EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS

ANALYSIS OF THE

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) 2019/816 [1]

AND OF THE

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 [2]

[1] COM(2019) 3 final.
[2] COM(2019) 4 final.

Table of Contents

1. Objective of this document

This analytical document aims at enabling the co-legislators to take an informed decision on the two Proposals adopted by the Commission on 7 January 2019. These two proposals are also known as the 'consequential amendments' of Regulation (EU) 2018/1240[3] which was adopted on 12 September 2018 and which establishes a European Travel Information and Authorisation System (hereinafter 'ETIAS Regulation'), namely:

- the 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) 2019/816; and
- the 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.

2. Background: the main elements of the European Travel Information and Authorisation System

In order to fully comprehend the rationale motivating the adoption of the two proposals mentioned above, it is important to understand first the main elements of the European Travel Information and Authorisation System (hereinafter 'ETIAS') established by Regulation (EU) 2018/1240. It includes the entities for processing the ETIAS applications, the objectives of ETIAS and the data that can be used.

2.1. The actors for the processing of applications for a travel authorisation

The ETIAS Regulation provides clear rules for the handling of an application for a travel authorisation. In its Articles 20, 22 and 26, the ETIAS Regulation specifies who is allowed to handle those applications and at which moment of the processing. ETIAS is a system consisting of three entities authorised to process applications for a travel authorisation:

- the ETIAS Central System;
- an ETIAS Central Unit; and
- the ETIAS National Units.

Furthermore, section 3.2.3. explains in further details how and when applications are handled by these different entities (please see below).

[3] 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 (OJ L 236, 19.9.2018, p. 1–71).

2.2. The objectives of ETIAS

ETIAS' objectives are to contribute to:

- a high level of security by providing for a thorough security risk assessment of applicants;
- the prevention of illegal immigration by providing for an illegal immigration risk assessment;
- the protection of public health by providing for an assessment of whether the applicant poses a high epidemic risk and;
- enhancing the effectiveness of border checks.

2.3. The data that can be used by ETIAS

In order to fulfil its objectives, ETIAS will support the competent Member States' authorities in their assessment of whether the presence in the territory of the Schengen Member States of a third-country national exempt from the visa-obligation would pose a security, illegal immigration or high epidemic risk.

This will be done by, amongst other things, comparing information contained in the ETIAS Information System with information contained in other EU information systems. In accordance with Article 20(2) of the ETIAS Regulation, the personal data that can be used by the ETIAS Central System for the purpose of performing that comparison are only a subset of the data submitted by the applicant in their application form. More specifically, only the data of points (a),(b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) of the ETIAS Regulation can be used.

3. Policy context

3.1. Rationale for the proposals

In order to compare the data contained in ETIAS to those contained in other EU information systems, it is necessary to:

(1) ensure interoperability between ETIAS and those other EU information system; the interoperability is indeed necessary to enable the comparisons required under Article 20 between the information in ETIAS applications with the information contained in the other EU information systems;
(2) specify the access rights to these other EU information systems by the ETIAS Central System, the ETIAS Central Unit and the ETIAS National Units; and
(3) determine in further detail which data will be exchanged between the ETIAS Central System and the other EU information systems.

However, these three elements mentioned above are missing in the ETIAS Regulation. The legislators have decided to postpone these detailed amendments and acknowledged, in Article 11(2) of the ETIAS Regulation, the need to adopt a separate legal act: "*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". That separate legal instrument is precisely the two proposals adopted by the Commission on 7 January 2019[4], referred to as the 'consequential amendments' and which are the subject of this analysis. Those 'consequential amendments' are further explained below.

Moreover, in Article 88(1) of the ETIAS Regulation, the legislator further specified the pre-conditions for ETIAS to enter into operations. Amongst those are:

- "*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*" (Article 88(1)(a));
- "*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*" (Article 88(1)(c)).

As a result of the combined reading of Articles 11 and 88 of the ETIAS Regulation, it is clear that the 'consequential amendments' should establish the interoperability and provide the ETIAS entities with the necessary access rights to the other EU information systems.

From a legal point of view, failure to do so would make it impossible for ETIAS to enter into operation, despite the fact that the system would have been developed. This is due to the fact that without a legal authorisation, ETIAS and its entities would not legally be allowed to connect, access and query the other EU information systems. In addition, from a broader legal perspective, failure to adopt the 'consequential amendments' would contradict the obligations set out in Article 11 of the ETIAS Regulation and would amount to a failure to act.

More than that, from a policy point of view, the consequences of ETIAS not entering into operations would be twofold:

- the policy objectives of ETIAS, as described in section 2.2., would not be fulfilled. More specifically, ETIAS is the only system allowing to assess, prior to their travel, whether a third-country national exempt from the visa obligation would pose a security, illegal immigration or high epidemic risk.
- the objectives defined by the Regulations (EU) 2019/817[5] and 2019/818[6] (the 'Interoperability Regulations') would not be entirely fulfilled and the framework for

[4] Ibid, footnotes 1 and 2.

[5] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 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. OJ L 135, 22.5.2019, p. 27–84.

[6] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial

interoperability between EU information systems established by these Regulations would not be complete.

Finally, from a financial point of view, not adopting the 'consequential amendments' would have a negative impact due to the fact that the development of ETIAS has already started and the expenses incurred both at EU level and national level would be completely foregone.

For these reasons, the Commission adopted the proposals for the Regulations establishing the conditions for accessing the other EU information systems and introducing technical legal amendments to those other EU information systems.

In addition, having in mind the need for privacy by design and by default, the Commission considered necessary to specify which "authorised" data of Article 17 (see section 2.3.) will be compared to the other EU information system. This is driven by the facts that:

- the purpose for consulting other EU information systems is provided for in Article 20 of the ETIAS Regulation; and
- some personal data provided by the applicant in the ETIAS application form are not recorded in other EU information systems.

3.2. How would ETIAS function?

The purpose of this section, is to give the reader an overview of how the system will function in practice and the elements that were taken into account in the drafting of the proposal.

3.2.1. Which EU information systems will be accessed by ETIAS?

To fulfil its objectives and to enter into operations, ETIAS needs to be connected to other EU information systems, as well as to access and query data in those systems.

In the light of Article 20 of the ETIAS Regulation[7], ETIAS interoperability should at least be established with and access should be given to the other EU information systems mentioned in that Article, namely: the Entry/Exit System[8] (hereinafter 'EES'), Eurodac[9], Europol data[10],

---

cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816. OJ L 135, 22.5.2019, p. 85–135.

[7] Article 20 of the ETIAS Regulation: "*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".*

[8] Established by Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. OJ L 327, 9.12.2017, p. 20–82.

the Schengen Information System[11] (hereinafter 'SIS') and the Visa Information System[12] (hereinafter 'VIS'). ETIAS should have the possibility to query the Interpol Stolen and Lost Travel Documents Database (hereinafter 'SLTD') and the Travel Documents Associated with Notices Database (hereinafter 'TDAWN') in an automated way and in accordance with the conditions laid down in Article 12 of the ETIAS Regulation.

Moreover, the legislator has in recital 58 of that Regulation, indicated that: "*In order to assess the security, illegal immigration or high epidemic risks which could be posed by a traveller, interoperability between the ETIAS Information System and other EU information systems should be established. Interoperability should be established in full compliance with the Union acquis concerning fundamental rights.* ***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***". In this recital, the legislator has clearly expressed that ETIAS should be able to query future systems which would be relevant for the specific purposes of ETIAS (which is to assess whether travellers for third countries would pose a security, illegal immigration or high epidemic risk).

With this recital, the legislator took a forward-looking approach, allowing for ETIAS to evolve in the future with regard to possible technological developments. This is important to ensure that ETIAS is able to fulfil its objectives making full use of the means available in terms of information and to the extent that they are relevant for ETIAS. Still, while this clearly expresses a political intention to allow for evolution, any future extension of the interoperability would require the proposal of new 'consequential amendments' for the legislator to consider. These 'consequential amendments' would specify the data that would

---

[9] Established by Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 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. OJ L 180, 29.6.2013, p. 1–30.

[10] Established under Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. OJ L 135, 24.5.2016, p. 53–114.

[11] Established by Regulation (EU) 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. OJ L 312, 7.12.2018, p. 14–55.
Regulation (EU) 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. OJ L 312, 7.12.2018, p. 56–106.

[12] Regulation (EC) No 767/2008.

be queried, who and how those data would be accessed and would need to ensure the protection of the fundamental rights.

In this forward-looking endeavour, the legislator specifically identifies the ECRIS-TCN Regulation[13] as a future system to be connected to ETIAS. It is important to note that during the negotiations of the ETIAS Regulation, the legislators had also been pursuing inter-institutional negotiations on the ECRIS-TCN proposal[14] and had the intention to include it in the operative part of the ETIAS Regulation. However, the ECRIS-TCN Regulation was adopted seven months after the adoption of the ETIAS Regulation, in April 2019. This Regulation established a European Criminal Records Information System for Third Country Nationals, allowing for identification of the Member States holding conviction information on third-country nationals and stateless persons. As a result, it was not possible to include ECRIS-TCN when the ETIAS Regulation was adopted.

Therefore, when adopting the proposals for the Regulations in accordance with the provisions of the ETIAS Regulation ('the consequential amendments' of ETIAS), the Commission introduced amendments to the EU information systems mentioned in Article 20, as well as to ECRIS-TCN mentioned in Recital 58. The Commission considered it part of its proposal having regard to the following considerations:

- the intention expressed in recital 58 is that ETIAS should be able to query ECRIS-TCN once available;
- the ECRIS-TCN Regulation had been agreed and subsequently adopted and therefore;
- the conditions are met to assess whether the presence in the EU of third-country nationals with past convictions in the EU for the most serious crimes (terrorist offence[15] or a serious criminal offence[16]) poses a security risk.

In this context, how could it be explained that ECRIS-TCN was not part of the proposal? More than that, one could say that "we" would fail to duly protect the citizen's right to security which is enshrined in Article 6 of the Charter of Fundamental Rights.

Following the same logic, amendments to Eurodac were not proposed even though it is specifically mentioned in Article 20 of the ETIAS Regulation due to the fact that currently only searches with biometric data are possible in Eurodac while ETIAS only contains

[13] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 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. OJ L 135, 22.5.2019, p. 1–26.

[14] Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011. COM(2017) 344 final.

[15] See Article 3(1)(15) of the ETIAS Regulation on the definitions which refers to Directive (EU) 2017/541.

[16] See Article 3(1)(16) of the ETIAS Regulation on the definitions which refers to Article 2(2) of Council Framework Decision 2002/584/JHA.

alphanumeric data. If in the future, Eurodac were to be revised and would also include alphanumeric data, a new 'consequential amendment' to the ETIAS Regulation and the future Eurodac legal basis would be proposed.

Finally, with regard to the Interpol databases, a cooperation agreement on the modalities for the exchange of information and on appropriate safeguards for the protection of personal data will be negotiated in order to fulfil the objectives of Article 12 of the ETIAS Regulation.

3.2.2. The comparison of ETIAS data with the data contained in other EU information systems

The data being queried are the data about identity and travel documents. Each central system currently stores data on identity and travel documents separately in spite of the fact that these data are mostly common across several EU Information Systems. The Interoperability Regulations have created the Common Identity Repository ('CIR'), a technical component, in which all identity and travel document data from the different EU information systems (with the exception of SIS and Europol data) will be stored. (See figure 1.)

With a view to ensure coherence between the ETIAS development and interoperability implementation, the proposed ETIAS 'consequential amendments' introduce the Shared Identity Repository ('SIR') which will contain the shared identity data of ETIAS and the EES. This component is the first step of the implementation of the 'CIR', which will use the 'SIR' as its foundation. They will be jointly referred to hereunder as 'CIR/SIR'.

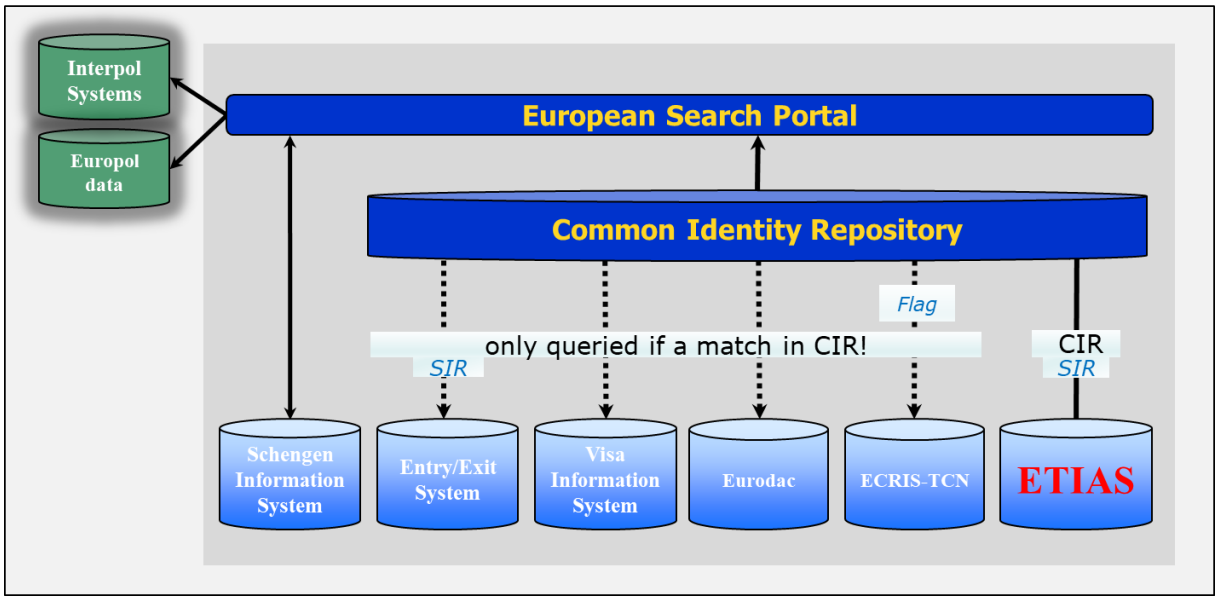
Without the 'CIR/SIR', each system would have to stand the 'query stress' generated by ETIAS. If the data were not accessed through the 'CIR/SIR' each system would have to be able to sustain a high number of constant queries from ETIAS which would have adverse consequences for the performance of the systems. Thus, by gathering the identity and travel document data, the 'query stress' is only taken once by this repository of data.

Therefore, in practice the queries will not be made to the Central Systems of the EES, VIS and ECRIS-TCN, but rather to the 'CIR/SIR' and on a 'hit-no-hit' basis. It is only in case of a 'hit' that ETIAS will go further and access individually the Central System of the other EU information systems to retrieve the specific data it contains. In addition to 'hit-no-hit' rule, a flag was proposed for ECRIS-TCN, in the ETIAS 'consequential amendments', limiting ETIAS access to records concerning persons convicted for *terrorist and serious criminal offences* which are the only relevant ones for attaining the objectives of ETIAS. Moreover, it is worth to underline that ECRIS-TCN does not store centrally the criminal records information per individual but it only informs about the Member State(s) which hold criminal records for a convicted third-country national. Consequently, access to the information contained in the criminal records will be handled at national level by the Member State where the individual has been convicted and in accordance with the national law of that Member State. As a result, the addition of a flag to those records concerning individuals convicted for

terrorist and serious criminal offences will avoid unnecessary accesses to national criminal records.

Finally, with regard to the specific cases of the SIS, Europol data and Interpol Systems, contrary to ETIAS, EES, VIS and ECRIS-TCN, the identity data will not be stored in the 'CIR/SIR' but in the information systems itself. Therefore, specific procedures have been established for ETIAS to access the relevant data.

Figure 1: ***Overview***



For further explanation regarding the European Search Portal or the 'CIR', please refer to the Interoperability Regulations.

3.2.3. Data from the EU information systems accessed by ETIAS

In order to be able to perform the tasks of Articles 20, 22 and 26 of the ETIAS Regulation, the ETIAS Central System, the ETIAS Central Unit and the ETIAS National Units need to have an appropriate access to the data contained in the other EU information systems.

To provide those three entities with the required access rights, the proposals amend the legislative acts establishing the other EU information systems. The access rights of the ETIAS Central System is addressed under the Articles[17] titled "*Interoperability with ETIAS in*

[17] Article 18b for VIS, Article 8b for EES and Article 36a for SIS [border].

the meaning of Article 11 of Regulation (EU) 2018/1240". The access rights of the ETIAS Central Unit and the ETIAS National Units are addressed under separate Articles[18].

The processing of an application: a three-step analysis

The functioning of ETIAS, as established by the ETIAS Regulation, is based on a three-step analysis of the applications, which comes down to the following[19]:

1. An automated processing of applications for a travel authorisation[20]. As mentioned, the data used by the ETIAS Central System to query and access the other EU information system are those of points (a),(b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) (see section 2.3.). The access to the data by the ETIAS Central System is on a 'hit-no-hit' basis through the 'CIR/SIR' as explained in the section 3.2.2.

2. If this process returns no 'hits', the travel authorisation is issued immediately. However, when one or several 'hits' are returned, the ETIAS Central Unit is required to compare the *identity data* stored in the ETIAS Central System to those stored in the other EU information systems. On that basis, the ETIAS Central Unit either:
   - determines that the identity data contained in the "hit" do not correspond to those of the applicant[21]. In that case, the travel authorisation is issued; or
   - confirms that the identity data contained in the "hit" corresponds to those of the applicant in the ETIAS application form. In that case the processing of the application is passed on to the ETIAS National Unit(s) responsible[22].

3. Where the processing of the application is passed on to the 'ETIAS National Unit responsible', that Unit processes manually each application that it receives. The task of the ETIAS National Units is to assess whether, based on the 'hits', the presence of the person in the territory of the Schengen area represents a security, illegal immigration or a high epidemic risk. It is also responsible for issuing or refusing the travel authorisation to the applicant on the basis of that assessment. To that end, the ETIAS National Unit responsible needs to have access to the corresponding file, alert or record contained in the EU other information system. That access is granted to the extent necessary to decide whether to issue or refuse the travel authorisation and in

[18] Articles 18b and 18c for VIS, Articles 25a and 25b for EES and Articles 34(1)(g) and 36a for SIS [border].
[19] When an applicant responds positively to one of the background questions, his/her application is still processed automatically but anyhow forwarded to a National Unit as this requires a specific handling of the case.
[20] See Article 20 of the ETIAS Regulation.
[21] See Article 22.
[22] See Article 25.

compliance with the legal framework of the systems accessed[23]. Moreover, in cases where a single application for a travel authorisation triggers several hits, the ETIAS National Unit responsible shall consult other ETIAS National Units – so called 'ETIAS National Units consulted'. More precisely, it will consult those Member States whose data, file or alert, contained in the EU information systems queried, triggered the hits. In such a case, the ETIAS National Unit responsible is in charge of the coordination of the answers from the other ETIAS National Units consulted and it remains responsible for issuing a decision on the application for a travel authorisation. Nevertheless, if one ETIAS National Unit consulted provides a negative answer, the ETIAS National Unit responsible is obliged to refuse the ETIAS application.

3.3. What are the effects of the proposal?

In this section, the impact of the ETIAS consequential amendments will be assessed. In particular, three elements will be analysed, the impact of the ETIAS scope, the impact on the other EU information systems' capacity and the associated costs and finally the impact on fundamental rights.

3.3.1. On ETIAS

The 'consequential amendments' enable ETIAS to access the different systems to meet the objectives of the system. These amendments do *not* modify the scope of ETIAS. ETIAS only concerns third-country nationals who are visa-exempt, visiting the Schengen area for intended short-stays and which do not fall in one of the categories of exceptions included under Article 2(2) (Scope) of the ETIAS Regulation. These categories of exceptions include family members of Union Citizens to whom the Directive 2004/38/EC (the "free movement" directive) applies as well as the third-country nationals having a reason for a regular stay in the Schengen area, such as third-country nationals holding a residence permit or a residence card.

3.3.2. On the other EU information Systems' capacity and associated costs

The most important impact of ETIAS on the other EU information systems is the increased number of queries of each information system, as each system will be queried per ETIAS application. The financial impacts on the different EU information systems have been anticipated at the stage of the initial proposal for the ETIAS Regulation and the Interoperability Regulations and were included in the Legislative Financial Statement of the

[23] See Article 26.

initial proposal[24] or in the Legislative Financial Statement for the Interoperability Regulations[25].

As explained above, this additional query load is handled with the components defined in the Interoperability Regulation(s). The major part of the query load will be handled through the 'CIR/SIR' as a first step. The cost of building those components will be borne by the EU budget according to the Interoperability Regulations[26] since the 'SIR' is the first step of the 'CIR' development. The consequential amendments do not modify the assumptions used for the respective Legislative Financial Statement which required the preparation of an implementation plan.

Moreover, for systems handling natively a large query load anyway (like EES, VIS, SIS) this increase remains sizable but does not change the order of magnitude of the systems' capacity.

With regard to the specific cases of the SIS and Europol data, as explained above, the identity data will not be stored in the 'CIR' but in the information systems themselves. As a result, an upgrade of these systems was needed. The costs for upgrading these systems were included in the Legislative Financial Statement for the Interoperability Regulations[27].

The national systems of the Member States will not be impacted financially neither by building the 'CIR/SIR' nor by upgrading the central systems because the interface towards the national systems remain the same and the changes only affect the architecture of the central systems.

Furthermore, as explained above, the ETIAS consequential amendments propose to use a flag for the access to ECRIS-TCN, in addition to the 'hit-no-hit' rule, so that only the cases that are relevant for ETIAS be queried, namely those of third country nationals who were convicted for a terrorist offence or other serious criminal offence. That flag *de facto* reduces the impact on the system. Additionally, in terms of human resources, it will be necessary for each Member States to establish the table of correspondence between the list of terrorist offences or other serious criminal offences referred to in Articles 3(1)(15) and (16) of the ETIAS Regulation and the corresponding offences in its national legislation. The human resources costs for establishing that table of correspondence should be marginal. Moreover,

---

[24] The Financial annex to the Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624. COM/2016/0731 final.

[25] The Financial annex to the Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]. COM/2018/478 final.

[26] Article 70 of Regulation (EU) 2019/817; OJ L 135, 22.5.2019, p. 27–84.
Article 66 of Regulation (EU) 2019/818; OJ L 135, 22.5.2019, p. 85–135.

[27] Ibid, footnote 21.

once that table is established, the flagging of terrorist offences or of other serious criminal offences can be automated if the Member States includes this operation in the process to upload records in ECRIS-TCN.
The Member States should take advantage of the fact that ECRIS-TCN has not yet been built to anticipate such automated function in parallel to the development of ECRIS-TCN.

In summary, the 'consequential amendments' capacity and financial impacts have been anticipated at the technical and budgetary levels.

3.3.3. On the fundamental rights

ETIAS

The impacts of the accesses established in the ETIAS Regulation were assessed and analysed already when adopting the ETIAS Regulation. Therefore, before going into details regarding the impact of the ETIAS consequential amendments, it is important to recall that the ETIAS Regulation is in line with the right to the protection of personal data.

ETIAS has an impact on the right to the protection of personal data. This right is guaranteed by Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the European Union, and in Article 8 of the European Convention on Human Rights. As underlined by the Court of Justice of the EU,[28] the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.[29]

Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(2) of the General Data Protection Regulation,[30] which indicates that the EU protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The General Data Protection Regulation, with 2018/1725,[31] and, where relevant, Directive (EU) 2016/680[32] apply to the processing of personal data carried out for the purpose of

[28] Court of Justice of the EU, judgment of 9.11.2010, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-0000.
[29] In line with Article 52(1) of the Charter, limitations may be imposed on the exercise of the right to data protection as long as the limitations are provided for by law, respect the essence of the right and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[31] 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.

ETIAS by the Member States and by the EU institutions, bodies and agencies involved, respectively.

According to the Commission Communication of July 2010 on information management in the area of freedom, security and justice,[33] data protection rules should be embedded in any new instruments relying on the use of information technology. This implies the inclusion of appropriate provisions limiting data processing to what is necessary for the specific purpose of that instrument and granting data access only to those entities that 'need to know'. It also implies the choice of appropriate and limited data retention periods depending solely on the objectives of the instrument and the adoption of mechanisms ensuring an accurate risk management and effective protection of the rights of data subjects.

As mentioned the ETIAS feasibility study, "*most of the safeguards existing for other systems and data sets are applicable to ETIAS, as ETIAS data would be processed centrally (safeguards aiming at eu-LISA apply) as well as by Member States (safeguards aiming at Member States apply)*". Moreover, ETIAS guarantees the rights of persons whose data is collected:

- Data protection is embedded into the design and architecture of the existing IT systems for borders and security.

- Specified purposes are clear, limited and relevant to the circumstances (purpose specification); the collection of personal information is limited to that which is necessary for the specified purposes (collection limitation); the collection of personally identifiable information is kept to a strict minimum (data minimisation); the use, retention, and disclosure of personal information is limited to the relevant purposes (use, retention and disclosure limitation); appeal procedures and specific rights to correct the data that are inaccurate.

- The security of personal information is ensured; the applied security standards assure the confidentiality, integrity and availability of personal data throughout its life cycle including, *inter alia*, strong access control and logging methods.

As a result, the right to personal data is affected by ETIAS only to a limited extent. Moreover, as mentioned above ETIAS supports the objectives of contributing to a high level of security by providing for a thorough security risk assessment of applicants; the prevention of illegal immigration by providing for an illegal immigration risk assessment; the protection of public health by providing for an assessment of whether the applicant poses a high

[32] 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.

[33] COM(2010) 385 final.

epidemic risk and enhancing the effectiveness of border checks. ETIAS significantly contributes to achieving those objectives as it is the only system allowing to assess, prior to their travel, whether a third-country national exempt from the visa obligation would pose a security, illegal immigration or high epidemic risk. Furthermore, the processing of data is limited to what is necessary to achieve the objectives.

The ETIAS consequential amendments

The ETIAS 'consequential amendments' are limited to 'technical' amendments implementing the agreement reached under ETIAS and Interoperability Regulations and as such are not creating new significant impacts on the protection of personal data.

The 'consequential amendments' set out with which data ETIAS will query in the other EU Information Systems. By definition these data can only be the ones already contained in the other EU Information Systems. The consequential amendments are not modifying which data these systems are storing, nor the ETIAS data that can be used (see section 2.3). In practice, ETIAS "asks" the other systems whether they contain information on an applicant with a certain identity - as supported by a travel document. ETIAS only uses the alphanumerical data of the applicant's identity and/or travel document for all its queries to the other EU information systems, as provided for in the ETIAS Regulation. Moreover, it does not modify how applications are being processed. Typically, ETIAS already provides that in case of a 'hit', the ETIAS Central Unit only accesses the minimum information necessary in order to verify whether the ETIAS and other EU information systems' identity data of the person correspond (Article 22 of the ETIAS Regulation).

Besides, the ETIAS consequential amendments provide for the definition, through an implementing act, of what a 'correspondence' is - whether the ETIAS and other EU information systems' identity data of the person correspond (Article 1(4)(9) of the ETIAS consequential amendments). The rationale behind that is that considering the fact that data across the different database are not necessarily recorded in the same manner, it is necessary to allow for partial correspondence. In this context, it seemed important to define what a partial correspondence is, including a degree of probability to limit the number false hits to the minimum possible and therefore limit the number of ETIAS application being manually processed to what is necessary.

The 'consequential amendments' include specific provisions that limit the access to the other EU information system to what is relevant for ETIAS: read-only access, further limitation of the data that can be queried; specific provisions limiting the data that can be recording as a result of the manual processing by the ETIAS Central Unit; specific provisions for the recording of the result of the assessment.

ECRIS-TCN

In its letter, the European Parliament requested that the Commission pay particular attention to the proposal on ECRIS-TCN, which *"proposes changes in the legal basis and purpose of the database"*.

The Commission considers that the proposal of connecting ECRIS-TCN to ETIAS would support the achievement of the ETIAS goals in an effective and efficient way. The ETIAS consequential amendment does not modify the natural scope of ECRIS-TCN but it extends it marginally to border management in so far as it supports the ETIAS objectives of identifying whether the presence of ETIAS applicants in the territory of the Member States would pose security risks. The extension of the ECRIS-TCN scope is limited to what is necessary to ensure that ETIAS can fulfil its purpose of enhancing security as the identification is limited to the most serious offences and it ensures the protection of citizen's right to security, which is enshrined in Article 6 of the Charter of fundamental rights.

Moreover, taking into account the principles of proportionality and necessity, the Commission considered it necessary to limit the access to ECRIS-TCN data to the most serious offences namely "terrorist and serious criminal" offences which are the only relevant ones for attaining the objectives of ETIAS. If no limitation was applied, it would have the consequence that a 'hit' will be issued every time information was held by a Member State on criminal conviction. It would mean that ETIAS applicants with only a track record for minor offenses would have a risk of having their application more scrutinised than necessary to meet ETIAS objectives. This would have the effect that more applications would be scrutinised than necessary. In order to ensure proportionality, the Commission proposed that the Member States add a flag in ECRIS-TCN to those records that are relevant for ETIAS, i.e. only those which concern terrorist and serious criminal offences. This flag allows ETIAS to query the limited set of ECRIS-TCN records that are relevant for ETIAS purposes. Consequently, criminal convictions which do not fall under one of those two types of offences are disregarded from the onset.

Furthermore, while the ETIAS consequential amendments allows for the ETIAS Central Unit to access the *identity data* contained in ECRIS-TCN, it is solely for the purpose of assessing the correspondence between the identity data contained in ETIAS and those in ECRIS-TCN. As explained above, the ETIAS Central Unit will not have access to the criminal record themselves. The ETIAS Consequential amendments do not modify the fact that those records can only be access by specifically designated central authorities of the Member States and therefore only these authorities will be able to provide an opinion as regards the ETIAS applications. In this respect, in cases where the ETIAS Central Unit confirms the identity, the 'consequential amendment' does not specify how the ETIAS National Unit should access the national criminal records to allow for flexibility within the Member States to establish such access by the ETIAS National unit in accordance with their national legislation.

Finally, the impacts of the inclusion of ECRIS-TCN data into the CIR were assessed and analysed already when adopting the Interoperability regulations[34].

4. Conclusion

This analytical document shows that the 'consequential amendments' are in line with the provisions of the ETIAS Regulation as well as the legislative framework related to ETIAS. It also shows that there is no adverse effect on the fundamental rights as a result of the 'consequential amendments'.

[34] SWD(2017) 473 final.