the national level are not relevant to the present study and these views are therefore not included.

[126] Article 24(1) of the ETIAS Regulation.

[127] European Commission, 'Policy Study' (n 82).

[128] See also Section 217 and 212 of the Immigration and Nationality Act, Pub. L. 89.

[129] European Commission, 'Policy Study' (n 82) 44-47.

Scrutinising necessity requires an examination as to whether the hits on the basis of ECRIS-TCN data may be produced through the consultation of other EU information systems which the ETIAS Regulation already prescribes for consultation. The operation of SIS is crucial in that respect, considering that one category of alerts involves third-country nationals who are unwelcome to enter or stay. In particular, Article 24(1)(a) of Regulation 2018/1861 on the operation of SIS for border checks stipulates that:

> 'Member States shall enter an alert for refusal of entry and stay when […] the Member State has concluded, based on an individual assessment which includes an assessment of the personal circumstances of the third-country national concerned and the consequences of refusing him or her entry and stay, that the presence of that third-country national on its territory poses a threat to public policy, to public security or to national security, and the Member State has consequently adopted a judicial or administrative decision in accordance with its national law to refuse entry and stay and issued a national alert for refusal of entry and stay'.

Article 24(2)(a) of the same Regulation prescribes that '[t]he situations covered by point (a) of paragraph 1 shall arise where: a third-country national has been convicted in a Member State of an offence carrying a penalty involving the deprivation of liberty of at least one year'.

The repeated use of the term 'shall' seems to indicate that the aforementioned requirement to record alerts for public policy, public security or national security purposes is mandatory for Member States' authorities. However, the registration of alerts is subject to a proportionality assessment of each individual case, pursuant to Article 21 of Regulation 2018/1861, which requires Member States to determine whether the case is 'adequate, relevant and important enough to warrant an alert in SIS'. Compared to Article 2018/1860 on the use of SIS in relation to recording return decisions, the EU legislator does not require such proportionality assessment.[130]

As a result, **alerts on convicted third-country nationals for the purposes of refusals of entry or stay may not always be entered in SIS, if national authorities do not deem it appropriate and proportionate**.

Complete overlap with SIS as regards to convictions on terrorist offences

Article 21(2) of Regulation 2018/1861 excludes terrorist offences stressing that:

> 'Where a person or an object is sought under an alert related to a terrorist offence, the case shall be considered adequate, relevant and important enough to warrant an alert in SIS'.

An exception to that rule is also included:

> 'For public or national security reasons, Member States may exceptionally refrain from entering an alert when it is likely to obstruct official or legal inquiries, investigations or procedures'.

However, this exception is unlikely to be relevant in the case of convicted third-country nationals as it involves official or legal inquiries, investigations or procedures, not convictions already handed down.

In the light of the use of the word 'shall', it is evident that since terrorist offences are excluded from the proportionality assessment, the convictions of third-country nationals in relation to terrorist offences, which feature in the Annex of the ETIAS Regulation, would already be recorded by SIS.

[130] Compare with Article 3 of Regulation 2018/1860.

There may be concerns regarding the transparency of including terrorist-related alerts in SIS and the violation of data protection law when the proportionality test is completely bypassed, but the fact remains that current EU legislation requires the inclusion of terrorist-related alerts in SIS on a mandatory basis.

This means that **if a third-country national convicted of a terrorist offence applies for travel authorisation through ETIAS, the automated processing of his or her details against SIS would necessarily generate a 'hit'** triggering the process under Articles 23 and 26 of the ETIAS Regulation. As a result, consultation of both SIS and ECRIS-TCN is redundant, as a comparison would generate two 'hits' in relation to the same conduct.

Opaque overlap with SIS as regards to convictions on offences other than terrorism-related ones

The likelihood of Member States excluding from reporting to SIS individuals convicted for the other criminal offences listed in the Annex attached to the ETIAS Regulation is dependent upon national practices. Indeed variations and divergences may exist.

Research in the 2016 European Commission evaluation of SIS,[131] the eu-LISA reports on the functioning of SIS[132] and the ad-hoc queries conducted by the European Migration Network (EMN)[133] did not reveal relevant information on current national practices with regards to the recording of alerts on third-country nationals convicted of serious offences other than terrorist-related ones. In 2005, a study by the Schnegen Joint Supervisory Authority[134] was published concerning the registration of alerts on third-country nationals under the old SIS legal framework. which highlights discrepancies among Member States when recording such alerts.[135] However, the study does not provide specific information on alerts concerning convicted third-country nationals that is relevant to the present impact assessment.[136] Overall, though Member States' authorities may record alerts on third-country nationals who have been convicted of serious offences, it is uncertain as to whether all convicted third-country nationals will be included in SIS.

Consequently, it is certain that **the revised Article 21 of Regulation 2018/1861 generates a complete overlap between ECRIS-TCN and SIS with regards to terrorist offences**. **It is also certain that there will be an overlap in the case of the other offences in the Annex of the ETIAS Regulation**. However, its full extent cannot be measured, as convicted third-country nationals for those other offences may or may not be entered in SIS. interview with the expert from the European

---

131 European Commission, 'Evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA' (Report) COM(2016) 880final.

132 For the latest report see eu-LISA, 'SIS II Technical Report 2017-18' (2019).

133 For example see European Migration Network (EMN), 'Ad Hoc Query on procedures for entering foreigner's data into the Schengen Information System' (07.01.2014) http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/505_emn_ahq_procedures_entering_foreigners_data_into_the_sis__7jan2014_(wider_dissemination).pdf accessed 18 November 2019.

134 The Schengen Joint Supervisory Authority was an independent body established under Article 115 of CISA (n 16) is an independent body established to ensure the protection of citizens' data protection rights in relation to the SIS.

135 Schengen Joint Supervisory Authority, 'Article 96 Inspection Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System' (2005).

136 Even if there was such information, the findings would be treated with caution due to the time that has passed by since the release of the study.

Commission confirms that the extent of the overlap is not verifiable.[137] The experts from eu-LISA refrained from commenting on the operations of SIS and the potential overlap with ECRIS-TCN, but highlighted that Article 21 of Regulation 2018/1861 is not yet applicable by the Member States.[138] The experts from the EDPS[139] and the FRA[140] also stressed the potential overlap between ECRIS-TCN and SIS and took note of the divergent practices of Member States. For the purposes of determining the full extent of this opaque overlap also in relation to the rest of the offences referred to in the Annex of the ETIAS Regulation, it may be worth conducting a separate study, as the existing published information in the evaluation of SIS operations by eu-LISA or the European Commission is inconclusive. Depending on national practices, that overlap may be very extensive.

Are SIS alerts on convicted third-country nationals sufficient for the operation of ETIAS?

Be that as it may, **since the purpose of these alerts is precisely to prevent the entry of unwelcome third-country nationals, those cases that deserve an alert in SIS are, and will, be entered.**

The national authorities that enter an alert in SIS for refusal of entry must have conducted an individual assessment in line with the proportionality principle to conclude that the third-country national should be refused entry or stay in the Schengen area. In fact, SIS alerts may be entered in connection to offences other than those listed in the Annex to the ETIAS Regulation, thus the scope of SIS alerts is even wider than the one of ECRIS-TCN consultation. This information should be sufficient for the ETIAS National Unit to determine the fate of the ETIAS application; after all, the alert is meant to be used for border control purposes.

There are also practicality issues. A hit in ECRIS-TCN would still require the ETIAS National Unit to have access to the criminal record of the individual through ECRIS-TCN. Only in extreme cases may the criminal record of the individual be useful to complement the SIS alert, particularly if such consultation would be to the benefit of the ETIAS applicant (for example, if the ETIAS National Unit suspects that the alert was issued disproportionately and the applicant may be granted travel authorisation).

Under the proposed rules, **querying both systems may even create friction in cases where automated processing reveals a hit with ECRIS-TCN, but no SIS alert exists**. If the national authority has already made such an assessment, it seems redundant for the ETIAS National Unit to devote time and resources to examine the hit with ECRIS-TCN. Therefore, under the proposed rules in cases where the ETIAS applicant has a criminal conviction without a corresponding SIS alert, he/she may still be denied an ETIAS authorisation. This runs counter to the individual assessment in line with the principle of proportionality that the national authorities of the convicting Member State has conducted. Depending on the Member State where the ETIAS Central Unit is based, an ETIAS applicant may have differentiated treatment. This approach may also raise concerns as to whether the proposed amendment denotes lack of trust among Member States that they do not make appropriate use of SIS to register alerts on convicted third-country nationals and, therefore, ECRIS-TCN may compensate in that respect. However, there is no such information suggesting that Member States are not using SIS efficiently to register alerts on unwelcome third-country nationals who have committed serious offences. If the EU co-legislators decide to go through with the proposed amendment, a provision determining the relationship between a SIS alert and a criminal

[137] Interview with expert from the European Commission (14.11.2019).

[138] Interview with experts from eu-LISA (21.11.2019).

[139] Interview with experts from the EDPS (03.12.2019).

[140] Interview with expert from the FRA (19.11.2019).

conviction should be included. A way forward could be to foresee that the lack of a SIS alert following an individual assessment by the convicting Member State must be taken into account when the ETIAS National Unit determines whether the applicant should be granted an ETIAS authorisation.

Since the nature of an alert differs from a conviction record, coupled by the divergent provisions laid down in ECRIS-TCN and SIS, it must be noted **that neither the personal data nor the retention period frustrate the aforementioned overlap between SIS and ECRIS-TCN with regards to terrorism offences**. In particular, a SIS alert on refusal of entry or stay is a ground for refusing entry to the Schengen area, in accordance with Articles 6(1)(d) and 14(1) of the Schengen Borders Code (SBC).[141] Furthermore, pursuant to Article 32(a)(v) of the Visa Code, it is mandatory that a short stay visa shall be refused to a person for whom an alert has been issued in SIS II for the purpose of refusing entry.[142] **Furthermore, as mentioned in the Commission evaluation of SIS, if the reason for the alert is a conviction of the third-country national in question, that is indicated in the alert.[143]**

With regard to the personal data that are collected in each case, a comparison between Article 5 of the ECRIS-TCN Regulation and Article 20(2) of Regulation 2018/1861 reveals that SIS stores more categories of personal data compared to the ECRIS-TCN. The only category of personal data that may be included in an ECRIS-TCN record which is not listed in Article 20(2) of Regulation 2018/1861 is the parents' names. However, according to Article 5(1)(a)(ii) of the ECRIS-TCN Regulation, parents' names is an optional category of information that is to be included only if it has been entered in the criminal record. Therefore, from that perspective, **there is no indication that ECRIS-TCN will provide further information than SIS that may be necessary for ETIAS-related purposes**. The criminal record obtained at a later stage by the ETIAS National Unit will provide further information, but it is suggested that this is not necessary to make an assessment on whether the applicant poses a risk. Otherwise, SIS would store that additional information as well to enable border control authorities to make an assessment.

As for the retention period of personal data, ECRIS-TCN records, which are retained in accordance with national law, could be useful when the alerts are deleted from SIS.[144] This is because, in principle, the retention period of SIS alerts is three years.[145] however the retention of alerts may be extended following a comprehensive individual assessment.[146] In an ad-hoc query of the EMN with regards to the entry of alerts on unwelcome third-country nationals it was found that in certain Member States the maximum retention period is five years, whereas in others it is 10 years or even up to 20;[147] in three Member States, there is no maximum retention period provided by law.[148] However, the Commission package (as amended by the Council) provides for consultation for ETIAS-related purposes only of those records in relation to offences listed in the Annex of the ETIAS

[141] 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) [2016] OJ L77/1.

[142] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) [2009] OJ 243/1 as amended by Regulation (EU) 2019/1155 of the European Parliament and of the Council of 20 June 2019 amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code) [2019] OJ L188/25. There are certain exceptions to those rules.

[143] Other possible indications are: Article 24(2)(b): 'security threat'; Article 24(3): 'illegal stay'; Article 26: 'restrictive measure'. See European Commission, 'Evaluation of SIS' (n 131) 31.

[144] According to Article 8 of the ECRIS-TCN Regulation criminal records are to be stored in ECRIS-TCN for as long as these are retained under national law.

[145] Article 39(2) of Regulation 2018/1861.

[146] Article 39(4) of Regulation 2018/1861.

[147] EMN (n 133).

[148] Ibid.

Regulation, which are the most serious ones, such as terrorism, participation in criminal organisation, trafficking in human beings, murder, money laundering, rape etc; in those cases, it is highly likely that Member States will extend the initial three-year period. Therefore, **depending on national practices the retention period of alerts in SIS may not be shorter than that of ECRIS-TCN records**.

In light of the above, repurposing ECRIS-TCN to also serve ETIAS-related purposes may be seen as consistent with the potential use of ECRIS-TCN data at the national level and the purpose of ETIAS to produce holistic assessments of all visa-free travellers. Furthermore, the US ESTA system consults criminal conviction information. However, **based on the operation of SIS, it is concluded that consultation of ECRIS-TCN is not necessary in relation to terrorist offences, due to the full overlap between ECRIS-TCN and SIS. The full extent of that overlap as regards to other offences is unknown due to the fact that criminal convictions in relation to serious offences other than terrorism-related ones is dependent upon national practices. Since the purpose of these alerts is for Member States to evaluate whether the conduct of an individual merits to be banned from entering or staying in the Schengen area. As a result, it is concluded that unless otherwise proven, those alerts are sufficient and suitable to serve ETIAS-related purposes.**

2.3.5. Consultation of ECRIS-TCN data on dual nationals

The scope of ECRIS-TCN does not only include information on convictions of third-country nationals, but of dual nationals as well (that is to say individuals who hold the nationality of an EU Member State and of a third country).[149] During the negotiations for the adoption of the ECRIS-TCN Regulation, the inclusion of dual nationals in the personal scope of ECRIS-TCN raised considerable criticism by legal scholars[150] and the European Parliament.[151] It is recalled that dual nationals are EU nationals and therefore enjoy free EU movement rights. This means that there will not be a dual national applying for an ETIAS authorisation – it is presumed that they will use their EU passport – and, therefore, there is no need for that data to be compared when examining ETIAS applications, as they will not generate a hit by default. As a result, the comparison of dual nationals' data against ETIAS applications is not in compliance with the principle of necessity, because those records in ECRIS-TCN are not relevant for the processing of ETIAS applications.[152] Be that as it may, the Commission package does not provide any justification as to why those data will be compared against ETIAS applications and does not make any differentiation or distinction between ECRIS-TCN data on third-country nationals and ECRIS-TCN data on dual nationals. The possibility of excluding ECRIS-TCN records on dual nationals must be considered as a way forward to avoid unnecessary processing, possibly through marking or blocking those data on dual nationals, so that the ESP is unable to compare these data against ETIAS applications.

---

149 Article 2 of the ECRIS-TCN Regulation.

150 Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), 'Registration of criminal records of Union citizens in ECRIS-TCN' (CM1812, 01.10.2018). The author agrees with this approach as ECRIS-TCN will effectively create different classes of EU nationals.

151 See Council Document 9894/18 (11.06.2018) where the European Parliament removed dual nationals from the scope of the proposal. Nevertheless, during the course of negotiations dual nationals were again included in the scope of ECRIS-TCN. See Chris Jones, 'Disproportionate and discriminatory: the European Criminal Records Information System on Third-Country Nationals (ECRIS- TCN)' (Statewatch Analysis 2019) 14-15.

152 Interview with expert from the FRA (19.11.2019).

2.3.6. The nature of personal data on criminal convictions and proportionality considerations

A key issue to be taken into consideration is the fact that **criminal records constitute a category of personal data which are more sensitive than other categories and should be subject to appropriate safeguards for the rights and freedoms of data subjects**.[153] Any processing of criminal convictions outside the framework of criminal justice cooperation is subject to the GDPR. Article 10 of the GDPR reads as follows:

> '1. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.
>
> 2. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.'

Therefore, **ECRIS-TCN data cannot be considered the same as any other type of personal data, the automated processing of which could be regulated under the same conditions as the records in other information systems**.

However, the proposed amendments provide for a series of safeguards which suggest that the special nature of criminal conviction data has been taken into consideration. This is a positive development that merits further exploration.

In particular, firstly, the Commission package prescribes that **information may only be accessible for ETIAS-related processing in respect of** terrorist offences and other serious crimes. This provision was amended by the Council to explicitly refer to **the criminal offences of the Annex attached to the ETIAS Regulation**, when punished by a custodial sentence or detention of a maximum of at least three years (as to the modalities of access by the ETIAS Central Unit and the ETIAS National Unit, see the next section).[154] This amendment ensures clarity and precision with regards to the offences which are relevant for ETIAS applications and rectifies the previous wording which was vague and allowed for expansive interpretation.

What is distinct in the case of ECRIS-TCN is that following the identification of the Member State that holds a criminal record, the ETIAS National Unit shall be able to request further information following the ECRIS route. If the convicting Member State is that of the ETIAS National Unit. the latter shall have direct access to the record. In the list of offences in the Annex, facilitation of irregular entry or stay is included within the list of offences relevant for cross-checking, which is punishable in Member States with a custodial sentence that falls within the remits of consultation.[155] It is recalled that facilitation of unauthorised entry or stay does not exclude the criminalisation of humanitarian

---

153 This understanding stems from the fact that the GDPR devotes its Article 10 to lay down specific rules as to how conviction data should be processed. The EDPS shares this understanding. See EDPS, 'Formal comments' (n 57) 4.

154 Council, Document 11300/19 of 16/07.2019 (n 88).

155 Council Framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence [2002] OJ L328/1; On the implementation see European Commission, 'Commission Staff Working Document – REFIT Evaluation of the EU legal framework against facilitation of unauthorised entry, transit and residence: the Facilitators Package (Directive 2002/90/EC and Framework Decision 2002/946/JHA)' SWD(2017) 117final.

assistance to refugees and migrants.[156] As a result, it is possible that individuals who have been convicted for providing humanitarian assistance in a Member State may be prevented from being granted an ETIAS authorisation.[157] As the expert from the FRA pointed out, the inclusion of a safeguard for those persons may be a way forward.[158] A safeguard regarding the processing of ECRIS-TCN data relating to children could also be included.[159]

The Commission package prescribes the keeping of logs of all consultations of ECRIS-TCN and the creation of statistical information by eu-LISA. If the negotiations would agree to open up ECRIS-TCN for border management purposes it is advisable that an amendment tabled by the EP requires that these statistics would be circulated to the EU institutions and the EDPS. Depending on the statistical information, it may be proven that access to ECRIS-TCN is unnecessary or redundant; therefore an additional clause that this issue could be re-evaluated in the future could also be added.

Furthermore, according to Article 5(1)(a)(iii) of the ECRIS-TCN Regulation the categories of personal data concerning the 'identity number, or the type and number of the person's identification documents, as well as the name of the issuing authority' and 'pseudonyms or aliases' constitute additional information which is to be inserted only if it is available to the central authority. Therefore, there needs to be a safeguard ensuring that any interconnection between ECRIS-TCN and ETIAS will not amount to requiring Member States to insert these categories of personal data on a mandatory basis. In other words, it is important that the table of correspondence will not lead to increasing the categories of personal data that national authorities include in their criminal records.

2.3.7. Danger of deepening the function creep?

Expanding the scope of ECRIS-TCN to assist ETIAS may grow the appetite for further expanding its purposes to assist in the operations of other EU information systems. The Commission package referred to 'border management' more generally, a term that is less precise than the one proposed by the Council.[160] Furthermore, as it will be demonstrated in the next section through the example of EES and ETIAS, there is a clear tendency to interconnect the purposes of EU information systems. By enabling one system to support others, the distinct functions of each system are progressively blurred.

Therefore, there lies the danger that the expansion of ECRIS-TCN to immigration-related purposes via ETIAS may be used as a precedent to make ECRIS-TCN available for future consultation by other EU information systems. It may increase the wish of Member States to seek consultation of criminal records of third-country nationals for border management purposes – outside the scope of Article 20 of the Interoperability Regulations – under the impression that third-country nationals are by default and *a priori* considered as security threats who are not entitled to their presumption of innocence.

Another possible effect of these amendments may be the indirect legitimisation of consulting criminal records in connection to immigration control-related procedures at the national level. That would be the case when Member States may not provide for consultation of criminal records information for certain procedures. It is recalled that Article 7 of the ECRIS-TCN Regulation enables such consultation only where, and under, the conditions national law allows. If law enforcement

---

156 See Sergio Carrera and others, *Policing Humanitarianism - EU Policies Against Human Smuggling and their Impact on Civil Society* (Hart 2019).

157 This is also possible if the convicted third-country nationals have been issued with a SIS alert.

158 Interview with expert from the FRA (19.11.2019).

159 Ibid.

160 See Council, Document 11300/19 of 16.07.2019 (n 88).

data could be routinely used in the course of examining ETIAS applications, which is an immigration procedure, then Member States may consider that criminal conviction data could be checked in the course of different types of immigration procedures, even if until now such possibility is not allowed by their national legislation. Such policies will further sustain the understanding that third-country nationals are suspected of criminality.

2.4. Key findings of Section 2

This section examined the first research question, namely whether the amendments in the Commission package concerning the use of ECRIS-TCN data for ETIAS-related purposes extend the scope of that information system and if so, whether such extension constitutes a proportionate interference with the fundamental rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter) in accordance with Article 52(1) of the EU Charter.

In a nutshell, the section found that the Commission package extends the scope of ECRIS-TCN beyond the wording of the ECRIS-TCN Regulation. This extension constitutes a serious interference with the fundamental rights to respect for private life and protection of personal data, as well as an breach of the purpose limitation principle. Though the Commission package foresees the flagging of criminal records –which is a welcome development-, the necessity of this expansion is not fully evident.

The key findings of this Section are the following:

Key finding 1:

The Commission package extends the scope of ECRIS-TCN beyond the wording of the ECRIS-TCN Regulation.

Key finding 2:

The use of ECRIS-TCN for ETIAS-related purposes is provided for in Recital 58 of the ETIAS Regulation. However, that expansion has evaded scrutiny at the level of an impact assessment, both when the ETIAS Regulation was adopted and when ECRIS-TCN was negotiated. The impact assessment gap is threefold, at the time: 1) when the ETIAS Regulation was proposed; 2) when the ECRIS-TCN was proposed and negotiated; and 3) when the Commission package was proposed.

Key finding 3:

The expansion of the scope of ECRIS-TCN constitutes a serious interference with the rights to respect for private life and protection of personal data. This is because ECRIS-TCN will be used for purposes in addition to those that were originally foreseen, and new forms of processing of personal data are proposed. This entails access to ECRIS-TCN data by the ETIAS Central Unit and the ETIAS National Units. Both rights are not absolute and interferences may be justified provided that the requirements of Article 8(2) ECHR and Article 52(1) of the EU Charter are met. Key in this respect is whether the interference complies with the principles of necessity and proportionality.

Key finding 4:

The expansion of the ECRIS-TCN scope is also difficult to reconcile with the purpose-limitation principle of EU data protection law. It is testament to the growing trend to blur the boundaries between immigration law and law enforcement, and the emergence of function creep, whereby the use of a system or a database is gradually widened beyond the purpose for which it was originally conceived. The principle of purpose limitation in the law enforcement context allows for exceptions under Article 4(2) of the Data Protection Directive for Law Enforcement Purposes. In order to assess whether the exception to the purpose limitation principle is justified an examination is required into whether the extension of the scope of ECRIS-TCN is necessary and proportionate.

Key finding 5:

The expansion of the scope of ECRIS-TCN may be seen as consistent with the potential use of ECRIS-TCN data at the national level for purposes related to immigration procedures, if these are provided for under national law. Furthermore, the purpose of ETIAS is to produce a risk assessment of visa-free travellers and all other EU information systems, certain Interpol databases and Europol data shall also be automatically consulted to identify potential hits.

Key finding 6:

The use of ECRIS-TCN data for ETIAS-related purposes is consistent with the approacgh of the the United States (ESTA), but not the Australian one (ETA). Both countries operate systems similar to ETIAS for the risk assessment of visa-free travellers.

Key finding 7:

SIS registers alerts on convicted third-country nationals for the purpose of refusing entry or stay in the Schengen area. On the one hand, alerts in connection to third-country nationals convicted of terrorist offences are mandatorily entered in SIS. On the other hand, alerts related to third-country nationals convicted of other offences are entered following an individual assessment in accordance with the principle of proportionality. There will be complete overlap between SIS and ECRIS-TCN with regards to convictions on terrorist offences. The overlap between SIS and ECRIS-TCN with regards to other offences listed in the Annex of the ETIAS Regulation will be opaque due to the discretion enjoyed by Member States in registering such alerts. Further information is required on the extent of that overlap.

Key finding 8:

The scope of SIS alerts is wider than the one for ECRIS-TCN and there is no publicly available information concerning the inadequacy of the SIS alerts in preventing the entry or stay of third-country nationals due to lack of registering alerts on convicted third-country nationals. Given that their purpose is precisely to prevent the entry of unwelcome third-county nationals, these alerts are sufficient for the purposes of examining ETIAS applications. A hit in ECRIS-TCN without an alert in SIS may complicate a decision on an ETIAS application. A comparison between the categories of personal data available to the ETIAS Central and Nationals Units demonstrates that SIS offers data sufficient and necessary for the purpose of processing ETIAS applications. As for the retention period, although SIS prescribes for a three-year retention period, the alerts may be renewed and research shows that Member States do indeed extend the retention period when necessary.

Key finding 9:

Comparing ETIAS applications against records of dual nationals is not necessary and their records should be excluded from automated processing.

Key finding 10:

The flagging of records concerning offences in the Annex of the ETIAS Regulation is a welcome approach that takes into account that criminal convictions constitute a special category of personal data in accordance with the GDPR. The keeping of logs is also a welcome addition.

Key finding 11:

Any statistical information created by eu-LISA on the basis of logs should be circulated to the EU institutions and the EDPS with a view to evaluating whether the extension of ECRIS-TCN was unnecessary.

Key finding 12:

Any interconnection between ECRIS-TCN and ETIAS should not lead to requiring Member States to collect and insert in ECRIS-TCN information which is only to be inserted if it is available to the central authority.

Key finding 13:

The expansion of ECRIS-TCN to assist ETIAS may be used as a precedent to make ECRIS-TCN available for future consultation by other EU information systems, thus eliminating the boundaries between immigration law and law enforcement. It may also legitimise the routine consultation of criminal records in the course of immigration procedures at the national level.

3. Automated processing of ETIAS application files

This section examines the second research question. This second research question concerns the fundamental rights impacts of the proposed amendments on the automated processing of ETIAS application files, which will take place by comparing the data provided by the applicant against data present in a record, file or alert registered in an EU information system (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), in Europol data and in certain Interpol databases. Given that the Commission package concerns amendments to the legal instruments of specific EU information systems, namely SIS, ECRIS-TCN, EES, ETIAS and VIS, the analysis in this section is devoted to the privacy and personal data implications of comparisons with data stored in those systems.

3.1. Preliminary remarks – Policy asymmetry

The proposal of the Commission package concerning amendments to the ETIAS, EES, VIS and SIS (law enforcement branch) Regulations (COM(2019) 4) includes amendments to the VIS Regulation to allow VIS to receive, process and answer ETIAS queries. However, this inclusion is notwithstanding the fact that in May 2018 the European Commission presented a proposal to amend the VIS Regulation.[161]

The Explanatory Memorandum of the Commission package states that the negotiations on the proposed upgrade of VIS are not sufficiently advanced and that depending on which proposal is adopted first, 'technical changes' could be required in the remaining proposal. This approach denotes an asymmetry. Although both VIS and Eurodac are under refurbishment, the Commission package has left aside amendments to Eurodac for future determinations. Nonetheless, the amendments to VIS are already being proposed on the basis of the currently applicable text.

This signifies firstly that a separate legal instrument will have to be proposed in order to govern the relations between Eurodac and ETIAS, and secondly that the VIS Regulation shall be subject to parallel amendments within a very short time frame. The EDPS took note of these developments, stressing that by interconnecting five EU information systems, the Commission package add 'both in legal and technical terms another layer of complexity to existing and future systems'.[162] As a result, the specific implications for fundamental rights of individuals 'are difficult to fully assess'.[163] Indeed, such asymmetries further complicate the convoluted legal framework on EU information systems and may undermine legal certainty and foreseeability of how the systems will operate.

3.2. Understanding automated processing

3.2.1. Automated processing in the ETIAS Regulation

ETIAS will be a platform requiring visa-exempt third-country nationals (or intermediaries) to apply for a travel authorisation to enter the Schengen area by registering a wide range of their personal data and paying a specific fee. The purpose of an ETIAS authorisation is to pre-vet visa-exempt travellers prior to their departure so as to determine whether the presence of certain third-country nationals in the territory of the Member States would pose a security, illegal immigration or high

161 See n 35.

162 EDPS, 'Formal comments' (n 57) 2.

163 Ibid.

epidemic risk. Processing ETIAS applications thus involves a comprehensive risk assessment of all visa-free travellers.

According to Article 20 of the ETIAS Regulation, the ETIAS applications shall be subject to automated processing within the ETIAS Central System with the aim of identifying one or more hits. Automated processing entails a comparison between certain categories of personal data that the ETIAS applicant shall provide[164] to the data already stored in a record, file or alert registered in ETIAS, SIS, EES and VIS. Automated processing also involves comparison with data present in the Eurodac and Europol databases as well as the Interpol SLTD and TDAWN Databases.[165] A hit will not be generated simply because personal data on an individual is present in another EU information system; Article 20(2) of the ETIAS Regulation sets out which alerts, files or records qualify as relevant to generate a hit (e.g. if the applicant is subject to specific alerts in SIS, or has been refused entry in EES, etc.).

The ETIAS Regulation also prescribes specific rules on automated processing in the following cases:

- Article 23 specifies the rules on the comparison between ETIAS applications and specific SIS alerts;
- Articles 24(6)(C)(ii) and 51(1)(b) lay down the retention period of application files in cases of refusal, revocation or annulment of an authorisation following hit(s); and
- Article 41 concerns the revocation of a travel authorisation.

In order to enable automated processing, rules on the interoperability between ETIAS, VIS, SIS, EES and ECRIS-TCN are required, since this function is not regulated in detail in the ETIAS Regulation.

Importantly, the legal instruments of the other EU information systems do not provide for the use of their respective data to assist in the administration of ETIAS applications. To those ends, the Commission package prescribes that interoperability among EU information systems will rely on the ESP, which is established by Articles 6-11 of the Interoperability Regulations.[166]

3.2.2. The requirements of automated processing

Automated processing is distinguished from automated decision-making; the former informs, and is pre-requisite of, the latter. The Article 29 Working Party[167] has defined automated decision-making

---

[164] See Article 17(2) (a), (b), (c), (d), (f), (g), (j), (k) and (m) and Article 17(8). These categories of personal data are: 1) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant; 2) other names (alias(es), artistic name(s), usual name(s)), if any; 3) other nationalities, if any; 4) type, number and country of issue of the travel document; 5) the applicant's home address or, if not available, his or her city and country of residence; 6) email address and, if available, phone numbers; 7) Member State of first intended stay, and optionally, the address of first intended stay; 8) for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian; 9) in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration; 10) IP address from which the application form was submitted.

[165] Comments on the need for an international cooperation agreement between the EU and Interpol are provided further below.

[166] During a transitional period, a tool shall be developed by eu-LISA.

[167] The Article 29 Working Party was an advisory body set up under Article 29 of Directive 95/46/EC (Data Protection Directive). It was made up of a representative from the data protection authority of each EU Member State, the EDPS and the Commission. On 25 May 2018, it has been replaced by the European Data Protection Board under the GDPR.

as 'the ability to make decisions by technological means without human involvement'.[168] Article 22 of the GDPR stipulates that:

> 'the data subject has the right not to be subject to a decision based solely on automated processing including profiling when it produces legal effects concerning him or her or at least it similarly significantly affects him or her'.

Automated decision-making is allowed when 'necessary for entering into, or performance of, a contract between the data subject and a data controller', or 'is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests', or 'is based on the consent of the individual'.[169] In the present case, automated decision-making is based on the rules in the ETIAS Regulation and therefore specific safeguards with regards to individual rights must be laid down.[170]

It must be highlighted that in the context of ETIAS processing, automated decision-making will take place in relation to all ETIAS applicants for whom, having been cross-checked against information systems and databases, no hit has been retrieved. Subsequently, a positive decision with regards to their application for an ETIAS authorisation shall be communicated to them. However, if consultation reveals one or more hits, automated processing of the ETIAS application will give way to manual processing of the personal data first by the ETIAS Central Unit, and possibly also by an ETIAS National Unit.

In its Opinion 1/15, the CJEU considered that automated processing of passengers' data would take place on the basis of pre-determined criteria and cross-checking against various Canadian databases. The CJEU found that the proportionality of the automated processing of PNR data 'depends on the pre-established models and criteria and on the databases on which that type of data processing is based'.[171]

In that respect, the Court developed a series of guidelines which are useful and relevant for the present impact assessment: firstly, 'the databases with which the PNR data is cross-checked must be reliable, up to date and limited to databases used […] in relation to the fight against terrorism and serious transnational crime'. Secondly,

> 'any positive result obtained following the automated processing of that data must […] be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the […] passengers concerned is adopted. Consequently, such a measure may not […] be based solely and decisively on the result of automated processing of PNR data'.[172]

Thirdly, it must be ensured that

> 'the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of

---

168 Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251, 2018) 8.

169 Article 22(2) of the GDPR.

170 It cannot be said that it is based on the consent of the individual. See *Schwarz* (n 104) para 32.

171 Opinion 1/15 (n 59) para 172.

172 Ibid, para 173.

> international research, be covered by the joint review of the implementation of the envisaged agreement'.[173]

The aforementioned pronouncements are central for this present section that examines the fundamental rights implications of automated processing of personal data through comparisons against data present in other EU information systems. Opinion 1/15 does not state that automated processing of personal data as such constitutes an interference with the rights to private life and protection of personal data. However, the CJEU essentially requires the information systems or databases consulted to hold reliable, updated personal data, that consultation is limited to databases which are relevant and that any individual measures that may have an adverse impact on passengers is not based solely on automated processing. For the purposes of the present study, it is submitted that access by the ETIAS National Unit constitutes an interference with the rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and to the protection of personal data (Article 8 of the EU Charter), because it enlarges the list of authorities which may consult the data and entails further processing of the personal data stored.[174] The analysis in Section 2.3.1 as regards to the case law of the European Courts remains relevant for this Section too. Therefore, it must be examined whether the modalities of such access are justified, in other words whether the proposed rules are in compliance with the principles of necessity and proportionality. The next sections will consider whether the Commission package raises concerns in that respect by reference to the criteria listed in Opinion 1/15, as laid down above.

3.2.3. The categories of personal data compared and data quality

Consultation of personal data stored in other EU information systems is not an easy process. Each system is governed by different EU instruments and pursue their own objectives[175] they also store different categories of personal data or the wording used is different. As a result, there is lack of correspondence between the categories of personal data collected in the ETIAS application files pursuant to Article 17 of the ETIAS Regulation and those present in other information systems. Such discrepancies may hamper automated processing. As the Explanatory Memorandum of the two proposals forming the Commission package notes, 'not all those data are collected or recorded in the same way in the other EU information systems'.[176] For example, the country of issue of the travel document is collected in one of the systems, while in another the same data is recorded in another way as a 'three letter code of the issuing country of the travel document'.[177] Furthermore, ETIAS will stored 'first names of parents of applicants', but this category of personal data is not processed in most of the other systems to be queried.

In order to create a level playing field, tables of correspondence have been created matching the possible extent of the data of the information systems with those of ETIAS.[178] Furthermore, Article 11 of the ETIAS Regulation is revised to lay down the categories that will be queried. A comparison between the tables and the categories of personal data collected shows that no additional data will be collected by any of the systems and that there is no discrepancy between the tables of correspondence and the proposed amended Article 11 of the ETIAS Regulation. This is a positive development, as it will ensure the smooth functioning of the automated process.

---

173 Ibid, para 174.

174 *Weber and Saravia v. Germany* (n 100).

175 Also it is recalled that the legal instrument was adopted in different timings.

176 Explanatory Memorandum attached to the Commission package foe ETIAS consequential amendments (n 50-51) 1.

177 Ibid.

178 Amendment 11 of Annex II, Amendment 4 of Annex IV, Amendment 8 of Annex V.

A key issue is whether automated processing may be affected by any concerns regarding the quality of the personal data stored. Data quality is a key principle of EU data protection law. Article 5(1)(d) of the GDPR prescribes that personal data should be 'accurate and, where necessary, kept up to date' and that 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.

The repercussions to the individual whose personal data are inaccurate may be significant, and also because the data are being shared among different actors at national and regional level (national authorities of administrative or law enforcement nature, EU agencies). Also, the larger the number of data processed and the number of processing operations, the higher the risk of inaccuracies, because the data are being compared with high volumes of personal data.[179]

The quality of personal data stored has been a longstanding problem of the currently operational EU information systems (SIS, VIS and Eurodac). Spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names into the Latin alphabet, recording of birth dates when the precise date is unknown and lack of training are only some of the reasons why EU information systems may record data that suffer in terms of quality.[180] Since the past few years, studies by the FRA have repeatedly highlighted the existence of such issues.[181] These findings are also corroborated by immigration control officers who confirm that they have identified significant mistakes in the entries included in the data systems over the course of their work.[182] In November 2019, the European Court of Auditors highlighted the importance of the quality of personal data stored and stressed that eu-LISA performs automated monthly data quality checks on certain SIS alerts.[183] These checks generate a report listing the individual alerts with potential quality issues and transmit it directly to the country concerned. The monthly reports show approximately three million warnings of potential data quality issues, which are not addressed sufficiently at the national level. Thus, their number is not significantly lower. The existence of incomplete records in SIS was also pointed out.[184]

In light of the above, **if the stored information is not of sufficient quality, any automated processing through interoperability of EU information systems may lead to incorrect processing, irregularities and false hits, with significant repercussions for third-country nationals**.[185] Interoperability of EU information systems is heavily dependent upon the high quality of the stored data.

---

179 Vavoula, *Immigration and Privacy in the Law of the EU* (n 34) Chapter 3.

180 Ibid. Since EU information systems have not generated any case law in terms of substance, therefore so far these issues have not gained the attention of the CJEU.

181 FRA, 'Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security' (2017) 30. The European Commission refers to data quality issues in VIS. See European Commission, '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) 655final, 9-10, 12.

182 'Inaccurate data in Schengen system "threatens rights"' (*euobserver,* 08.01.2018) https://euobserver.com/tickers/140468 accessed 18 November 2019.

183 European Court of Auditors, 'EU information systems supporting border control – a strong tool, but more focus needed on timely and complete data' (2019) 29-30.

184 Ibid, 31.

185 Mirja Gutheil and others, 'Interoperability of Justice and Home Affairs Information Systems (Study for the European Parliament LIBE Committee, PE 604.947 2018). Also see Quintel (n 46); Evelien Brouwer, *Interoperability and Interstate Trust: A Perilous Combination for Fundamental Rights* (*EU Immigration and Asylum Law and Policy*, 11.06.2019)

In order to rectify this thorny issue, the Interoperability Regulations empower eu-LISA to establish automated data quality control mechanisms and common data quality indicators, so that only data fulfilling the minimum quality standards are stored.[186] This is testament to the ongoing concern over improving the quality of the personal data present in the systems, **If the data stored is not of sufficient quality, then the number of false hits may rise.** A hit will trigger the intervention by the ETIAS Central Unit pursuant to Article 22 of the ETIAS Regulation. A false hit also has significant implications from an operational perspective, as it may constitute a burden for the resources of the ETIAS Central Unit, which in any case has limited capacities and may not amend the data stored.

3.2.4. Relevance of SIS data

Concerns are also raised in relation to certain alerts stored in SIS. In particular, national authorities enjoy discretion in recording alerts in SIS, which must be based on an individual assessment in accordance with the principle of proportionality. An increased number of alerts may indicate the possibility of misusing the system by inserting alerts even in cases where it is not necessary, which may have significant implications for the individuals affected.

In the context of ETIAS operations, if certain Member States are overzealous in recording alerts in SIS, when the individuals who are subject to an alert apply for an ETIAS authorisation, the automated processing of their application will generate a hit with SIS. As a result, their application may be manually processed by an ETIAS National Unit. Therefore, the national practices of entering alerts will affect the chances of ETIAS applicants receiving an ETIAS authorisation without the intervention of the ETIAS Central or National Units; this danger is real. An issue that has arisen in this respect involves the recording of alerts on individuals who should be subject to discreet checks or specific checks (or inquiry checks, under the new rules) in accordance with Articles 36-37 of the Regulation 2018/1862. The purpose of these alerts is to obtain information on persons or related objects for the purposes of preventing, detecting, investigating or prosecuting criminal offences, executing a criminal sentence and preventing threats to public security.[187] A discreet check comprises the discreet collection of information during routine activities carried out by the national competent authorities of the executing Member State.[188] An inquiry check comprises of an interview of the person,[189] whereas during specific checks, persons and objects may be searched.[190] It has been reported that alerts on discreet checks have been subject to variable practices by Member States.

https://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/ accessed 18 November 2019.

186 Recital 48 and Article 37 of the Interoperability Regulations. See also Article 12 of Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 [2019] OJ L 295/99. This is a welcome but not sufficient development, particularly given the role of eu-LISA to manage the ecisting and develop the new EU information systems. Furthermore, eu-LISA is not an agency with a clear fundamental rights mandate and has a strong technical approach. Increased supervision by the national supervisory authorities and the EDPS on how the systems operate and training of the national staff authorised to access the systems are necessary.

187 Article 36(3) of Regulation 2018/1862.

188 Article 37(3) of Regulation 2018/1862.

189 Article 37(4) of Regulation 2018/1862.

190 Article 37(5) of Regulation 2018/1862.

For example, in France it seems that alerts on discreet checks were registered 'en masse' as a response to terrorist events that occurred in 2015.[191]

This example is illustrative of how the varied application of the proportionality assessment by national authorities may have indirect repercussions in the automated processing of ETIAS application files, resulting in manual processing of the applications. Depending on the national practices and how lenient or strict certain States are in registering SIS alerts, an ETIAS application may or may not be subjected to manual processing. This means that the same conduct may not warrant a SIS alert in all Member States due to divergent practices. As a result, certain ETIAS applicants may be found to have their applications processed manually and the outcome of the processing will be uncertain, solely because a Member State may have recorded SIS alerts in bulk, potentially circumventing an individual assessment.

3.2.5. Relevance of VIS data

Another issue that merits further attention is whether automated processing of ETIAS application files against VIS data is necessary, and to what extent. The FRA Opinion on the Commission proposal for the establishment of ETIAS emphasised on the scope of VIS that it covers short-stay (Schengen) visa applicants and not visa-free travellers. The FRA opined that since VIS is not consulted during border checks in the case of visa-free nationals, consultation of VIS data when examining an ETIAS application is not necessary.[192] The present study uses the existing legal framework as a baseline. However, the author concurs that in the vast majority of situations consulting VIS data is not necessary. Such data *may* become relevant only in cases where a country was removed from the common list of countries whose citizens must have a visa when crossing the external borders ('black list'). If the country was removed since 2011, which is the year when VIS started its operations, then it is possible that VIS will contain data on nationals from these countries.[193] However, in such cases it must be justified that the cross-checking of VIS data is necessary, because the removal of a country from the 'black list' may be based on different criteria such as illegal immigration, public policy and security, economic benefit and the EU's external relations with the relevant third countries.[194] Otherwise, if the ETIAS applicant comes from a country whose nationals are not required to obtain a visa, and this has been a longstanding EU policy, before the establishment of VIS, then the automated processing against VIS will not generate a hit. Furthermore, VIS data may be relevant in the case of dual nationals who hold the nationality of two countries, one of which is on the black list and the other is on the white list. In addition, if in the future VIS will store data on long-stay visa applicants or holders of residence permits and residence cards, the VIS data may be useful for consultation. Otherwise, a comparison between the ETIAS application and VIS will not generate a hit and therefore any automated processing will be unnecessary. If a recast of the VIS Regulation is adopted in the future, it may be worth examining the possibility of distinguishing these categories

---

191 Lori Hinnant, 'France puts 78,000 security threats in vast police database' (*Associated Press*, 04.04.2018) https://apnews.com/a1690ac25cea4d5b8d2b622d3fd4e646/France-puts-78,000-security-threats-on-vast-police-database accessed 18 November 2019.

192 FRA, 'The impact on fundamental rights' (n 40) 22-24.

193 In the past years, the visa liberalisation policy has resulted in increased number of countries which have been removed from the black list due to economic considerations. The list may be found in Regulation (EU) 2018/1806 of the European Parliament and of the Council of 14 November 2018 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 [2018] OJ L303/39.

194 Article 1 of Regulation 2018/1806. As a result if the removal of a country from the 'black list' took place on the basis of economic considerations it may be held that it is justified to consult VIS because the applicants from that country may remain a risk for irregular migration.

of records in VIS to differentiate between treatment of records when ETIAS applications are cross-checked against VIS data.

3.2.6. Triggering a hit

According to the proposed Article 11(9) of the ETIAS Regulation '[a] hit shall be triggered where all or some of the data from the ETIAS application file used for the query correspond fully or partially to the data present in a record, alert, or file of the other EU information systems consulted'. It is further prescribed that it will be for the European Commission to define partial correspondence through an implementing act, including a degree of probability.

It must be recalled that a hit may result in the ETIAS Central Unit, and possibly an ETIAS National Unit, accessing the file of the ETIAS applicant in question and (as it will be mentioned below) it may have significant impact on the rights to private life and personal data protection. Therefore, it should be assessed whether it is appropriate to decide on such modalities by means of an implementing act, as proposed by the Commission, which is outside the ordinary legislative process and, therefore, the democratic control of the European Parliament. It could certainly be possible to include certain indications – perhaps in the Preamble – already in the EU legal instruments that will be adopted by the co-legislators.

3.2.7. Access by ETIAS Central Unit for verification of one or more hits

According to Article 22 of the ETIAS Regulation, the ETIAS Central Unit shall be consulted in case of one or more hits. The current wording of the Regulation stipulates that the ETIAS Central Unit shall have 'access to the application file and any linked application files, as well as to all the hits triggered during automated processing'. The purpose for such access is to verify whether the data recorded in the application file correspond to the risk indicators, the ETIAS watch list, Europol data or any data in the EU information systems. In order for the ETIAS Central Unit to have access to the hits for such verification, changes in the EU legal instruments of the underlying systems were necessary to reflect this.

The Commission package amends all relevant EU legal instruments as follows: the Regulations concerning SIS (both border control and police branch), VIS, EES and ECRIS-TCN are amended to include a new provision according to which the 'ETIAS Central Unit […] shall have, for the purposes of its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search data entered in that EU information system'.[195]

The proposed Article 11(8) of the ETIAS Regulation further specifies that:

> 'Where hits are identified, the tool referred to in Article 11, shall make temporarily available the results in the application file to the ETIAS Central Unit, until the end of the manual process pursuant to Article 22(2) and Article 23(3).'[196]

The Commission package thus expands the categories of authorities able to get access to the personal data stored in the EU information systems to include the ETIAS Central Unit. According to the proposed Article 11(8) of the ETIAS Regulation, the ETIAS Central Unit shall only have temporary access to the results of the automated processing for as long as the manual processing is ongoing.

---

[195] Compare Amendment 5 of Annex V, Amendment 3 of Annex 1 and VI, Amendment 6 of Annex II and Amendment 2 of Annex IV. In the case of ECRIS-TCN it is recalled that the ETIAS Central Unit shall onl have access to those data records to which flags have been added.

[196] Amendment 4 of Annex III. The Council has clarified that the results 'of the automated processing' shall be available. See Council, Document 11300/19 of 16 July 2019 (n 88) 47.

As stated in Section 2.3.1 and reiterated in Section 3.2.2 of this study, the transfer of data that expands the categories of authorities that get access to the data constitutes an interference with the rights to private life and to the protection of personal data. This is because the personal data stored are re-purposed to assist in the administration of ETIAS applications. Therefore, the amendments must be evaluated with regards to their compliance with the principles of necessity and proportionality.

This assessment, however, does not concern ETIAS; according to Article 13 of the ETIAS Regulation, the ETIAS Central Unit has access to the ETIAS Information System. Key issues to consider in that respect are a) the records, files or alerts available to the ETIAS Central Unit, b) the temporal scope of that availability and c) the processing activities.

The personal data available to the ETIAS Central Unit

Firstly, with regards to the personal data available, the proposed amendments provide for 'a right to access and search relevant data' in accordance with the proposed Article 11(8). The latter refers to the 'results of the automated processing'. **The term 'relevant' data must be interpreted in a strict manner, so as to include only the hits that have been produced during the automated process by the ETIAS Central System and not to include the processing of the whole record, alert or file in respect of the third-country national in question.** Such interpretation is confirmed by an expert in the European Commission who noted that only the identity information that triggered the hit shall be temporarily accessed by the ETIAS Central Unit. [197]

Limited time of availability of personal data

Secondly, in relation to the time for which the ETIAS Central Unit shall be able to have access to the relevant data, the proposed Article 11(8) of the ETIAS Regulation limits access for the duration of the manual process. This provision should be interpreted as meaning a maximum of 12 hours from receipt of an application file in accordance with Article 22(6) of the ETIAS Regulation. It should not be interpreted as allowing access to the ETIAS Central Unit when the application is processed by an ETIAS National Unit, pursuant to Article 26 of the ETIAS Regulation. This interpretation is in line with the operation of the ETIAS Central Unit, the task of which is solely to verify the existence of one or more hits.[198]

Limited processing of personal data

Thirdly, the ETIAS Central Unit shall have limited room for manoeuvre when accessing and searching the relevant data in the EU information systems, as its mandate is limited to verifying the existence of one or more hits, or the existence of doubts as to the identity of the ETIAS applicant. In case there is no correspondence between the ETIAS file and data in the EU information systems, the ETIAS Central Unit shall be able to delete the false hit.[199] No correction or deletion of personal data is possible and the only change that the ETIAS Central Unit should be able to make should be in relation to deleting false hits. This is a welcome approach and in line with the fact that the ETIAS Central Unit will not be a competent authority that shall have full access to the EU information systems aside from the identity data that produced a hit.[200]

---

197 Interview with expert from the European Commission (14.11.2019).

198 This interpretation is also confirmed by the interview with the expert from the European Commission (14.11.2019).

199 Article 22(4) of the ETIAS Regulation.

200 In that respect, it culd be added that in cases of false hits the ETIAS Central Unit could notify the competent authorities of the Member State that inserted the data that produced a hit so that it draws their attention to the potential of an

As will be shown below, the ETIAS National Units will also have the possibility to consult the systems whereby only the outcome of the processing shall be recorded.[201] **It may be questioned why there is no reference to the fact that the ETIAS Central Unit will also have a read-only access to the information systems, given that aside from deleting false hits, no other operations are foreseeable**.

Finally, the ETIAS Central Unit shall not be able to copy or transfer data or combine data from EU information systems with data of the EBCG. Otherwise, temporary access will become a window of opportunity for the ETIAS Central Unit to search relevant data for purposes unrelated with the automated processing of ETIAS applications. A welcome provision in that respect is the proposed Article 22(7) of the ETIAS Regulation.[202] It stipulates that a record shall be kept of all data processing operations carried out for assessment of the applications by the ETIAS Central Unit.

3.2.8. Manual processing by the ETIAS National Units

In cases where a hit is verified, or any doubt with regards to the identity of the ETIAS applicant remains, Articles 25 and 26 provide for the intervention by the responsible ETIAS National Unit, which will manually process the application. In that regard, Article 26 of the ETIAS Regulation allows for access to the application file and any linked application files, as well as to any hits triggered during the automated processing.

In order for ETIAS National Units to manually process the applications, the EU legal instruments concerning the operation of EU information systems must specify that the ETIAS National Units are among the national authorities granted access to the EU information systems. This is not currently the case. This has led to the addition of the ETIAS National Units in the list of the national competent authorities allowed to have direct access to the EU information systems in a read-only format for the purpose of manually processing the ETIAS applications.[203]

Both Articles 22 and 26 of the current ETIAS Regulation use the same wording when referring to the access by the ETIAS Central and National Units: 'access to the application file and any linked application files, as well as to all the hits triggered during automated processing […]'. This does not mean that access by the ETIAS Central Unit and the ETIAS National Units should necessarily take place under the same conditions. This is because the ETIAS Central Unit will be based in the EBCG, which is an EU institution and will solely have limited capacities (to verify a hit), whereas the ETIAS National Unit shall have the task to determine whether an ETIAS applicant shall be granted a travel authorisation.

Thus the ETIAS National Unit looks into the application file in much greater depth than the ETIAS Central Unit to reach a decision on the ETIAS application files. Such determination may involve a request for additional information or documentation to be provided by the applicant, including through an interview.[204] Therefore, it is necessary that the ETIAS National Unit has access to the alert, record or file in the EU information systems where one or more hits have been found.

Given that the ETIAS National Unit shall only be able to record in the application file the outcome of the manual process in the ETIAS application file, access to other EU information systems is provided

error (perhaps the MID would also be useful). Such possibility could lead to the enhancement of the quality of the data in the EU information systems and prevent false hits in the future.

201 See below Section 3.2.7.

202 Amendment 8 of Annex III.

203 Compare Amendment 2 of Annex I, Amendment 10 of Annex III, Amendment 1 of Annex IV; Amendment 2 of Annex IV; Amendment 3 of Annex 5; Amendment 3 of Annex VI.

204 Article 27 of the ETIAS Regulation.

for on a read-only basis. In the case of ECRIS-TCN, access concerns the identification of the Member State that holds records. Therefore, direct access to the criminal record of the ETIAS applicant shall be able only if the convicting Member State is the same as the Member State of the ETIAS National Unit that manually processes the application. In other cases, the ETIAS Central Unit shall have access to the criminal record via the de-centralised ECRIS route, namely by contacting the convicting Member State to obtain the criminal record. The ETIAS National Units will thus become competent national authorities that can have access to all EU information systems.

It must be highlighted that whereas the proposed Article 25a of the ETIAS Regulation refers to a read-only format in relation all EU information systems, **the amendments to the SIS Regulations do not make a reference to the fact that access by the ETIAS National Units is on a read-only basis**. The amendments related to EES and VIS, however, explicitly refer to read-only access. The lack of consistent wording is significant, because a reader of the SIS Regulations should be able to understand how authorities shall access the SIS data without having to cross-check other EU legal instruments on the side.

3.2.9. Other amendments on automated processing

This Section focuses on other amendments included in the Commission package that relate to the automated processing of ETIAS application files, namely the keeping of logs of data processing operations, the requirement to conclude an agreement with Interpol and the inclusion of 'inquiry checks' among the alerts compared against ETIAS data. Though not directly involving the expansion of categories of authorities that shall process data from the EU information systems, these amendments relate to automated processing of ETIAS applications.

Keeping of logs and supervision

Another amendment common to all EU instruments involves the requirement of keeping logs for the purpose of interoperability with ETIAS.[205] In particular, logs of each data processing operation carried out within each system and ETIAS shall be kept. This is a key amendment that will enable transparency of operations and facilitate supervision of the activities carried out both by national supervisory authorities[206] and the EDPS.[207] Supervisory duties are dependent upon the ability to track previous logs. This requirement is also crucial, as according to Article 67(3) of the ETIAS Regulation, the EDPS may ask eu-LISA and the ETIAS Central Unit to give them access to all documents and to their logs. Therefore, any misuse of data or inappropriate data processing activities may be tracked through the keeping of logs.

Automated processing of ETIAS application files through comparison against SIS alerts on 'inquiry checks'

According to the Explanatory Memorandum of the Commission package, one of the main objectives of the proposals is to establish the relations between ETIAS and SIS, the legal basis of which was agreed after the adoption of the ETIAS Regulation. It is recalled that according to Article 4 of the ETIAS Regulation, one of the objectives of the system is:

> 'to support the objectives of SIS related to alerts of third-country nationals subject to a refusal of entry and stay, alerts on persons wanted for arrest for surrender purposes

[205] Amendment 1 of Annex I, Amendment 10 of Annex II, Amendment 3 of Annex IV, Amendment 6,7 of Annex V, Amendment 1 of Annex VI.

[206] Supervision by national data protection authorities is enshrined in Article 66 of the ETIAS Regulation.

[207] Supervision by the EDPS is enshrined in Article 67 of the ETIAS Regulation. Furthermore, each system contains its own rules on supervision.

> or extradition purposes, alerts on missing persons, alerts on persons sought to assist with a judicial procedure and alerts on persons for discreet checks or specific checks'.

Article 23 of the ETIAS Regulation further elaborates on the use of specific SIS alerts in determining ETIAS applications and the respective modalities and safeguards.

Articles 36 and 37 of Regulation 2018/1862 establish a new alert category on inquiry checks. In particular, Article 37(4) of Regulation 2018/1862 prescribes that an inquiry check shall comprise an interview of the person, including on the basis of information or specific questions added to the alert by the issuing Member State. One of the consequential amendments to the ETIAS Regulation has been the inclusion of inquiry checks among the alerts cross-checked against the ETIAS application file during the automated process. This amendment expands the categories of alerts, which will be available to ETIAS for verification. In case of a hit, the applicant's data shall be accessed by the ETIAS Central Unit and potentially the ETIAS National Unit. An assessment seems to have been conducted by the Commission since the Explanatory Memorandum of the Commission package excludes from cross-checking alerts on return decisions,[208] noting that:

> 'It is not proposed to include the alert category on return decisions as such alerts are erased at the moment a return decision is implemented. This means that persons that apply for an ETIAS authorisation after having left the EU will –by definition – not have a return record in the SIS'.[209]

Given that the alerts on specific and discreet checks are also included within the alerts compared with ETIAS applications, it is not disproportionate to extend this requirement to inquiry checks. As mentioned in Section 3.2.4., a discreet check involves the discreet collection of information during routine activities carried out by the national competent authorities of the executing Member State.[210] An inquiry check comprises of an interview of the person[211] and during specific checks, persons and objects may be searched.[212] An inquiry check thus constitutes an intermediary step between discreet checks and specific checks. As a result, since the ETIAS Regulation already allows the cross-checking of alerts on discreet checks, which are lighter in terms of the impact to individuals subject to the SIS alert that is flagged up on inquiry checks, *a minore ad maius* it is concluded that an inquiry check should also be consulted during the examination of an ETIAS application.

Nevertheless, reference must again be made to the requirements for registering these alerts; it is recalled that an individual assessment is required, in accordance with the principle of proportionality and on the basis of a national decision.[213] Therefore, the analysis in Section 3.2.3 remains relevant for this Section as well. In a nutshell, since the insertion of these alerts is dependent upon national practices, which may vary significantly among Member States, individuals with the same conduct and characteristics may be subject to inquiry checks in one Member State, but not in another.

---

208 As mentioned earlier, Article 3 of Regulation 2018//1860 requires the mandatory registration of all SIS alerts on return decision against third-country nationals.

209 Explanatory Memorandum attached to the Commission package foe ETIAS consequential amendments (n 51-52) 2-3.

210 Article 37(3) of Regulation 2018/1862.

211 Article 37(4) of Regulation 2018/1862.

212 Article 37(5) of Regulation 2018/1862.

213 Article 21 of Regulation 2018/1862.

International agreement with Interpol for the purpose of comparing ETIAS applications against Interpol databases

Article 12(1) of the ETIAS Regulation envisages that ETIAS shall query the Interpol SLTD and TDAWN databases. The only safeguard that is currently included is that 'no information shall be revealed to the owner of the Interpol alert'. In conjunction with Article 65 of the ETIAS Regulation, it is evident that ETIAS applications would be made available to Interpol for the purpose of automated processing.

Therefore, the Commission package requires the conclusion of a cooperation agreement between the EU and Interpol that will lay down the modalities of exchanging information and the inclusion of safeguards for the protection of personal data. The conclusion of such a cooperation agreement will be subject to Article 218 TFEU, according to which the European Parliament will be required to provide its consent. The reference to the need for an international agreement must be seen in the broader context of the difficulties in concluding an agreement between the EU and Interpol, which would need to be in compliance with EU data protection law. The inclusion of this provision is a welcome development.

It is also welcome that in the wait for this agreement, no comparison between ETIAS application files and Interpol data shall occur.[214] Given that the ETIAS Regulation already contains a safeguard that the owner of the Interpol alert shall not be aware of the annual processing it may be worth adding further safeguards. For example, the keeping of logs of each data processing operation within Interpol could be required, regular supervision, as well as prohibition of further transfer not only to the owner of the Interpol alert, but also to other national or international entities.

3.3. Effective remedies

The right to an effective remedy is enshrined in Article 47 of the EU Charter, as well as in Article 13 ECHR. In the context of personal data processing in EU information systems, this right is also essential to ensure that the rights of private life and of personal data protection are respected. The impact assessment requires considering whether the Commission package has an impact on the exercise of the right to effective remedies. Furthermore, in a complex legal framework of numerous EU information systems that are interoperable, the effective protection of the right becomes all the more important. Each EU information system contains provisions concerning the exercise of the right to effective remedies, but the exercise of the right is subject to national law. This may lead to significantly divergent practices between the Member States,resulting in uneven protection of the right.[215]

The right to an effective remedy is envisaged in the ETIAS Regulation in cases of applications refused, annulled or revoked. In case an application is refused, the applicant shall be provided with a statement of the grounds for refusal of the travel authorisation, indicating which ground is applicable in their case (information in an EU system, information in Europol databases, etc.) and by allowing individuals whose ETIAS applications have been refused, annulled or revoked to have a right to lodge an appeal.[216]

---

214 Amendment 13 of Annex III.

215 For the exercise of the right to effective remedies as regards SIS see Brouwer, *Digital Borders and Effective Rights* (n 29). With respect to VIS, there is no legal scholarship available, but the exercise of the right has been discussed by the European Commission in its evaluation of VIS. See European Commission, 'Evaluation of VIS' (n 178) 12.

216 Article 38(2)(d), Article 40(3) and Article 41(7) of the ETIAS Regulation.

In his Opinion on the ETIAS Regulation, the EDPS stressed that an applicant should receive sufficiently clear indication of the ground(s) for refusal in order to efficiently exercise his or her appeal and contest the reasons for the refusal.[217] In that respect, the EDPS rightly suggested specifying the information to be provided to rejected applicants, notably if the refusal is due to a hit with any other IT system.

In light of the above, **it is crucial that individuals whose applications were refused have knowledge that a record exists, and which information system has generated a hit that led to the refusal of their application. This will enable them to exercise their individual rights under the ETIAS Regulation, but also under the legal instruments in other EU information systems.** Providing the applicant with such information must remain subject to the existing rules and limitations regarding the exercise of the right to information, as found in the legal instruments of each EU information system (e.g. individuals subject to SIS alerts have different rights of information compared to visa applicants whose personal data are present in VIS). Although the Commission package does not provide for an amendment in that respect, given the forthcoming negotiations it may be worth revisiting this issue, because this is an opportunity to strengthen the exercise of individual rights of ETIAS applicants who will be enabled to obtain knowledge with regards to the records stored in EU information systems and resort to national procedures for rectification or deletion of these records, if they consider such processes are necessary.

3.4. Automated processing of personal data between EES and ETIAS

The final part of this study is devoted to the amendments that involve the relationship between EES and ETIAS. In particular, Article 4 of the ETIAS Regulation on the objectives of the system will be expanded to include that ETIAS will support the objectives of EES. Similarly, Article 6(1) of the EES Regulation will include 'support of the objectives of ETIAS' among its objectives.

This is not a new development; the ETIAS Regulation already states that the system shall support the objectives of another information system, SIS, in relation to alerts on unwelcomed third-country nationals.[218] The close link between the two systems stems from the fact that the scope *ratione personae* of EES includes visa-free travellers for a short-say, which is precisely the scope of the application of ETIAS.

Furthermore, the setting up of these two information systems coincides with the forthcoming development of the CIR under the Interoperability Regulations. Therefore, the current text of the ETIAS Regulation provides in Article 6(3) that these systems should share and re-use hardware and software components. The revised Article 6(3) stipulates that the future CIR shall be built on the basis of data by both ETIAS applicants and third-country nationals registered in EES. The data shall be logically separated and subject to existing access rights.

This quasi-co-dependence between the two information systems is further exemplified by the automated querying and importation of certain categories of personal data from the ETIAS application file to EES. The Explanatory Memorandum of the Commission package states that it is required to align the way in which the two systems are working together, so as to rationalise and simplify the work of border guards through the implementation of a more uniform border control process for all third-country nationals entering for a short-stay. Therefore, the reasons behind these

[217] EDPS, 'Opinion 3/2017' (n 79) 17-18.

[218] Article 4(e) of the ETIAS Regulation.

changes mostly pertain to the efficiency of the border control process. In particular, the following elements shall be inserted in the EES from ETIAS:

(a) Whether or not the person has a valid travel authorisation and, in case of an authorisation with limited territorial validity, the Member State that granted it;

(b) Any flag attached to the travel authorisation (pursuant to Articles 36(2) and (3) of the ETIAS Regulation);

(c) Whether the travel authorisation shall expire within the next 90 days and the remaining validity period;

(d) For minors, the surname and first name, home address, email address and (if available) phone number of the person exercising parental authority or of the applicant's legal guardian;

(e) Where he or she claims the status of family member exempt of a visa requirement pursuant to Article 2(1), his or her status of family member, as well as the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties; also his or her family ties with that family member;

(f) Application number; and

(g) End of the validity period of an ETIAS authorisation.

The direct insertion of certain ctegories of personal data from the ETIAS record to EES, expands the categories of personal data that are inserted in EES when an entry/exit record of a visa-exempt third-country national is created. Data minimisation is a key principle of EU data protection, which is relevant in the present case. The fact that these categories of personal data have already been collected by ETIAS does not automatically mean that EES is entitled to also import data, even if the two systems have a partially overlapping personal data scope.

Article 5(1)(c) of the GDPR requires that the personal data processed must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (data minimisation). Furthermore, the categories of personal data must not go beyond what is necessary and proportionate in relation to the objectives pursued by EES.

With regard to element (d) as listed above regarding the inclusion of information on family members of the ETIAS applicant, it is worth comparing the proposed provision with the current rules on the interoperability between EES and VIS in relation to visa holders who cross the external EU border. In particular, Article 8 of the EES Regulation states that visa-related data shall be retrieved and imported automatically, and Article 16(2) of the EES Regulation specifies the categories of personal data as follows:

i) The date and time of the entry;
ii) The border crossing point of the entry and the authority that authorised the entry;
iii) Where applicable, the status of the third-country national indicating that he or she is a third-country national who is a member of the family of a Union citizen and does not hold a residence card or a residence permit;
iv) The short-stay visa sticker number, including the three letter code of the issuing Member State, the type of short-stay visa, the end date of the maximum duration of the stay, and the date of expiry of the validity of the short-stay visa;
v) Number of entries and duration of stay;
vi) Information on whether the visa was issued with a limited territorial validity; and

vii) For Member States which are not full Schengen States a notification that the third-country national used a national short-stay visa for the entry.

Therefore, and by analogy to the categories of personal data imported to EES from VIS, the elements listed above under (a), (b), (c), (f) and (g) are directly related to the administration of visa-free travellers at the borders so as to determine the duration of authorised stay, pursuant to Article 11 of the EES Regulation, and as such do not raise proportionality concerns.

With respect to the addition in EES that a visa-exempt traveller has family ties to a person enjoying EU free movement rights, that status is also imported from VIS. However, there is a discrepancy in that EES will not hold any personal data in relation to the family members of visa applicants, whereas a series of personal data will be directly imported from ETIAS. Such information shall enable the border control authorities to verify at a later stage whether the visa-free traveller remains a family member of a person enjoying EU free movement rights.

The storage of these data in ETIAS would be sufficient for such subsequent checks at the borders since both EES and ETIAS may be accessed by border control authorities, but only EES may be accessed by national competent authorities during checks on national territory.[219] Finally, with regard to the inclusion of data on legal guardians of minors, this addition is meant to assist in identifying minors who are victims of human trafficking. However, that objective is not among the purposes of EES as laid down in Article 6 of the EES Regulation.

[219] Compare Articles 4 of ETIAS Regulation and 6 of EES Regulation.

3.5. Key findings of Section 3

This section examined the second research question, namely whether the amendments in the Commission package concerning the automated processing of personal data pose challenges to the protection of the rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter). Due to its close link with the aforementioned rights, compliance with the right to effective remedies (Article 47 of the EU Charter and Article 13 ECHR) was also examined.

In a nutshell, the section found that the provisions on manual processing by the ETIAS Central and National Units are relatively well-balanced, but certain clarifications are useful. However, automated processing may suffer due to existing data quality issues from which EU information systems suffer. The relevance of unlawful SIS alerts and all VIS data is doubtful.

The key findings of this Section are the following:

Key finding 14:

The Commission package complicates the convoluted legal framework of EU information systems and undermines legal certainty and foreseeability of how the systems will operate. Further amendments will be required with regards to the relationship between Eurodac and ETIAS (through a separate act) and the relationship between VIS and ETIAS (since the revised legal framework of VIS is currently negotiated).

Key finding 15:

Drawing from the pronouncements of the CJEU on the automated processing of personal data in Opinion 1/15, automated processing of personal data should take place by comparing ETIAS application files against personal data present in databases that are reliable, up to date and limited to those necessary for the purpose of processing. Any individual measures that may have an adverse impact on travellers must not be based solely on automated processing.

Key finding 16:

Automated processing of ETIAS applications through consultation of EU information systems constitutes an interference with the rights to respect for private life (Article 7 EU Charter and Article 8 ECHR) and to the protection of personal data. This is because new forms of processing of personal data are foreseen and new authorities will have access to stored data. The ETIAS Central Unit will have access to the identity data that have generated a hit, whereas the ETIAS National Units will have access to the EU information systems. In order to assess the necessity and proportionality of this interference, the pronouncements of the CJEU in Opinion 1/15, as outlined above, were used as the benchmark.

Key finding 17:

No additional data will be collected by any of the systems and no discrepancies are evident when comparing the tables of correspondences and the proposed Article 11 of the ETIAS Regulation.

Key finding 18:

EU information systems suffer from data quality issues (spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names, etc.). If the stored information is not of sufficient quality, any automated processing may lead to incorrect processing and irregularities, with significant repercussions for third-country nationals. Besides, the greater the number of information systems and the more data contained therein, the greater the possibility of a false hit.

Key finding 19:

Depending on national practices, some SIS alerts may not be relevant for ETIAS-related purposes. SIS has been criticised for storing alerts of doubtful lawfulness, because certain Member States may have applied a very strict proportionality assessment.

Key finding 20:

The relevance of VIS data is also uncertain, as its scope involves visa applicants, whereas ETIAS concerns visa-free travellers. As a result, the automated processing of ETIAS applications against personal data on third-country nationals coming from countries which are not 'black-listed' may not generate a hit, due to the different scope between the two EU information systems. VIS may be of interest in relation to dual nationals (nationals coming from one country on the black list and a country on the white list) and following the adoption of a revised EU legal framework on VIS that will expand its scope. Under this expanded scope VIS will store records on long-stay visa applicants and holders of residence permits and residence cards.

Key finding 21:

Temporary access by the ETIAS Central Unit is necessary and proportionate to the purpose of manually processing the hits produced by the ETIAS Central System. If the ETIAS Central Unit does not have some form of access to the data that generated a hit, the verification of a hit will not be possible. The purpose of processing is limited to verifying the hits or the existence of doubt with regards to the identity of the applicant, whereby the ETIAS Central Unit may only delete a false hit from the system and perform no other operation. An addition that their right to search and access the relevant data is on a read-only basis and merely involves the data that generated a hit may be useful in order to make the provisions in the SIS, VIS, EES and ECRIS-TCN Regulations clearer. This addition will mean that there will be no need to cross-check the rules in the ETIAS Regulation which refer to read-only access.

Key finding 22:

ETIAS National Units shall become competent authorities for the purpose of manually processing ETIAS applications, which means that they will have read-only access to all EU information systems. The amendments to the SIS Regulations do not make a reference to the fact that access by the ETIAS National Units is on a read-only basis.

Key finding 23:

The keeping of logs on data processing operations is a welcome development, as it will allow supervision of the data processing activities.

Key finding 24:

Comparison of ETIAS application files against the new category of SIS alerts on 'inquiry checks' is not disproportionate to the aims pursued by SIS, as long as the registration of these alerts is lawful. This is because 'inquiry checks' constitute an intermediate step in between 'discreet checks' and 'specific checks'. Under the ETIAS Regulation, both these alerts will be consulted when examining an ETIAS application.

Key finding 25:

The requirement to conclude an international cooperation agreement with Interpol for the purpose of enabling comparison of ETIAS application files against certain Interpol databases is a welcome development. The EU co-legislators may wish to consider the addition of some safeguards in the ETIAS Regulation.

Key finding 26:

The right to effective remedies requires informing the ETIAS applicant about the database which has generated a hit that resulted in the refusal of the travel authorisation; however, this provision of information should be subject to the limitations of the rights to information in the underlying systems (e.g. SIS).

Key finding 27:

With regards to the automated processing of ETIAS data through direct importing in EES, there are divergences between the data that will be imported from VIS and the data that will be imported from ETIAS (details on family members and minors), which are not necessary in light of the objectives of EES.

4. Conclusion

This targeted impact assessment examined the following two main research questions:

a) Whether the amendments in the Commission package concerning the use of ECRIS-TCN data for ETIAS-related purposes extend the scope of that information system and if so, whether such extension constitutes a proportionate interference with the fundamental rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter), in accordance with Article 52(1) of the EU Charter;
b) Whether the amendments in the Commission package concerning the automated processing of personal data raise concerns as regards to the protection of the rights to respect for private life (Article 7 of the EU Charter and Article 8 ECHR) and protection of personal data (Article 8 of the EU Charter). Due to its close link with the aforementioned rights, compliance with the right to effective remedies (Article 47 of the EU Charter and Article 13 ECHR) was also examined.

Having provided the contextual framework within which the Commission package was proposed, the study devoted one section per research question, basing the findings on desk research and four semi-structured interviews with EU stakeholders. The study was conducted in accordance with the European Commission's 2017 Better Regulation Guidelines,[220] particularly its chapter 3, and corresponding relevant parts of the Toolbox 15 when conducting the analysis, notably Tool#28 on fundamental rights and human rights.[221]

4.1. Summary of findings: Section 2

Section 2 highlighted that the **Commission package extends the scope of ECRIS-TCN beyond the wording of the ECRIS-TCN Regulation**. **The fact that Recital 58 of the ETIAS Regulation refers to the possible use of ECRIS-TCN for ETIAS-related purposes is not sufficient legal basis**.

This expansion constitutes a serious interference with the rights to respect for private life and protection of personal data; ECRIS-TCN will be used for **purposes other than those that were originally foreseen, and new forms of processing of personal data are proposed**. This entails access to ECRIS-TCN data by the ETIAS Central Unit and the ETIAS National Units. Both rights are not absolute and interferences may be justified provided that the requirements of Article 8(2) ECHR and Article 52(1) of the EU Charter are met. Key in this respect is whether the interference complies with the principles of necessity and proportionality.

From the perspective of EU secondary law on protection of personal data the study concluded that the extension of the scope of ECRIS-TCN is **difficult to reconcile with the purpose-limitation**. It is testament to the growing trend to blur the boundaries between immigration law and law enforcement, and the **emergence of function creep, understood as the use of a system or a database is gradually widened beyond the purpose for which it was originally conceived**. The principle of purpose limitation in the law enforcement context allows for exceptions under Article

[220] 2017 Better Regulation Guidelines, chapter 3 : Guidelines on impact assessment: https://ec.europa.eu/info/sites/info/files/better-regulation-guidelines.pdf accessed 18 November 2019.

[221] 2017 Better Regulation Toolbox: https://ec.europa.eu/info/better-regulation-toolbox_en accessed 18 November 2019.

4(2) of the Data Protection Directive for Law Enforcement Purposes (Directive 2016/681). In order to assess whether the exception to the purpose limitation principle is justified an examination is required into whether the extension of the scope of ECRIS-TCN is necessary and proportionate.

4.1.1. Issues that are assessed (relatively) positively[222]

Consistency with EU and US policies

The study found that the extension of the scope of ECRIS-TCN may be seen as **consistent with the potential use of ECRIS-TCN data at the national level for purposes related to immigration procedures, if these are provided for under national law and subject to domestic rules**. Furthermore, the purpose of ETIAS is to produce **a risk assessment of visa-free travellers** and all other EU information systems, certain Interpol databases and Europol data shall also be automatically consulted to identify potential hits. The dedicated ETIAS watchlist will hold information on persons suspected of having committed or taken part in a terrorist event or serious crime. Furthermore, the use of ECRIS-TCN data for ETIAS-related purposes is consistent with the approach of the United States as regards to the operation of the Electronic System for Travel Authorisation (ESTA), but not with the Australian approach.

Flagging of records

The flagging of records concerning offences in the Annex of the ETIAS Regulation is a welcome development that takes into account that criminal convictions constitute a special category of personal data in accordance with the GDPR.

4.1.2. Issues of concern

Overlap with SIS and lack of evidence that SIS alerts are insufficient for assessing the risk that ETIAS applicants pose

The study stressed that SIS registers alerts on convicted third-country nationals for the purpose of refusing entry or stay in the Schengen area. On the one hand, **according to the current legal framework of SIS, alerts in connection to third-country nationals convicted of terrorist offences are mandatorily entered in SIS**. On the other hand, **alerts related to third-country nationals convicted of other offences are entered following an individual assessment in accordance with the principle of proportionality**. **There will be complete overlap between SIS and ECRIS-TCN with regards to convictions on terrorist offences. The overlap between SIS and ECRIS-TCN with regards to other offences listed in the Annex of the ETIAS Regulation will be opaque due to the discretion enjoyed by Member States in registering such alerts**. The full extent of the overlap is unknown.

However, the scope of SIS alerts is wider than the one for ECRIS-TCN and **there is no publicly available information concerning the inadequacy of the SIS alerts in preventing the entry or stay of third-country nationals due to lack of registering alerts on convicted third-country nationals**. **Given that their purpose is precisely to prevent the entry of unwelcome third-county nationals, these alerts are sufficient for the purposes of examining ETIAS applications**. A hit in ECRIS-TCN without an alert in SIS may even complicate a decision on an ETIAS application. The information offered by SIS is necessary and sufficient for the purpose of processing ETIAS applications. As for the retention period, although SIS prescribes for a three-year retention period,

[222] The term 'relatively' is used firstly because the analysis is based on the current regulatory framework, despite any concerns that could be raised, and secondly because in relation to some aspects of the Commission package which have been assessed as proportionate the author makes certain recommendations.

the alerts may be renewed and research shows that Member States do indeed extend the retention period when necessary.

Dual nationals

Comparing ETIAS applications against records of dual nationals is not necessary and their records should be excluded from automated processing.

Danger of deepening the function creep

The expansion of ECRIS-TCN to assist ETIAS may be used as a precedent to make ECRIS-TCN available for future consultation by other EU information systems, thus eliminating the boundaries between immigration law and law enforcement. It may also legitimise the routine consultation of criminal records in the course of immigration procedures at the national level.

4.2. Summary of findings: Section 3

Section 3 stressed that the Commission package complicates the convoluted legal framework of EU information systems and undermines legal certainty and foreseeability of how the systems will operate. Further amendments will be required with regards to the relationship between Eurodac and ETIAS (through a separate act) and the relationship between VIS and ETIAS (since the revised legal framework of VIS is currently negotiated).

The study found that automated processing constitutes an interference with the rights to respect for private life (Article 7 EU Charter and Article 8 ECHR) and to the protection of personal data. This is because new forms of processing of personal data are foreseen and new authorities will have access to stored data. The ETIAS Central Unit will have access to the identity data that have generated a hit, whereas the ETIAS National Units will have access to the EU information systems. In order to assess the necessity and proportionality of this interference, the pronouncements of the CJEU in Opinion 1/15 were used as the benchmark.

4.2.1. Issues that are assessed (relatively) positively[223]

Personal data processed

No additional data will be collected by any of the systems and no discrepancies are evident when comparing the tables of correspondences and the proposed Article 11 of the ETIAS Regulation.

Access by the ETIAS Central Unit

Temporary access by the ETIAS Central Unit is necessary and proportionate to the purpose of manually processing the hits produced by the ETIAS Central System. If the ETIAS Central Unit does not have some form of access to the data that generated a hit, the verification of a hit will not be possible. The purpose of processing is limited to verifying the hits or the existence of doubt with regards to the identity of the applicant, whereby the ETIAS Central Unit may only delete a false hit from the system and perform no other operation.

Access by the ETIAS National Units

ETIAS National Units shall become competent authorities for the purpose of manually processing ETIAS applications, but they will have read-only access to all EU information systems.

223 Ibid.

Keeping of logs

The keeping of logs is a welcome development, as it will allow supervision of the data processing activities.

Automated processing of SIS alerts on 'inquiry checks'

Comparison of ETIAS application files against the new category of SIS alerts on 'inquiry checks' is not disproportionate to the aims pursued by SIS, **as long as the registration of these alerts is lawful**. This is because 'inquiry checks' constitute an intermediate step in between 'discreet checks' and 'specific checks'. Under the ETIAS Regulation, both these alerts will be consulted when examining an ETIAS application.

Cooperation agreement with Interpol

The requirement to conclude an international cooperation agreement with Interpol for the purpose of enabling comparison of ETIAS application files against certain Interpol databases is a welcome development.

4.2.2. Issues of concern

Data quality and increased number of false hits

EU information systems suffer from data quality issues (spelling errors, lack of documentation, insufficient language skills, technical deficiencies, incorrect transcription of names, etc.). **If the stored information is not of sufficient quality, any automated processing may lead to incorrect processing and irregularities, with significant repercussions for third-country nationals**. Besides, the greater the number of databases and the more data contained, the greater the possibility of a false hit.

Relevance of certain (unlawfully registered) SIS alerts

Depending on national practices, some SIS alerts may not be relevant for ETIAS-related purposes. SIS has been criticised for storing alerts of doubtful lawfulness, because certain Member States may have circumvented the proportionality assessment.

Relevance of VIS records

The relevance of VIS data is also uncertain, as its scope involves visa applicants, whereas ETIAS concerns visa-free travellers. As a result, the automated processing of ETIAS applications against personal data on third-country nationals coming from countries which are not 'black-listed' may not generate a hit, due to the different scope between the two EU information systems. VIS may be of interest in relation to dual nationals (nationals of a country on the black list and a country on the white list) and following the adoption of a revised EU legal framework on VIS that will expand its scope. Under this expanded scope VIS will store records on long-stay visa applicants and holders of residence permits and residence cards.

Right to effective remedies

The right to effective remedies requires informing the ETIAS applicant about the database which has generated a hit that resulted in the refusal of the travel authorisation; however, this provision of information should be subject to the limitations of the rights to information as envisaged in the legal instruments of the information systems (e.g. SIS).

Interoperability between EES and ETIAS

With regards to the automated processing of ETIAS data through direct importing in EES, there are divergences between the data that will be imported from VIS and the data that will be imported from ETIAS (details on family members and minors), which are not necessary in light of the objectives of EES.

4.3. Recommendations

Throughout the study, a series of recommendations have been proposed to the co-legislators. Overall, the main recommendations are the following:

- Inclusion of a recital on a general fundamental rights and data protection safeguard;
- Evaluation of why SIS alerts are not sufficient for the purpose of examining ETIAS application files and removal of ECRIS-TCN from the list of EU information systems consulted during the automated process; More information could be requested from the Commission and/or eu-LISA;
- Exclusion of dual nationals' data stored in ECRIS-TCN from being compared against ETIAS applications;
- The language used when describing the purpose of ECRIS-TCN is precise and clear (the Council approach as evidence in Council Document 11300/19 is welcome in that respect);
- A provision could be included accoding to which the lack of a SIS alert is taken into account when the ETIAS National Unit assesses the ETIAS application file.
- Any statistical information created by eu-LISA on the basis of logs should be circulated to the EU institutions and the EDPS with a view to evaluating in the future whether the extension of ECRIS-TCN was unnecessary;
- Any interconnection between ECRIS-TCN and ETIAS should not lead to requiring Member States to collect and insert in ECRIS-TCN information which is only to be inserted if it is available to the central authority;
- Inclusion of a safeguard for persons who are convicted for providing humanitarian assistance and a safeguard for children.
- It should be assessed whether it is appropriate to decide on the modalities of determining the existence of a hit by means of an implementing act, which is outside the ordinary legislative process and, therefore, the democratic control of the European Parliament.
- An addition in the legal instruments of the EU information systems that the right to search and access the relevant data by the ETIAS Central Unit is on a read-only basis and merely involves the data that generated a hit may be useful. This will make the provisions in the SIS, VIS, EES and ECRIS-TCN Regulations clearer and there will be no need to cross-check the rules in the ETIAS Regulation which refer to read-only access.
- The amendments to the SIS Regulations do not make a reference to the fact that access by the ETIAS National Units is on a read-only basis.
- The EU co-legislators may wish to consider the addition in the ETIAS Regulation of some safeguards as regards to the cooperation agreement with Interpol.

4.4. Final remarks

This targeted impact assessment was necessary in order to inform the negotiations between the co-legislators on the amendments proposed in the Commission package. According to Article 39 of Regulation 2018/1725 on the protection of natural persons with regard to the processing of

personal data by the EU institutions, bodies, offices and agencies,[224] the controller must carry out a Data Protection Impact Assessment (DPIA) for all processing operations likely to result in a high risk to the rights and freedoms of data subjects before the start of the processing.

Overall, the study has shown that **the proposed amendments do not qualify as 'technical adjustments',** as indicated in the Explanatory Memorandum of the Commission package. On the contrary, the amendments **have considerable fundamental rights implications, particularly with regards to the rights to respect for private life and protection of personal data**.

Article 39(10) of Regulation 2018/1725 creates an exemption from the requirement to carry out a DPIA provided that (a) a specific legal basis regulates the specific processing operation or set of operations in question, and (b) a DPIA was already carried out as part of a general impact assessment for the proposed legal basis. The study has demonstrated that **the Commision package has evaded scrutiny at the level of an impact assessment, both when the ETIAS Regulation was adopted and when ECRIS-TCN was negotiated.**

The impact assessment gap is threefold, at the time: 1) when the ETIAS Regulation was proposed; 2) when the ECRIS-TCN was proposed and negotiated; and 3) when the Commission package was proposed.

[224] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] 295/39.

REFERENCES

Article 29 Working Party, 'Guidelines on Automated individual deision-making and Profiling for the purposes of Regulation 2016/679' (WP251, 2018).

Brouwer E, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff, 2008.

_____, 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders - Citizens, Migrants, Humans: Liber Amicorum in honour of prof.dr. Elspeth Guild* (Wolf Legal Publishers 2019).

_____, 'Interoperability and Interstate Trust: A Perilous Combination for Fundamental Rights' (*EU Immigration and Asylum Law and Policy*, 11.06.2019) https://eumigrationlawblog.eu/interoperability-and-interstate-trust-a-perilous-combination-for-fundamental-rights/.

Carrera S and others, *Policing Humanitarianism - EU Policies Against Human Smuggling and their Impact on Civil Society* (Hart 2019).

Cole C and Quintel T, 'Data Retention under the Proposal for an EU Entry/Exit System (EES) Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union' (Legal Opinion for the Greens, 2017).

Council of the EU, Document 11300/19 (16.07.2019).

_____, Document 9894/18 (11.06.2018).

_____, Document 9376/16 (30.05.2016).

European Commission, 'Commission Staff Working Document – REFIT Evaluation of the EU legal framework against facilitation of unauthorised entry, transit and residence: the Facilitators Package (Directive 2002/90/EC and Framework Decision 2002/946/JHA)' SWD(2017) 117final.

_____, 'Evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA' (Report) COM(2016) 880final.

_____, 'Staff Working Document – Impact Assessment accompanying the proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA' SWD(2016) 5final.

_____, '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) 655final.

_____, 'Feasibility Study for a European Travel Information and Authorisation System (ETIAS)' (16.11.2016).

_____, 'Stronger and Smarter Information Systems for Borders and Security' (Communication) COM(2016) 205final.

_____, 'The European Agenda on Security' (Communication) COM(2015) 185final.

_____, 'Policy study on an EU Electronic System for travel Authorization (EU ESTA)' (2011).

_____, 'Overview of information management in the area of freedom, security and justice' (Communication) COM(2010) 385final.

European Court of Auditors, 'EU information systems supporting border control – a strong tool, but more focus needed on timely and complete data' (2019).

EDPS, 'Formal comments of the EDPS on two proposals to establish the conditions for accessing other EU information systems for ETIAS purposes' (13.03.2019).

_____, 'Opinion 3/2017 EDPS - Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)' (06.03.2017).

_____, 'Opinion 06/2016 on the Second EU Smart Borders Package (21.09.2016).

_____, 'Opinion of the European Data Protection Supervisor on the proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)' (18.07.2013).

_____, 'Opinion of the European Data Protection Supervisor on the amended 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 […/…] (Recast version)' [2013] OJ C28/3.

European Migration Network, 'Ad Hoc Query on procedures for entering foreigner's data into the Schengen Information System' (07.01.2014) http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/ad-hoc-queries/border/505_emn_ahq_procedures_entering_foreigners_data_into_the_sis__7jan2014_(wider_dissemination).pdf.

eu-LISA, 'SIS II Technical Report 2017-18' (2019).

FRA, 'The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS) – Opinion of the European Union Agency for Fundamental Rights' (2017).

_____, 'Fundamental Rights and the Interoperability of EU Information Systems: Borders and Security' (2017).

_____, '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' (2015).

General Secretariat of the Council of the European Union, 'Manual of precedents for acts established within the Council of the European Communities' (2009) https://op.europa.eu/en/publication-detail/-/publication/d451bf6b-1889-4551-a102-48bfda08340f/language-en.

Gutheil M and others, 'Interoperability of Justice and Home Affairs Information Systems (Study for the European Parliament LIBE Committee, PE 604.947 2018).

Hinnant L, 'France puts 78,000 security threats in vast police database' (*Associated Press*, 04.04.2018) https://apnews.com/a1690ac25cea4d5b8d2b622d3fd4e646/France-puts-78,000-security-threats-on-vast-police-database.

ICT, 'ICT Final Report - Assessment of ICT impacts of the legislative proposal for ECRIS TCN system regarding the exchange of convictions for third country nationals and stateless people (TCN)' (4.12.2015).

Jeandesboz J, Alegre S and Vavoula N, European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection, European Parliament Study for the LIBE Committee, PE 583.148, 2017.

Jones C, 'Disproportionate and discriminatory: the European Criminal Records Information System on Third-Country Nationals (ECRIS- TCN)' (Statewatch Analysis 2019).

Klimas T and Vaičiukaité J, 'The Law of Recitals in European Community Legislation' (2008) 15(1) *ILSA Journal of International and Comparative Law* 63.

Menezes Queiroz B, *Illegally Staying in the EU - An Analysis of Illegality in EU Migration Law* (Hart 2018).

Quintel T, 'Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals' (2018) 4 *European Data Protection Law Review* 470.

_____, 'Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention' (University of Luxembourg Law Working Paper No. 002-2018)

https://orbilu.uni.lu/bitstream/10993/35318/1/Teresa%20Quintel%20Interoperability%20of%20EU%20Databases.pdf.

Schengen Joint Supervisory Authority, 'Article 96 Inspection Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System' (2005).

Standing Committee of Experts on International Immigration, Refugee and Criminal Law (Meijers Committee), 'Registration of criminal records of Union citizens in ECRIS-TCN' (CM1812, 01.10.2018).

UNiSYS, 'Feasibility Study: Establishing a European Index of Convicted Third Country Nationals' (11.06.2010).

Vavoula N, *Immigration and Privacy in the Law of the European Union: The Case of Databases,* Brill Nijhoff, forthcoming 2020.

_____, 'The "Puzzle" of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Data Protection', *European Law Review* (forthcoming 2020) https://www.academia.edu/40601618/The_Puzzle_of_EU_Large-Scale_Information_Systems.

_____, 'Consultation of Immigration Databases for Law Enforcement Purposes: A Necessary and Proportionate Interference with Privacy and Data Protection Rights?' *European Journal of Migration and Law* (forthcoming 2020) https://www.academia.edu/41195137/_Consultation_of_Immigration_Databases_for_Law_Enforcement_Purposes_A_Necessary_and_Proportionate_Interference_with_Privacy_and_Data_Protection_Rights.

_____, 'The Recast Eurodac Regulation: Are Asylum Seekers Treated as Suspected Criminals?' in Céline Bauloz and others (eds), *Seeking Asylum in the European Union: Selected Protection Issues Raised by the Second Phase of the Common European Asylum System* (Brill 2015).

_____, 'Interoperability of European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?' (*EU Immigration and Asylum Law and Policy*, 08.07.2019) https://eumigrationlawblog.eu/interoperability-of-european-centralised-databases-another-nail-in-the-coffin-of-third-country-nationals-privacy/.

'Inaccurate data in Schengen system "threatens rights"' (*euobserver,* 08.01.2018) https://euobserver.com/tickers/140468.

Case Law

Case C-70/18 *Staatssecretaris van Justitie en Veiligheid v A and Others*, ECLI:EU:C:2019:823.

Case C-207/16 *Ministerio Fiscal,* ECLI:EU:C:2018:788.

Opinion 1/15, ECLI:EU:C:2017:592.

Joined Cases C-203/15 and C-698/15 T*ele2 Sverige AB v Post-och Telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*, ECLI:EU:C:2016:970.

Case C-362/14 *Maximilian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

C-291/12 *Michael Schwarz v Stadt Bochum*, ECLI:EU:C:2013:670.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662.

C-482/08 *UK v Council* ECLI:EU:C:2010:631.

Case C-162/97 *Nilsson and Others* ECLI:EU:C:1998:554.

Leander v. Sweden (1987) 9 EHRR 433.

Rotaru v. Romania (2000) 8 BHRC 449.

Weber and Saravia v. Germany (2008) 46 EHRR SE5.

Annex I: Amendments to Regulation (EU) 2018/1862 (SIS – law enforcement branch)

Amendment 1

New Article 18a: Keeping of logs for the purpose of the interoperability with ETIAS

Logs of each data processing operation carried out within SIS and ETIAS pursuant to Article 50a and 50b shall be kept in accordance with Article 18 of this Regulation and Article 69 of Regulation (EU) No 2018/1240 of the European Parliament and of the Council.

Amendment 2

Revision of Article 44(1): National competent authorities having a right to access data in SIS

Current wording	Proposed amendment
1. National competent authorities shall have access to data entered in SIS and the right to search such data directly or in a copy of the SIS database for the purposes of: (a) border control, in accordance with Regulation (EU) 2016/399; (b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities; (c) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies; (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third country nationals who are illegally entering or staying on the territory of the Member States; (e) security checks on third-country nationals who apply for international protection, insofar as authorities performing the checks are not 'determining authorities' as defined in point (f) of Article 2 of Directive 2013/32/EU of the European Parliament and of the Council, and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004	Addition of element under (f) that reads: (f) manual processing of ETIAS applications by the ETIAS National Unit, pursuant to Article 8 of Regulation (EU) 2018/1240.

Comments: Addition of ETIAS National Unit among the authorities accessing SIS.

Amendment 3

New Articles 50a and b: Access to SIS data by the ETIAS Central Unit and interoperability with ETIAS

1. The ETIAS Central Unit, established within the European Border and Coast Guard Agency in accordance with Article 7 of Regulation (EU) 2018/1240, shall have, for the purpose of performing its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search relevant data entered in SIS. Article 50(4) to (8) of this Regulation shall apply to this access and search.

2. Where a verification by the ETIAS Central Unit confirms the correspondence of the data recorded in the ETIAS application files to an alert in SIS, Articles 23, 24 and 26 of Regulation (EU) 2018/1240 shall apply.

Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240

1. From the start of operations of ETIAS, as provided for in Article 88(1) of Regulation (EU) 2018/1240, the Central System of SIS shall be connected to the tool referred to in Article 11 of Regulation (EU) 2018/1240 to enable the automated processing referred to in that Article.

2. The automated processing referred to in Article 11 of Regulation (EU) 2018/1240 shall enable the verifications provided for in Articles 20, 23, Article 24(6)(c)(ii), Article 41 and Article 54(1)(b) and the subsequent verifications provided for in Articles 22, 23 and 26 of that Regulation.

3. For the purpose of verifications referred to in Article 20(2)(a), (d) and (m)(i) and Article 23 of Regulation (EU) 2018/1240, the ETIAS Central System shall use the tool referred to in Article 11 of that Regulation to compare the data referred to in Article 11(5) Regulation 2018/1240 to data in SIS, in accordance with Article 11(8) of that Regulation.

4. Where a search by ETIAS reports one or several hits pursuant to Article 23(1) of Regulation (EU) 2018/1240, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that entered the alert in accordance with Article 23(2) and (3) of that Regulation.

Where a new alert referred to in Article 41(3) of Regulation (EU) 2018/1240 is entered in SIS on travel documents, reported stolen, misappropriated, lost or invalidated, SIS shall transmit the information on this alert, using the automated processing and the tool referred to in Article 11 of that Regulation to the ETIAS Central System in order to verify whether this new alert corresponds to an existing travel authorisation

Comments: These articles enable the ETIAS Central Unit to access SIS data and regulate interoperability between ETIAS and SIS for the purpose of automated processing of ETIAS applications.

Annex II: Amendments to Regulation (EU) 2019/816 (ECRIS-TCN)

Amendment 1

Revision of Article 1: Subject matter of ECRIS-TCN

Current wording	Proposed amendment
(a) a system to identify the Member States holding information on previous convictions of third-country nationals ('ECRIS-TCN'); (b) the conditions under which ECRIS-TCN shall be used by the central authorities in order to obtain information on such previous convictions through the European Criminal Records Information System (ECRIS) established by Decision 2009/316/JHA, as well as the conditions under which Eurojust, Europol and the EPPO shall use ECRIS- TCN.	Addition of paragraph that reads: (d) the conditions under which data included in the ECRIS-TCN system may be used for the purpose of border management in accordance with Regulation (EU) 2018/1240 of the European Parliament and of the Council.

Comments: This amendment prescribes an additional objective for which ECRIS-TCN will be related to border management. Note the change in the Council Document 11300/19 of 16 July 2019.

Amendment 2

Revision of Article 2: Scope of ECRIS-TCN

Current wording	Proposed amendment
This Regulation applies to the processing of identity information of third-country nationals who have been subject to convictions in the Member States for the purpose of identifying the Member States where such convictions were handed down. With the exception of point (b)(ii) of Article 5(1), the provisions of this Regulation that apply to third-country nationals also apply to citizens of the Union who also hold the nationality of a third country and who have been subject to convictions in the Member States.	This Regulation applies to the processing of identity information of third country nationals who have been subject to convictions in the Member States for the purpose of identifying the Member State(s) where such convictions were handed down, **as well as for the purposes of border management [and contributing to facilitating and assisting in the correct identification of persons].** With the exception of point (ii) of Article 5(1)(b), the provisions of this Regulation that apply to third country nationals also apply to citizens of the Union who also hold a nationality of a third country and who have been subject to convictions in the Member States.";

Comments: This amendment in the scope of the ECRIS-TCN is meant to reflect the added purpose of the system and the interoperability of ECRIS-TCN within the framework of CIR.

Amendment 3

Revision of Article 3: Definitions

Current wording	Proposed amendment
'competent authorities' means the central authorities and Eurojust, Europol and the EPPO, which are competent to access or query ECRIS-TCN in accordance with this Regulation;	'competent authorities' means the central authorities and the Union bodies (Eurojust, Europol, the European Public Prosecutor's Office, the ETIAS Central Unit established within the European Border and Coast Guard Agency) competent to access or query the ECRIS-TCN system in accordance with this Regulation;"
-	'terrorist offence' means an offence which corresponds or is equivalent to one of the offences referred to in Directive (EU) 2017/541 of the European Parliament and of the Council.
-	'serious criminal offence' means an offence which corresponds or is equivalent to one of the offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA**, if it is punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

Comments: With this amendment, the definition of competent authorities includes also the ETIAS Central Unit and definitions of terrorist offences and serious crimes are added. Note the changes in the Council Document 11300/19 of 16 July 2019.

Amendment 4

Revision of Article 5: Data entry in ECRIS-TCN

Current wording	Proposed amendment
1. For each convicted third-country national, the central authority of the convicting Member State shall create a data record in the central system. The data record shall include: (a) as concerns alphanumeric data: (i) information to be included unless, in individual cases, such information is not known to the central authority (obligatory information): — surname (family name), — first names (given names), — date of birth, — place of birth (town and country), — nationality or nationalities, — gender, — previous names, if applicable, — the code of the convicting Member State,	In addition to the data referred to the left side of this table, ECRIS-TCN shall store: (c) where applicable, a flag indicating that the person concerned has been convicted for a terrorist offence or other serious criminal offence, and in those cases the code of the convicting Member State(s). The CIR shall contain the data referred to in points (b) and (c) of paragraph 1 and in paragraph 2, as well as the following data referred to in point (a) of paragraph 1: surname (family name); first name(s) (given name(s)); date of birth; place of birth (town and country); nationality or nationalities; gender; the type and number of the person's travel document(s), as well as the name of the issuing authority thereof; and where applicable previous names, pseudonyms(s) and/or alias name(s), as well as, in the cases referred to in point (c) of paragraph 1, the code of the convicting Member State. The remaining ECRIS-TCN data shall be stored in the ECRIS-TCN Central System.

(ii) information to be included if it has been entered in the criminal record (optional information): — parents' names, (iii) information to be included if it is available to the central authority (additional information): — identity number, or the type and number of the person's identification documents, as well as the name of the issuing authority, - pseudonyms or aliases; (b) as concerns fingerprint data: (i) fingerprint data that have been collected in accordance with national law during criminal proceedings; (ii) as a minimum, fingerprint data collected on the basis of either of the following criteria: — where the third-country national has received a custodial sentence of at least 6 months; or — where the third-country national has been convicted of a criminal offence which is punishable under the law of the Member State by a custodial sentence of a maximum period of at least 12 months.	

Comments: Differentiation of criminal records through the creation of a flag.

Amendment 5

Revision of Article 7(5): Use of ECRIS-TCN for identifying the Member States holding criminal records information

Current wording	Proposed amendment
When querying ECRIS-TCN, the competent authorities may use all or only some of the data referred to in Article 5(1). The minimum set of data that is required to query the system shall be specified in an implementing act adopted in accordance with point (g) of Article 10(1).	In the event of a hit, the Central System [or the CIR] shall automatically provide the competent authority with information on the Member State(s) holding criminal record information on the third country national, along with the associated reference number(s) referred to in Article 5(1) and any corresponding identity information. Such identity information shall only be used for the purpose of verification of the identity of the third country national concerned. The result of a search in the Central System may only be used for the purpose of making a request according to Article 6 of Framework Decision 2009/315/JHA, a request referred to in Article 16(4) of this Regulation, or for the purposes of border management [and facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN system].

Comments: This amendment is meant to assist ECRIS-TCN in supporting ETIAS.

Amendment 6

New Article 7a: Use of the ECRIS-TCN system for ETIAS verifications

1. The ETIAS Central Unit, established within the European Border and Coast Guard Agency in accordance with Article 7 of Regulation (EU) 2018/1240, shall have, for the purpose of performing its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search ECRIS-TCN data in the [CIR]. However, it shall only have access to data records to which a flag has been added in accordance with Article 5(1)(c) of this Regulation.

2. The [CIR] shall be connected to the tool referred to in Article 11 of Regulation (EU) 2018/1240 to enable the automated processing referred to in that Article.

3. Without prejudice to Article 24 of Regulation (EU) 2018/1240, the automated processing referred to in Article 11 of Regulation (EU) 2018/1240 shall enable the verifications provided for in Article 20 and the subsequent verifications of Articles 22 and 26 of that Regulation.

For the purpose of proceeding to the verifications of Article 20(2)(n) of Regulation (EU) 2018/1240, the ETIAS Central System shall use the tool referred to in Article 11 of Regulation (EU) 2018/1240 to compare the data in ETIAS with the data flagged in ECRIS-TCN [in the CIR], pursuant to Article 5(1)(c) of this Regulation and in accordance with Article 11(8) of Regulation 2018/1240, and using the correspondences listed in the table in Annex II.";

Comments: This change allows ECRIS-TCN to be used for ETIAS-related purposes and enables the ETIAS Central Unit to have access to specific ECRIS-TCN records.

Amendment 7

Revision of Article 8(2): Retention period for data storage

Current wording	Proposed amendment
Upon expiry of the retention period referred to in paragraph 1, the central authority of the convicting Member State shall erase the data record, including any fingerprint data or facial images, from the central system. The erasure shall be done automatically, where possible, and in any event no later than one month after the expiry of the retention period.	Upon expiry of the retention period referred to in paragraph 1, the central authority of the convicting Member State shall erase the data record, including any fingerprints, facial images or flags as referred to in Article 5(1)(c), from the Central System [and the CIR]. In those cases where the data related to a conviction for a terrorist offence or other form of serious crime as referred to in Article 5(1)(c) are deleted from the national criminal record, but information on other convictions of the same person is retained, only the flag referred to in Article 5(1)(c) shall be removed from the data record. This erasure shall take place automatically, where possible, and in any event no later than one month after the expiry of the retention period.

Comments: This amendment ensures that where a criminal record includes a flag for a terrorist offence or a serious crime and the retention period expires the flag is removed. If the person has other convictions, which are more recent, then these will remain.

Amendment 8

Revision of Article 24(1): Purpose of the processing of personal data

Current wording	Proposed amendment
1. The data entered into the central system shall only be processed for the purpose of the identification of the Member States holding the criminal records information on third-country nationals.	The data included in the Central System [and the CIR] shall only be processed for the purpose of the identification of the Member State(s) holding the criminal records information of third country nationals, as well as for the purposes of border management [as well as for facilitating and assisting in the correct identification of persons registered in the ECRIS-TCN system].

Amendment 9

Article 32(3): Use of data for reporting and statistics

Current wording	Proposed amendment
Every month eu-LISA shall submit to the Commission statistics relating to the recording, storage and exchange of information extracted from criminal records through ECRIS-TCN and the ECRIS reference implementation. eu-LISA shall ensure that it is not possible to identify individuals on the basis of those statistics. At the request of the Commission, eu-LISA shall provide it with statistics on specific aspects related to the implementation of this Regulation.	Every month eu-LISA shall submit to the Commission statistics without allowing for individual identification relating to the recording, storage and exchange of information extracted from criminal records through the ECRIS-TCN system and the ECRIS Reference implementation, including on the data records which include a flag in accordance with Article 5(1)(c).

Amendment 10

New Article 29a: Keeping of logs for the purpose of ETIAS

Current wording	Proposed amendment
-	For the consultations listed in Article 7a of this Regulation, a log of each ECRIS-TCN data processing operation carried out within [the CIR] and ETIAS shall be kept in accordance with Article 69 of Regulation (EU) No 2018/1240.

Amendment 11

New Annex II: Table of correspondences referred to in Article 7a

Data of Article 17(2) of Regulation 2018/1240 sent by ETIAS Central System	**The ECRIS-TCN corresponding data of Article 5(1) of this Regulation in [the CIR] against which the ETIAS data should be checked**
surname (family name)	surname (family name)
surname at birth	previous name(s)
first name(s) (given name(s))	first name(s) (given name(s))
other names (alias(es), artistic name(s), usual name(s))	pseudonym and/or alias name(s)
date of birth	date of birth
place of birth	place of birth (town and country)
country of birth	place of birth (town and country)
sex	gender
current nationality	nationality or nationalities
other nationalities (if any)	nationality or nationalities
type of the travel document	type of the person's identification documents
number of the travel document	number of the person's identification documents
country of issue of the travel document	name of the issuing authority

Comments: This table of correspondence assists in rectifying the divergences that exist in the language used in the respective legal bases.

Annex III: Amendments to Regulation (EU) 2018/1240 (ETIAS)

Amendment 1

Revision of Article 3(1): Definitions

'other EU information systems' means the Entry/Exist System ('EES'), the Visa Information System ('VIS'), the Schengen Information System ('SIS') and the European Criminal Record Information System – Third Country Nationals ('ECRIS-TCN').

Comments: This amendment aims at adding ECRIS-TCN among the EU information systems which the ETIAS National and Central Units shall be able to consult.

Amendment 2

Revision of Article 4: Objectives of ETIAS

Current wording	Proposed amendment
By supporting the competent authorities of the Member States, ETIAS shall: (a) contribute to a high level of security by providing for a thorough security risk assessment of applicants, prior to their arrival at external border crossing points, in order to determine whether there are factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security risk; (b) contribute to the prevention of illegal immigration by providing for an illegal immigration risk assessment of applicants prior to their arrival at external border crossing points; © contribute to the protection of public health by providing for an assessment of whether the applicant poses a high epidemic risk within the meaning of point 8 of Article 3(1) prior to his or her arrival at external border crossing points; (d) enhance the effectiveness of border checks; (e) support the objectives of SIS related to alerts on third-country nationals subject to a refusal of entry and stay, alerts on persons wanted for arrest for surrender purposes or extradition purposes, alerts on missing persons, alerts on persons sought to assist with a judicial procedure and alerts on persons for discreet checks or specific checks;	(h) support the objectives of the EES.[225]

[225] A further objective under (g) was added with Regulation 2019/817 on interoperability.

(f) contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences.	

Comments: In essence, ETIAS subsumes the purposes of EES.

Amendment 3

Revision of Article 6(3): Establishment and technical architecture of the ETIAS Information System

Current wording	Proposed amendment
The ETIAS Central System, the NUIs, the web service, the carrier gateway and the communication infrastructure of ETIAS shall to the extent technically possible share and re-use the hardware and software components of the EES Central System, of the EES National Uniform Interfaces, of the EES web service and of the EES Communication Infrastructure referred to in Regulation (EU) 2017/2226.	In particular, the ETIAS Central System shall build upon the EES Central System hardware and software components in order to establish a shared identity repository for the storage of the identity alphanumeric data of both ETIAS applicants and third-country nationals registered in EES. The identity alphanumeric data of ETIAS applicants stored in the shared identity repository shall form part of the ETIAS Central System. [This shared identity repository shall be the basis for the implementation of the Common Identity Repository ('CIR') established by Regulation Interoperability.] This is without prejudice to keeping the EES and ETIAS data logically separated and subject to access as defined in the regulations establishing the respective information systems.

Comments: This amendment is meant to assist interoperability among EU information systems. The forthcoming ETIAS and EES shall be built as a common database with some data being separate from one another.

Amendment 4

Revision of Article 11: Interoperability with other EU information systems and Europol data

Current wording	Proposed wording
1. Interoperability between the ETIAS Information System, other EU information systems and Europol data shall be established to enable the verification referred to in Article 20. 2. The amendments to the legal acts establishing the EU information systems that are necessary for establishing their interoperability with ETIAS as well as the addition of corresponding provisions in this Regulation shall be the subject of a separate legal instrument.	Interoperability between the ETIAS Information System, other EU information systems and Europol data shall be established to enable the automated processing referred to in Articles 20, 23, Article 24(6)(c)(ii), Article 41 and Article 54(1)(b). [Interoperability shall rely on the European Search Portal ('ESP'), established by Article 6 of Regulation (EU) 2018/XXX (interoperability). During a transitional period, before the ESP is available, the automated processing shall rely on a tool developed by eu-LISA for the purpose of this paragraph. This tool shall be used as the basis for the development and implementation of the ESP, in accordance with Article 52 of that Regulation]. 1. For the purpose of proceeding to the verifications referred to in Article 20(2)(i), the automated processing referred to in Article 11(1), shall enable the ETIAS Central

System to query the VIS, established by Regulation (EC) 767/2008 of the European Parliament and of the Council, with the following data of Articles 17(2)(a), (ab), (c) and (d) of this Regulation: (a) surname (family name); (b) surname at birth; (c) first name(s) (given name(s)); (d) date of birth; (e) place of birth; (f) country of birth; (g) sex; (h) current nationality; (i) other nationalities (if any); (j) type, number, the country of issue of the travel document.

3. For the purpose of proceeding to the verifications referred to in Article 20(2)(g) and (h), the automated processing referred to in Article 11(1), shall enable the ETIAS Central System to query the EES, established by Regulation (EU) 2017/2226, with the following data of Article 17(2)(a) to (d): (a) surname (family name); (b) surname at birth; (c) first name(s) (given name(s)); (d) date of birth; (e) sex; (f) current nationality; (g) other names (alias(es); (h) artistic name(s); (i) usual name(s)); (j) other nationalities (if any); (k) type, number, the country of issue of the travel document.

4. For the purpose of proceeding to the verifications referred to in Article 20(2)(c), (m)(ii) and (o), and Article 23(1), the automated processing referred to in Article 11(1), shall enable the ETIAS Central System to query the SIS established by Regulation (EU) 2018/1860 (border checks) with the following data of Articles 17(2)(a) to (d) and Article 17(2)(k): (a) surname (family name); (b) surname at birth; (c) first name(s) (given name(s)); (d) date of birth; (e) place of birth; (f) sex; (g) current nationality; (h) other names (alias(es); (i) artistic name(s); (j) usual name(s)); (k) other nationalities (if any); (l) type, number, the country of issue of the travel document; (m) for minors, surname and first name(s) of applicant's parental authority or legal guardian.

5. For the purpose of proceeding to the verifications referred to in Article 20(2)(a), (d) and (m)(i) and Article 23(1), the automated processing referred to in Article 11(1), shall enable the ETIAS Central System to query the SIS established by Regulation (EU) 2018/1862 (police), with the following data of Articles 17(2)(a) to (d) and Article 17(2)(k): (a) surname (family name); (b) surname at birth; (c) first name(s) (given name(s)); (d) date of birth; (e) place of birth; (f) sex; (g) current nationality; (h) other names (alias(es); (i) artistic name(s); (j) usual name(s)); (k) other nationalities (if any); (l) type, number, the country of issue of the travel document; (m) for minors, surname and first name(s) of applicant's parental authority or legal guardian.

6. For the purpose of proceeding to the verifications referred to in Article 20(2)(n), the automated processing referred to in Article 11(1), shall enable the ETIAS Central System to query the ECRIS-TCN data [in the CIR] established by [Regulation (EU) 2018/XXX], with the following data of Article 17(2)(a) to (d): (a) surname (family name); (b) surname at birth; (c) first name(s) (given name(s)); (d) date of birth; (e) place of birth; (f) sex; (g) current nationality; (h) other names (alias(es); (i) artistic name(s); (j) usual name(s)); (k) other nationalities (if any); (l) type, number, the country of issue of the travel document.

7. For the purpose of proceeding to the verifications referred to in Article 20(2)(j), the automated processing referred to in Article 11(1) shall enable the ETIAS Central System to query

	the Europol data, with the information of Article 17(2) as listed in Article 20(2) of this Regulation. 8. Where hits are identified, the tool referred to in Article 11, shall make temporarily available the results in the application file to the ETIAS Central Unit, until the end of the manual process pursuant to Article 22(2) and Article 23(2). Where the data made available correspond to those of the applicant or where doubts remain, the unique ID code of the data having triggered a hit shall be kept in the application file. Where hits are identified, pursuant to this paragraph, the automated processing shall receive the appropriate notification in accordance with Article 21(1a) of Regulation (EU) 2016/794. 9. A hit shall be triggered where all or some of the data from the ETIAS application file used for the query correspond fully or partially to the data present in a record, alert or file of the other EU information systems consulted. The Commission shall, by means of an implementing act, define partial correspondence, including a degree of probability. 10. For the purpose of paragraph 1, the Commission, shall, by means of an implementing act, define the technical modalities for the implementation of Article 24(6)(c)(ii) and Article 54(1)(b) related to data retention. 11. For the purpose of Article 25(2), Article 28(8) and Article 29(9) when registering the data related to hits into the ETIAS application file, the origin of the data shall be indicated. This shall include the type of the alert, except for alerts referred to in Article 23(1), the source of the data (which other EU information systems or Europol data), the unique identification number used in the source of the data having triggered the hit and the Member State that entered or supplied the data having triggered the hit and, where available, the date and time when the data was entered in the other EU information systems or Europol data.

Comments: This amendment is necessary in order to ensure interoperability with EU information systems. It lays down the data on the basis of which comparison between ETIAS application files against data in EU information systems will take place.

Amendment 5

New Article 11A: Support of the objectives of the EES

For the purpose of Articles 6, 14 and 17 of Regulation (EU) 2017/2226, an automated process, using the secure communication infrastructure of Article 6(2)(d) of this Regulation, shall query and import from the ETIAS Central System, the information referred to in Article 47(2) of this Regulation, as well as the application number and the end of validity period of an ETIAS travel authorisation, and update the entry/exit record in the EES accordingly.

Comments: New data inserted in the EES on the basis of Article 47(2): (a) whether or not the person has a valid travel authorisation, and in the case of a travel authorisation with limited territorial validity issued under Article 44, the Member State(s) for which it is valid; (b) any flag attached to the travel authorisation under Article 36(2) and ((c) whether the travel authorisation will expire within the next 90 days and the remaining validity period; (d) the data referred to in points (k) and (l) of

Article 17(2). These are: (k) for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian; (l) where he or she claims the status of family member referred to in point (c) of Article 2(1): (i) his or her status of family member; (ii) the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties; (iii) his or her family ties with that family member in accordance with Article 2(2) of Directive 2004/38/EC.

Amendment 6

Revision of Article 12(1): Querying the Interpol databases

Current wording	Proposed amendment
The ETIAS Central System shall query the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (TDAWN). Any queries and verification shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.	Addition of a second paragraph that reads: For the purpose of paragraph 1, a cooperation agreement is to be agreed upon between the European Union and INTERPOL. This cooperation agreement shall provide for the modalities for the exchange of information and safeguards for the protection of personal data.

Amendment 7

Revision of Article 20(2): Automated processing

Current wording	Proposed amendment
2. The ETIAS Central System shall compare the relevant data referred to in points (a),(b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in a record, file or alert registered in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol SLTD and TDAWN databases. In particular, the ETIAS Central System shall verify: (a) whether the travel document used for the application corresponds to a travel document reported lost, stolen, misappropriated or invalidated in SIS; (b) whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD; (c) whether the applicant is subject to a refusal of entry and stay alert entered in SIS; (d) whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS; (e) whether the applicant and the travel document correspond to a refused, revoked or annulled travel authorisation in the ETIAS Central System;	Addition of element under (n) which reads: whether the applicant corresponds to a person whose data is recorded in the ECRIS-TCN for terrorists offences and other serious criminal offences.

(f) whether the data provided in the application concerning the travel document correspond to another application for travel authorisation associated with different identity data referred to in point (a) of Article 17(2) in the ETIAS Central System; (g) whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES; (h) whether the applicant is recorded as having been refused entry in the EES; (i) whether the applicant has been subject to a decision to refuse, annul or revoke a short stay visa recorded in VIS; (j) whether the data provided in the application correspond to data recorded in Europol data; (k) whether the applicant is registered in Eurodac; (l) whether the travel document used for the application corresponds to a travel document recorded in a file in TDAWN; (m) in cases where the applicant is a minor, whether the applicant's parental authority or legal guardian: (i) is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS; (ii) is subject to a refusal of entry and stay alert entered in SIS.	

Comments: This amendment serves to add a query in ECRIS-TCN for the purposes of ETIAS automated processing.

Amendment 8

New Article 22: Verification by the ETIAS Central Unit

Current wording	Proposed amendment
1. Where the automated processing pursuant to Article 20(2) to (5) reports one or several hits the ETIAS Central System shall automatically consult the ETIAS Central Unit. 2. When consulted, the ETIAS Central Unit shall have access to the application file and any linked application files, as well as to all the hits triggered during automated processing pursuant to Article 20(2) to (5) and to the information identified by the ETIAS Central System under Article 20(7) and (8). 3. The ETIAS Central Unit shall verify whether the data recorded in the application file correspond to one or more of the following: (a) the specific risk indicators referred to in Article 33; (b) the data present in the ETIAS Central System,	7. The ETIAS Information System shall keep records of all data processing operations carried out for assessments under paragraphs 1 to 6 by the ETIAS Central Unit. Those records shall be created and entered automatically in the application file. They shall show the date and time of each operation, the data linked to the hit received, the staff member having performed the manual processing under paragraphs 1 to 6 and the outcome of the verification and the corresponding justification.

including the ETIAS watchlist referred to in Article 34; (c) the data present in one of the EU information systems that are consulted; (d) Europol data; (e) the data present in the Interpol SLTD or TDAWN databases. 4. Where the data do not correspond, and no other hit has been reported during automated processing pursuant to Article 20(2) to (5), the ETIAS Central Unit shall delete the false hit from the application file and the ETIAS Central System shall automatically issue a travel authorisation in accordance with Article 36. 5. Where the data correspond to those of the applicant or where doubts remain concerning the identity of the applicant, the application shall be processed manually in accordance with the procedure laid down in Article 26. 6. The ETIAS Central Unit shall complete the manual processing within a maximum of 12 hours from receipt of the application file.	

Amendment 9

Revision of Article 23: Support of the objectives of SIS

Current wording	Proposed amendment
1. For the purposes of point (e) of Article 4, the ETIAS Central System shall compare the relevant data referred to in points (a), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts: (a) an alert on missing persons; (b) an alert on persons sought to assist with a judicial procedure; (c) an alert on persons for discreet checks or specific checks. 2. Where the comparison referred to in paragraph 1 reports one or several hits, the ETIAS Central System shall send an automated notification to the ETIAS Central Unit. The ETIAS Central Unit shall verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered that hit and if a correspondence is confirmed, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that entered the alert. The SIRENE Bureau concerned shall further verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered the hit and take any appropriate follow-up action. The ETIAS Central System shall also send an automated notification to the SIRENE Bureau of the Member State that entered the alert having triggered a hit against SIS during the automated processing referred to in Article 20 where, following verification	1. For the purposes of point (e) of Article 4, the ETIAS Central System shall compare the relevant data referred to in points (a), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts: (a) an alert on missing persons; (b) an alert on persons sought to assist with a judicial procedure; (c) an alert on persons for discreet checks, **inquiry checks** or specific checks. 2. Where the comparison referred to in paragraph 1 reports one or several hits, the ETIAS Central System shall send an automated notification to the ETIAS Central Unit. **When notified, the ETIAS Central Unit shall have access to the application file and any linked application files**, in order to verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered that hit and if a correspondence is confirmed, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that entered the alert. The SIRENE Bureau concerned shall further verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered the hit and take any appropriate follow-up action. The ETIAS Central System shall also send an automated notification to the SIRENE Bureau of the Member State that entered the alert having triggered a hit against SIS during the automated processing referred to in Article 20 where, following verification by the ETIAS Central Unit as referred to

by the ETIAS Central Unit as referred to in Article 22, that alert has led to manual processing of the application in accordance with Article 26. 3. The notification provided to the SIRENE Bureau of the Member State that entered the alert shall contain the following data: (a) surname(s), first name(s) and, if any, alias(es); (b) place and date of birth; (c) sex; (d) nationality and, if any, other nationalities; (e) Member State of first intended stay, and if available, the address of first intended stay; (f) the applicant's home address or, if not available, his or her city and country of residence; (g) travel authorisation status information, indicating whether a travel authorisation has been issued, refused or whether the application is subject to manual processing pursuant to Article 26; (h) a reference to any hits obtained in accordance with paragraphs 1 and 2, including the date and time of the hit. 4. The ETIAS Central System shall add a reference to any hit obtained pursuant to paragraph 1 to the application file.	in Article 22, that alert has led to manual processing of the application in accordance with Article 26. 3. The notification provided to the SIRENE Bureau of the Member State that entered the alert shall contain the following data: (a) surname(s), first name(s) and, if any, alias(es); (b) place and date of birth; (c) sex; (d) nationality and, if any, other nationalities; (e) Member State of first intended stay, and if available, the address of first intended stay; (f) the applicant's home address or, if not available, his or her city and country of residence; (g) travel authorisation status information, indicating whether a travel authorisation has been issued, refused or whether the application is subject to manual processing pursuant to Article 26; (h) a reference to any hits obtained in accordance with paragraphs 1 and 2, including the date and time of the hit. 4. The ETIAS Central System shall add a reference to any hit obtained pursuant to paragraph 1 to the application file. 5. The ETIAS Information System shall keep records of all data processing operations carried out for assessments under paragraphs 1 to 4 by the ETIAS Central Unit. Those records shall be created and entered automatically in the application file. They shall show the date and time of each operation, the data linked to the hit received, the staff member of the Central Unit having performed the manual processing under paragraphs 1 to 4, the outcome of the verification and the corresponding justification.

Comments: The proposed amendment is threefold: 1) it adds inquiry checks; 2) it clarifies that the ETIAS Central Unit shall have access to SIS; 3) it adds the requirement to keep logs.

Amendment 10

New Article 25a: Use of other EU information systems for the manual processing of application by the ETIAS National Unit

1. Without prejudice to Article 13(1) of this Regulation, ETIAS National Units shall have a direct access to and may consult, in a read-only format, the other EU information systems for examining applications for travel authorisation and adopting decisions relating to those applications in accordance with Article 26 of this Regulation. The ETIAS National Units may consult the data referred to in the following provisions:

(a) Articles 16 to 18 of Regulation (EU) 2017/2226;

(b) Articles 9 to 14 of the Regulation (EC) No 767/2008;

(c) Articles 24 and 25 of the SIS Regulation (EU) No 2018/1861 (Border checks);

(d) Articles 26, 32, 34, 36 and Article 38(2)(k) and (l), of the SIS Regulation (EU) No 2018/1862 (Police);

2. The ETIAS National Units shall also have access to the national criminal records registers in order to obtain the information on third country national and stateless persons convicted for a terrorist offence or other serious criminal offence for the purposes referred to in paragraph 1.

Comments: This amendment gives direct access rights to the ETIAS National Units on a read-only format.

Amendment 11

Revision of Article 26(3): Manual processing of applications by the ETIAS National Units

Current wording	Proposed amendment
3. Where the automated processing laid down in Article 20(2) has reported a hit, the ETIAS National Unit of the Member State responsible shall: (a) refuse a travel authorisation where the hit corresponds to one or several of the verifications referred to in points (a) and (c) of Article 20(2); (b) assess the security or illegal immigration risk and decide whether to issue or refuse a travel authorisation where the hit corresponds to any of the verifications referred to in points (b) and (d) to (m) of Article 20(2).	(b) assess the security or illegal immigration risk and decide whether to issue or refuse a travel authorisation where the hit corresponds to any of the verifications referred to in point (b) and points (d) to (n) of Article 20(2).

Com**ments:** This amendment is linked to the ECRIS-TCN.

Amendment 12

Revision of Article 41(3): Revocation of a travel authorisation

Current wording	Proposed amendment
Without prejudice to paragraph 2, where a new alert is issued in SIS concerning **a new** refusal of entry and stay or concerning a travel document reported as lost, stolen, misappropriated or invalidated, SIS shall inform the ETIAS Central System. The ETIAS Central System shall verify whether this new alert corresponds to a valid travel authorisation. Where this is the case, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having entered the alert. Where a new alert for refusal of entry and stay has been issued, the ETIAS National Unit shall revoke the travel authorisation. Where the travel authorisation is linked to a travel document reported as lost, stolen, misappropriated or invalidated in SIS or SLTD, the ETIAS National Unit shall manually process the application file.	Without prejudice to paragraph 2, where a new alert is issued in SIS concerning refusal of entry and stay, or concerning a travel document reported as lost, stolen, misappropriated or invalidated, SIS shall inform the ETIAS Central System. The ETIAS Central System shall verify whether this new alert corresponds to a valid travel authorisation. Where this is the case, the ETIAS Central System shall transfer the application file to the ETIAS National Unit of the Member State having entered the alert. Where a new alert for refusal of entry and stay has been issued, the ETIAS National Unit shall revoke the travel authorisation. Where the travel authorisation is linked to a travel document reported as lost, stolen, misappropriated or invalidated in SIS or SLTD, the ETIAS National Unit shall manually process the application file.

Comments: This amendment involves a small change in Article 41(3) (deletion of 'a new') according to which it will not necessary for SIS to hold a new alert in respect of a third-country national to revoke the travel authorisation. This means that a revocation may be based on the fact that a third-country national was issued with an alert for the first time after the issuance of an ETIAS authorisation. The current wording of the ETIAS Regulation seems to suggest that the provision only involves cases where the individual has already been issued an alert, but a travel authorisation would have nonetheless been granted.

Amendment 13

Revision of Article 88 – Start of operations

Current wording	Proposed amendment
1. The Commission shall determine the date from which ETIAS is to start operations once the following conditions have been met:	1. The Commission shall determine the date from which ETIAS is to start operations once the following conditions have been met:
(a) the necessary amendments to the legal acts establishing the EU information systems referred to in Article 11(2) with which interoperability shall be established with the ETIAS Information System have entered into force;	(a) the necessary amendments to the legal acts establishing the EU information systems referred to in **Article 11 with which interoperability, in the meaning of Article 11 of this Regulation, shall be established with the ETIAS Information System have entered into force, with the exception of the Eurodac recast.**
(b) the Regulation entrusting eu-LISA with the operational management of ETIAS has entered into force;	(b) the Regulation entrusting eu-LISA with the operational management of ETIAS has entered into force;
(c) the necessary amendments to the legal acts establishing the EU information systems referred to in Article 20(2) providing for an access to these databases for the ETIAS Central Unit have entered into force;	(c) the necessary amendments to the legal acts establishing the EU information systems referred to in Article 20(2) providing for an access to these databases for the ETIAS Central Unit have entered into force;
(d) the measures referred to in Article 15(5), Article 17(3), (5) and (6), Article 18(4), Article 27(3) and (5), Article 33(2) and (3), Articles 36(3), 38(3), 39(2), 45(3), 46(4), 48(4), 59(4), Article 73(3)(b), Article 83(1), (3), and (4) and Article 85(3) have been adopted;	**(d)** the measures referred to in **Article 11(8), Article 11(9),** Article 15(5), Article 17(3), (5) and (6), Article 18(4), Article 27(3) and (5), Article 33(2) and (3), Article 36(3), Article 38(3), Article 39(2), Article 45(3), Article 46(4), Article 48(4), Article 59(4), Article 73(3)(b), Article 83(1), (3), and (4) and Article 85(3) have been adopted;
(e) eu-LISA has declared the successful completion of a comprehensive test of ETIAS;	(e) eu-LISA has declared the successful completion of a comprehensive test of ETIAS;
(f) eu-LISA and the ETIAS Central Unit have validated the technical and legal arrangements to collect and transmit the data referred to in Article 17 to the ETIAS Central System and have notified them to the Commission;	(f) eu-LISA and the ETIAS Central Unit have validated the technical and legal arrangements to collect and transmit the data referred to in Article 17 to the ETIAS Central System and have notified them to the Commission;
(g) the Member States and the ETIAS Central Unit have notified to the Commission the data concerning the various authorities referred to in Article 87(1) and (3).	(g) the Member States and the ETIAS Central Unit have notified to the Commission the data concerning the various authorities referred to in Article 87(1) and (3).
2. The test of ETIAS referred to in point (e) of paragraph 1 shall be conducted by eu-LISA in cooperation with the Member States and the ETIAS Central Unit.	2. The test of ETIAS referred to in point (e) of paragraph 1 shall be conducted by eu-LISA in cooperation with the Member States and the ETIAS Central Unit.
3. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to point (e) of paragraph 1.	3. The Commission shall inform the European Parliament and the Council of the results of the test carried out pursuant to point (e) of paragraph 1.
4. The Commission decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.	4. The Commission decision referred to in paragraph 1 shall be published in the *Official Journal of the European Union*.
5. The Member States and the ETIAS Central Unit shall start using ETIAS from the date determined by the Commission in accordance with paragraph 1.	5. The Member States and the ETIAS Central Unit shall start using ETIAS from the date determined by the Commission in accordance with paragraph 1.
	6. The interoperability, referred to in Article 11, with ECRIS-TCN shall start when [the CIR] enters into operations, which is scheduled in 2022. ETIAS' operations

	shall start irrespective of whether that interoperability with ECRIS- TCN is put in place. **7. ETIAS shall start its operations irrespective of whether a cooperation agreement between the European Union and INTERPOL as referred to in Article 12(2) has been concluded and irrespective of whether it is possible to query Interpol's databases.**

Comments: Eurodac is exempted and Articles 11(8) and (9) were added. With regards to ECRIS-TCN it is clarified that ETIAS will operate irrespective of whether interoperability with ECRIS-TCN is in place or whether the cooperation agreement with Interpol has been concluded.

Amendment 14

Revision of Article 96 second paragraph: Entry into force and applicability

Current wording	Proposed amendment
This Regulation shall apply from the date determined by the Commission in accordance with Article 88, with the exception of Articles 6, 11, 12, 33, 34, 35, 59, 71, 72, 73, Articles 75 to 79, Articles 82, 85, 87, 89, 90, 91, Article 92(1) and (2), Articles 93 and 95, as well as the provisions related to the measures referred to in point (d) of Article 88(1), which shall apply from 9 October 2018.	This Regulation shall apply from the date determined by the Commission in accordance with Article 88, with the exception of Articles 6, 11, **11a**, 12, 33, 34, 35, 59, 71, 72, 73, Articles 75 to 79, Articles 82, 85, 87, 89, 90, 91, Article 92(1) and (2), Articles 93 and 95, as well as the provisions related to the measures referred to in point (d) of Article 88(1), which shall apply from 9 October 2018.

Comments: This amendment adds Article 11a.

Annex IV: Amendments to Regulation 787/2008 (VIS)

Amendment 1

Revision of Article 6(2): Access for entering, amending, deleting and consulting data

Current wording	Proposed amendment
Access to the VIS for consulting the data shall be reserved exclusively to the duly authorised staff of the authorities of each Member State which are competent for the purposes laid down in Articles 15 to 22, limited to the extent that the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued.	Access to the VIS for consulting the data shall be reserved exclusively to the duly authorised staff of the authorities of each Member State, **including to duly authorised staff of the ETIAS National Units, designated pursuant to Article 8 of Regulation (EU) 2018/1240 of the European Parliament and of the Council**, which are competent for the purposes laid down in Articles 15 to 22, **and for the duly authorised staff of the national authorities of each Member States and of the EU bodies which are competent for the purposes laid down in [Article 20 and Article 21 of the Regulation 2018/xx on interoperability] limited to the extent that the data are required for the performance of their tasks in accordance with those purposes, and proportionate to the objectives pursued.**

Comments: This amendment increases access to the ETIAS National System and other national authorities designated under Articles 20 and 21 of the Interoperability Regulations.

Amendment 2

New Articles 18b, c and d: Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240 / Access to data from VIS by the ETIAS Central Unit / Use of VIS for the manual processing by ETIAS National Units

Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240
1. From the start of operations of ETIAS, as provided for in Article 88(1) of Regulation (EU) 2018/1240, the 'CS-VIS' shall be connected to the tool referred to in Article 11 of Regulation (EU) 2018/1240 to enable the automated processing referred to in that Article.
2. The automated processing referred to in Article 11 of Regulation (EU) 2018/1240 shall enable the verifications provided for in Article 20 of that Regulation and the subsequent verifications of Articles 22 and 26 of that Regulation.
For the purpose of proceeding to the verifications point (i) of Article 20(2) of Regulation (EU) 2018/1240, the ETIAS Central System shall use the tool referred to in Article 11 of that Regulation to compare the data in ETIAS with the data in the VIS, in accordance with Article 11(8) of that Regulation, using the correspondences listed in the table in annex II.
Access to data from VIS by the ETIAS Central Unit
1. The ETIAS Central Unit, established within the European Border and Coast Guard Agency in accordance with Article 7 of Regulation (EU) 2018/1240, shall have, for the purpose of performing its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search relevant data in VIS in accordance with Article 11(8) of that Regulation.

2. Where a verification by the ETIAS Central Unit confirms the correspondence between data recorded in the ETIAS application file and data in the EES or where doubts remain, the procedure set out in Article 26 of Regulation (EU) 2018/1240 applies, without prejudice to Article 24 of Regulation (EU) 2018/1240.

Use of VIS for the manual processing by ETIAS National Units

1. Consultation of VIS by ETIAS National Units shall be done using the same alphanumerical data as those used for the automated processing referred to in Article 18b(2).
2. The ETIAS National Units, designated pursuant to Article 8(1) of Regulation (EU) 2018/1240, shall have access to and may consult VIS, in a read-only format, for the purpose of examining applications for travel authorisation pursuant to Article 8(2) of that Regulation. The ETIAS National Units may consult the data referred to in Articles 9 to 14 of this Regulation.
3. 3. Following an access pursuant to paragraph 1, duly authorised staff of the ETIAS National Units shall only record the result of the assessment and shall record this result in the ETIAS application files.

Comments: The article enables interoperability and allows ETIAS Central and National Units to access VIS data.

Amendment 3

New Article 34a: Keeping of logs

For the consultations listed in Article 18b of this Regulation, a log of each data processing operation carried out within VIS and ETIAS shall be kept in accordance with Article 34 of this Regulation and Article 69 of Regulation (EU) No 2018/1240.

Amendment 4

New Annex II: Table of correspondences referred to in Article 18b

Data of Article 17(2) of Regulation 2018/1240 sent by ETIAS Central System	**The VIS corresponding data of Article 9(4) of this Regulation against which the ETIAS data should be checked**
surname (family name)	surnames
surname at birth	surnames at birth (former surname(s))
first name(s) (given name(s))	first name(s)
date of birth	date of birth
place of birth	place of birth
country of birth	country of birth
sex	Sex
current nationality	current nationality and nationality at birth
other nationalities (if any)	current nationality and nationality at birth
type of the travel document	type of the travel document
number of the travel document	number of the travel document
country of issue of the travel document	the authority which issued the travel document

Comments: A number of discrepancies exist between the categories of personal data processed under the ETIAS and VIS Regulations, however, the correspondence does not present issues. The categories of data which can be queried are not more extensive than the ones gathered by ETIAS.

Annex V: Amendments to Regulation (EU) 2017/2226 (EES)

Amendment 1

Revision of Article 6(1): Objectives of the EES

Current wording	Proposed amendment
By recording and storing data in the EES and by providing Member States with access to such data, the objectives of the EES shall be to: (a) enhance the efficiency of border checks by calculating and monitoring the duration of the authorised stay on the entry and exit of third-country nationals admitted for a short stay; (b) assist in the identification of third-country nationals who do not or no longer fulfil the conditions for entry to, or for short stay on, the territory of the Member States; (c) allow the identification and detection of overstayers and enable the competent national authorities of the Member States to take appropriate measures; (d) allow refusals of entry in the EES to be checked electronically; (e) enable automation of border checks on third-country nationals; (f) enable visa authorities to have access to information on the lawful use of previous visas; (g) inform third-country nationals of the duration of their authorised stay; (h) gather statistics on the entries and exits, refusals of entry and overstays of third-country nationals in order to improve the assessment of the risk of overstays and support evidence-based Union migration policy making; (i) combat identity fraud and the misuse of travel documents.	**Addition of element under (k) which reads:** support the objectives of ETIAS established by Regulation (EU) 2018/1240 of the European Parliament and of the Council.

Comments: This amendment includes the objectives of ETIAS within the objectives of EES.

Amendment 2

New Articles 8a and b: Automated process with ETIAS / Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240

Automated process with ETIAS

An automated process, using the secure communication infrastructure of Article 6(2)(d) of Regulation (EU) 2018/1240, shall enable the EES to create or update the entry/exit record or the refusal of entry record of a visa exempt third country national in the EES in accordance with Articles 14 and 17 of this Regulation.

Where an entry/exit record of a visa exempt third country national is created, the automated process shall enable the Central System of the EES the following:

(a) to query and import from the ETIAS Central System the information referred to in Article 47(2) of Regulation (EU) 2018/1240, the application number and the end of validity period of an ETIAS travel authorisation;

(b) to update the entry/exit record in the EES in accordance with Article 17(2) of this Regulation.

Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240

1. From the start of operations of ETIAS, as provided for in Article 88(1) of Regulation (EU) 2018/1240, the Central System of the EES shall be connected to the tool referred to in Article 11 of Regulation (EU) 2018/1240 to enable the automated processing referred to in that Article.

2. Without prejudice to Article 24 of Regulation (EU) 2018/1240, the automated processing referred to in Article 11 of Regulation (EU) 2018/1240 shall enable the verifications provided for in Article 20 of that Regulation and the subsequent verifications of Articles 22 and 26 of that Regulation.

For the purpose of proceeding to the verifications referred to in points (g) and (h) of Article 20(2) of Regulation (EU) 2018/1240, the ETIAS Central System shall use the tool referred to in Article 11 of that Regulation to compare the data in ETIAS with the data in the EES, in accordance with Article 11(8) of that Regulation, using the correspondences listed in the table in annex III.

The verifications shall be without prejudice to the specific rules provided for in Article 24(3) of Regulation (EU) No 2018/1240.

Comments: See Amendment 5 of Annex III.

Amendment 3

Revision of Article 9: Access to the EES for entering, amending, erasing and consulting data

Current wording	Proposed amendment
Access to the EES for entering, amending, erasing and consulting the data referred to in Article 14 and Articles 16 to 20 shall be reserved exclusively for the duly authorised staff of the national authorities of each Member State which are competent for the purposes laid down in Articles 23 to 35. That access shall be limited to the extent necessary for the performance of the tasks of those national authorities in accordance with those purposes and shall be proportionate to the objectives pursued. 2. Each Member State shall designate the competent national authorities which shall be border authorities, visa authorities and immigration authorities for the purposes of this Regulation. The duly authorised staff of the competent national authorities shall have access to the EES to enter, amend, erase or consult data. Each Member State shall communicate a list of those competent national authorities to eu-LISA without delay. That list shall specify for which purpose each authority is to have access to the data stored in the EES. 3. The authorities entitled to consult or access the EES data in order to prevent, detect and investigate terrorist offences or other serious criminal offences shall be designated in accordance with Chapter IV.	Addition of paragraph 2a which reads: The duly authorised staff of the ETIAS National Units, designated pursuant to Article 8 of Regulation (EU) 2018/1240, shall have access to the EES to consult data in a read-only format.

Comments: This amendment allows access to EES by ETIAS Nationals Units on read-only format.

Amendment 4

Revision of Article 17(2): Personal data of visa-exempt third-country nationals

Current wording	Proposed amendment
For visa-exempt third-country nationals, points (a), (b) and (c) of Article 16(2), points (a) and (b) of Article 16(3) and Article 16(4) shall apply *mutatis mutandis*.	Addition of sub-paragraph which reads: The following data shall also be entered in the entry/exit record: (a) the application number; (b) the end of validity period of an ETIAS travel authorisation; (c) in case of a travel authorisation with limited territorial validity, the Member State(s) for which it is valid.

Comments: See Amendment 5 of Annex III.

Amendment 5

New Articles 25a and b: Access to data from the EES by the ETIAS Central Unit / Use of the EES for the manual processing by ETIAS National Units

Access to data from the EES by the ETIAS Central Unit 1, The ETIAS Central Unit, established within the European Border and Coast Guard Agency in accordance with Article 7 of Regulation (EU) 2018/1240, shall have, for the purpose of performing its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search data in the EES in accordance with Article 11(8) of that Regulation. 2. Where a verification by the ETIAS Central Unit confirms the correspondence between data recorded in the ETIAS application file and data in the EES or where doubts remain, the procedure set out in Article 26 of Regulation (EU) 2018/1240 applies.
Use of the EES for the manual processing by ETIAS National Units 1. Consultation of EES by ETIAS National Units referred to in Article 8(1) of Regulation (EU) 2018/1240 shall be done using the same alphanumerical data as those used for the automated processing referred to in Article 8b(2) of this Regulation. 2. The ETIAS National Units shall have access to and may consult the EES, in a read- only format, for the purpose of examining applications for travel authorisation, pursuant to Article 8(2) of that Regulation. The ETIAS National Units may consult the data referred to in Articles 16 to 18 of this Regulation, without prejudice to Article 24 of Regulation (EU) 2018/1240. 3. Following an access pursuant to paragraph 1, duly authorised staff of the ETIAS National Units shall record only the result of the assessment and shall record this result in the ETIAS application files.

Comments: Access by the ETIAS Central and Nationals Units.

Amendment 6

Revision of Article 28: Keeping of data retrieved from the EES

Current wording	Proposed amendment
Data retrieved from the EES pursuant to this Chapter may be kept in national files only where necessary in an individual case, in accordance with the purpose for which they were retrieved and with relevant Union law, in particular on data protection, and for no longer than strictly necessary in that individual case.	Data retrieved from the EES pursuant to Articles 24, 25, 26 and 27 may be kept in national files and data retrieved from the EES pursuant to Article 25a may be kept in the ETIAS application files only where necessary in an individual case, in accordance with the purpose for which they were retrieved and with relevant Union law, in particular on data protection, and for no longer than strictly necessary in that individual case.

Amendment 7

New Article 46(2): Keeping of logs by eu-LISA and Member States

Current wording	Proposed amendment
For the consultations listed in Article 8, a log of each data processing operation carried out within the EES and the VIS shall be kept in accordance with this Article and Article 34 of Regulation (EC) No 767/2008. eu-LISA shall ensure, in particular, that the relevant log of the concerned data processing operations is kept when the competent authorities launch a data processing operation directly from one system to the other.	Addition of second subparagraph that reads: For the consultations listed in Articles 8a, 8b and 25a of this Regulation, a log of each data processing operation carried out within the EES and ETIAS shall be kept in accordance with this Article and Article 69 of Regulation (EU) No 2018/1240.

Amendment 8

New Annex III: Table of correspondences referred to in Article 8b

Data of Article 17(2) of Regulation 2018/1240 sent by ETIAS Central System	**The EES corresponding data of Article 17(1)(a) of this Regulation against which the ETIAS data should be checked**
surname (family name)	surnames
surname at birth	surnames
first name(s) (given name(s))	first name or names (given names)
other names (alias(es), artistic name(s), usual name(s))	first name or names (given names)
date of birth	date of birth
sex	sex
current nationality	nationality or nationalities
other nationalities (if any)	nationality or nationalities
type of the travel document	type of the travel document
number of the travel document	number of the travel document
country of issue of the travel document	the three letter code of the issuing country of the travel document

Comments: This amendment is meant to align the categories of data to be consulted. The table does not show any issues with collection of additional personal data.

Annex VI: Amendments to Regulation (EU) 2018/1862 (SIS – border checks branch)

Amendment 1

New Article 18a: Keeping of logs

Keeping of logs for the purpose of the interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240 Logs of each data processing operation carried out within SIS and ETIAS pursuant to Article 36a and 36b shall be kept in accordance with Article 18 of this Regulation and Article 69 of Regulation (EU) No 2018/1240 of the European Parliament and of the Council.

Amendment 2

Revision of Article 34(1): National competent authorities having a right of access to SIS

Current wording	Proposed amendment
National competent authorities having a right to access data in SIS 1. National competent authorities responsible for the identification of third-country nationals shall have access to data entered in SIS and the right to search such data directly or in a copy of the SIS database for the purposes of: (a) border control, in accordance with Regulation (EU) 2016/399; (b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities; (c) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies; (d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third-country nationals who are illegally entering or staying on the territory of the Member States; (e) security checks on third-country nationals who apply for international protection, insofar as authorities performing the checks are not 'determining authorities' as defined in point (f) of Article 2 of Directive 2013/32/EU of the European	Addition of element under (g) which reads: (g) manual processing of ETIAS applications by the ETIAS National Unit, pursuant to Article 8 of Regulation (EU) 2018/1240.

Parliament and of the advice in accordance with Council Regulation (EC) No 377/2004; (f) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Regulation (EC) No 810/2009 of the European Parliament and of the Council.	

Comments: This amendment add ETIAS National Units amongst the authorities granted access to SIS.

Amendment 3

New Articles 36a and b: Access to SIS data by the ETIAS Central Unit / Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240

Access to SIS data by the ETIAS Central Unit 1. The ETIAS Central Unit, established within the European Border and Coast Guard Agency in accordance with Article 7 of Regulation (EU) 2018/1240, shall have, for the purpose of performing its tasks conferred on it by Regulation (EU) 2018/1240, the right to access and search relevant data entered in SIS. The provisions of Article 36(4)-(8) apply to this access and search. 2. Without prejudice to Article 24 of Regulation (EU) 2018/1240, where a verification by the ETIAS Central Unit confirms the correspondence of the data recorded in the ETIAS application file to an alert in SIS, the procedure set out in Article 26 of Regulation (EU) 2018/1240 applies.
Interoperability with ETIAS in the meaning of Article 11 of Regulation (EU) 2018/1240 1. From the start of operations of ETIAS, as provided for in Article 88(1) of Regulation (EU) 2018/1240, the Central System of SIS shall be connected to the tool referred to in Article 11 of Regulation (EU) 2018/1240 to enable the automated processing referred to in that Article. 2. For the purpose of proceeding to the verifications of Article 20(2)(c), (m)(ii) and (o) of Regulation (EU) 2018/1240, the ETIAS Central System shall use the tool, referred to in Article 11 of that Regulation, to compare the data referred to in Article 11(4) Regulation (EU) 2018/1240, to data in SIS, in accordance with Article 11(8) of that Regulation. 3. Where a new alert referred to in Article 41(3) of Regulation (EU) 2018/1240 is entered in SIS, the Central System shall transmit the information on this alert, using the automated processing and the tool referred to in Article 11 of that Regulation, to the ETIAS Central System, in order to verify whether this new alert corresponds to an existing travel authorisation.

Comments: These amendments enable access to SIS data by the ETIAS Central Unit and ensures interoperability between ETIAS and SIS.

On 7 January 2019, the European Commission presented two proposals for amendments to the legal instruments of the EU information systems following the adoption of Regulation 2018/1240 on the establishment of a European Travel Information and Authorisation System (ETIAS). The ETIAS Regulation requires all visa-exempt non-EU nationals to apply online for travel authorisation prior to the date of their departure. Neither the original Commission proposal for ETIAS, nor the two subsequent proposals ('the Commission package') were accompanied by Commission impact assessments.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) therefore requested a targeted substitute impact assessment of the expected fundamental rights impacts of specific elements of the Commission package.

In particular, this study assesses: 1) whether the amendments to the ECRIS-TCN Regulation provided for in the Commission package extend the scope of that information system and, if so, whether such an extension is necessary and proportionate in accordance with Article 52(1) of the EU Charter; and 2) whether the amendments regarding the automated processing of ETIAS application files through comparisons against data present in EU information systems raise concerns in relation to the rights to respect for private life and protection of personal data.

This is a publication of the Ex-ante Impact Assessment Unit
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PDF ISBN 978-92-846-6080-3 | doi:10.2861/156127 | QA-02-19-968-EN-N