

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT **C**

CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

**European Travel Information
and Authorisation System
(ETIAS): Border management,
fundamental rights and
data protection**

STUDY FOR THE LIBE COMMITTEE



DIRECTORATE GENERAL FOR INTERNAL POLICIES

**POLICY DEPARTMENT C: CITIZENS' RIGHTS AND
CONSTITUTIONAL AFFAIRS**

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, appraises the proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS), adopted by the European Commission on 16 November 2016. It provides an assessment of the necessity, implications in relation to interoperability, and impact in terms of fundamental rights, including the right to personal data protection and the right to privacy. It finds that the necessity of ETIAS has not been made, that the proposal is likely to introduce interoperability through the backdoor, and that it constitutes a significant interference with fundamental rights.

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and commissioned, overseen and published by the Policy Department for Citizen's Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizen's Rights and Constitutional Affairs or to subscribe to its newsletter please write to:

Poldep-citizens@ep.europa.eu

Research Administrator Responsible

Kristiina MILT

Policy Department C: Citizen's Rights and Constitutional Affairs

European Parliament

B-1047 Brussels

E-mail: Poldep-citizens@ep.europa.eu

AUTHORS

Susie ALEGRE, Director, Alegre Consulting Ltd and Associate Tenant, Doughty Street Chambers

Dr. Julien JEANDESBOZ (Coordinator), Associate Researcher, CCLS (*Centre d'étude sur les conflits*)

Dr. Niovi VAVOULA, Queen Mary University of London

LINGUISTIC VERSION

Original: EN

Manuscript completed in April 2017

© European Union, 2017

This document is available on the internet at:

<http://www.europarl.europa.eu/supporting-analyses>

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

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

CONTENTS

LIST OF ABBREVIATIONS	5
LIST OF BOXES	7
1. EXECUTIVE SUMMARY	8
2. INTRODUCTION	13
2.1. Context of the study	13
2.2. Questions, argument and organisation of the study	14
3. THE ETIAS PROPOSAL: SCOPE, SUBSTANCE AND EVIDENCE BASIS	16
3.1. From EU-ESTA to ETIAS: a measure with a chequered background	16
3.2. Subject matter, scope and objectives of the proposal	18
3.3. Substance of the measure	20
3.3.1. ETIAS structure	20
3.3.2. ETIAS as an application platform	20
3.3.3. ETIAS as an automatic and manual data processing platform	21
3.3.4. ETIAS as a platform for accessing personal data: carriers and law enforcement access	22
3.3.5. ETIAS as a future-oriented, data mining and profiling platform: the ETIAS screening rules and watchlist	23
3.3.6. Who has authority over ETIAS, and who has oversight? The role of EU agencies and bodies	26
3.4. Assessing the case for ETIAS: evidence basis and demonstrated necessity of the measure	27
3.4.1. The evidence gathering process for the ETIAS proposal	27
3.4.2. Quality of evidence for the ETIAS proposal	28
3.4.3. Questions requiring further evidence to establish necessity in the ETIAS proposal	31
4. ETIAS: STREAMLINING INTEROPERABILITY IN THE SECURITY UNION	35
4.1. Interoperability of information systems: a walk down memory lane	35
4.2. Interoperability in the ETIAS proposal: inserted through the backdoor with minimum scrutiny	37
5. THE ETIAS PROPOSAL: A FUNDAMENTAL RIGHTS ASSESSMENT	41
5.1. Interference with fundamental rights	42
5.2. In accordance with the law	42
5.3. Necessity and purpose	43

- 5.4. Proportionality 44
- 5.5. Discrimination 45
- 6. CONCLUSIONS AND RECOMMENDATIONS 48**
- 6.1. Conclusions 48
- 6.2. Recommendations 49
 - 6.2.1. Points requiring clarification from the European Commission 49
 - 6.2.2. Regarding impact assessment and necessity 50
 - 6.2.3. Regarding interoperability 51
 - 6.2.4. Regarding the ETIAS screening rules and watchlist 51
 - 6.2.5. Regarding fundamental rights compliance 52
- REFERENCES 54**

LIST OF ABBREVIATIONS

API	Advanced Passenger Information
CFR	Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
CRC	Convention on the Rights of the Child
EBCG	European Border and Coast Guard Agency
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECRIS	European Criminal Record Information System
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EES	Entry-Exit System
ESTA	Electronic System for Travel Authorisation
ETIAS	European Travel and Information Authorisation System
ETIAS-CU	ETIAS Central Unit
ETIAS-IS	ETIAS Information System
ETIAS- NUs	ETIAS National Units
ETIAS-SB	ETIAS Screening Board
eu-LISA	European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
FRA	Fundamental Rights Agency
GDPR	European Union General Data Protection Regulation
GAO	United States Government Accountability Office

- HLEG** High-Level Expert Group on Information Systems and Interoperability
- LIBE** European Parliament's Committee on Civil Liberties, Justice and Home Affairs
- PNR** Passenger Name Record
- PwC** PricewaterhouseCoopers
- SLTD** Interpol Stolen and Lost Travel Document database
- SIS** Schengen Information System
- TDAWN** Interpol Travel Documents Associated with Notices database
- VIS** Visa Information System

LIST OF BOXES

Box 1: How many people would be affected by the proposed ETIAS measure?	29
Box 2: Considering alternative ETIAS policy options	30

1. EXECUTIVE SUMMARY

Background

On 16 November 2016, the European Commission adopted 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 (hereafter ETIAS proposal). The ETIAS proposal is the latest initiative following the April 2015 adoption by the European Commission of the European Agenda on Security, the April 2016 adoption of a proposal for the establishment of the Entry-Exit System (EES), and the September 2016 Commission Communication on 'Enhancing security in a world of mobility'.

The introduction of an EU travel authorisation scheme for persons who are not subject to visa requirements was first considered in the 2008 **Commission communication on 'Preparing the next steps in border management in the European Union'**. The proposed measure was dubbed 'EU-ESTA' in reference to the **Electronic System for Travel Authorization** that US authorities eventually introduced in 2009 for travellers from countries participating in the Visa Waiving Program (VWP). In 2011 plans for EU-ESTA were discarded after the Commission communication on '**Smart borders – options and the way ahead**' raised doubts about the necessity of such a measure. Despite this assessment, and less than five years later, the European Commission announced its intention to return to this matter in its April 2016 communication on '**Stronger and Smarter Information Systems for Borders and Security**'.

Aim

This study appraises the ETIAS proposal on the following points:

- the evidence basis for the proposal, in particular the potential new evidence that would demonstrate the necessity for a measure dismissed less than five years ago on such grounds;
- the implications for interoperability, in particular given that the ETIAS proposal explicitly aims for interoperability between multiple EU and international information systems, despite the fact that current policy discussions on interoperability in the EU through the High Level Expert Group on Information Systems and Interoperability (HLEG) have not yet been concluded;
- the fundamental rights implications of the proposal, taking into account that the explanatory statement of the ETIAS proposal considers, but does not give, a full fundamental rights impact assessment.

Findings

With regards to the **evidence basis of the proposal** and the demonstration of necessity, the study finds:

- Overall, the **case for the necessity of ETIAS has not been made.**
- **The ETIAS proposal is not accompanied by a Commission-produced impact assessment document** considering different policy options available to achieve the proposal's stated objectives or its relationship with other instruments in the same policy areas. As such, the proposal **does not conform to the European Commission's 'Better Regulation Guidelines' or the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.**

- Due to the fact that the proposal accumulates objectives, it is **difficult to determine either what parts are necessary or to what extent the measure as a whole is necessary in the first place**. A clearer assessment would be possible if the proposal were to explicitly identify and prioritise the area of public policy to which it is intended to contribute primarily and the specific objectives it is designed to meet.
- The **same contractor, PricewaterhouseCoopers (PwC)**, was asked to gather evidence **on EU-ESTA in 2011 and then in 2016 on ETIAS**. In addition, the **quality of submitted evidence is uneven, and the Commission's argument for the proposal is based at times on partial, ambivalent or inaccurate information**. As a result, some features of the proposal, such as the collection of IP addresses, are unjustified and appear unnecessary, while the specific necessity for a measure related to irregular migration and security targeting visa-exempt third-country nationals is never fully established.
- Due to the volume of personal data it will process, ETIAS should be conceived of as a **platform for mining and profiling personal data** rather than just a platform for issuing automated or manual travel authorisation decisions. The **ETIAS screening rules** aim to **identify persons who are otherwise unknown** to responsible authorities of the Member States **but are assumed to be of interest** for irregular migration, security or public health purposes. These persons are flagged not because of specific actions they have engaged in but because they display particular category traits. While not a data mining and profiling measure, the **ETIAS watchlist** is equally **future-oriented** by aiming to deny travel authorisation to individuals who authorities believe are likely to commit criminal offences in the future. Both measures, while **supplemental, rather than essential, to the core objectives of ETIAS**, constitute particularly severe infringements on fundamental rights.
- The proposal is, furthermore, not accompanied by a **fundamental rights or data protection impact assessment**.

With regard to the **implications for interoperability**, the study finds:

- The forthcoming ETIAS Regulation foresees the introduction of interoperability of existing and new large-scale information systems **through the back door and without a proper and necessary impact assessment** of the privacy and data protection implications.
- The ETIAS proposal **does not foresee detailed rules** on how interoperability will be ensured, which model will be preferred or how it may be embedded in ETIAS.
- The implications of interoperability to the fundamental rights of individuals will be magnified when compared to the current compartmentalisation of databases; the **specific purpose(s) for which a system was set up will be nullified**; and there is a risk of **extensive profiling**, as authorities may be able to compile a profile of travellers on the basis of information from different systems, with the result that individual rights and supervision may be more difficult to exercise.

With regard to a fundamental rights assessment of the ETIAS proposal, the study finds:

- The proposal would **amount to a significant interference with human rights**, in particular the right to private life and the right to data protection, but the justification for and necessity of the interference have not been clearly explained.
- It is **impossible to assess the proportionality** of the measure as **the need to be met has not been clearly expressed**. There is no indication that alternative, less intrusive options have been considered, and the **effectiveness of the proposal has not been demonstrated**.

- The range of data collected and the wide scope for its use give rise to concerns that data may be used for **profiling**, with **potentially discriminatory consequences**.
- The broad scope of information requested from applicants seems unnecessarily intrusive, interfering with the right to dignity.

Recommendations

The study outlines a **series of clarifications** that the LIBE Committee should consider requesting from the European Commission to indicate, firstly, why the Commission considers that there has been a change of circumstances in the last five years making the measure necessary now, on the circumstances that made **PricewaterhouseCoopers** the **exclusive contractor** for **both** EU-ESTA in 2011 and ETIAS in 2016, and, finally, the reasons to **not submit a full impact assessment**.

Regarding the **case for the necessity** of ETIAS, the study recommends the following:

- The LIBE Committee should **insist that the ETIAS proposal comply with the European Commission's 'Better Regulation Guidelines'** and that it be **accompanied by a full impact assessment**, together with a positive opinion by the European Commission Regulatory Scrutiny Board. **This request may be based on Point 16 of the Interinstitutional Agreement of 13 April 2016 on Better Law-Making**.¹
- The impact assessment process **should give enough time for proper inter-service consultation within the European Commission and other EU bodies**, including the European External Action Service (EEAS), the European Data Protection Supervisor (EDPS) and the Fundamental Rights Agency (FRA).
- The impact assessment should clearly provide and state any **evidence that, firstly, circumstances have changed sufficiently in the five years since the EU-ESTA initiative was abandoned to justify the necessity of ETIAS** and, **secondly, that visa-exempt third-country nationals are of particular concern with regard to irregular migration and security risks**.
- The impact assessment should provide **an appropriate list of policy options**, including the **impact of 'no ETIAS'**, the possibility of establishing ETIAS without screening rules, the ETIAS watchlist, or Europol and law enforcement access, as well as **explore further possibilities for data minimisation**, including the impact of not collecting IP addresses or health-related personal data.
- The impact assessment **should include an analysis of the effect on the EU's international relations**, in particular on third countries whose citizens currently benefit from visa exemption or are likely to do so in the foreseeable future. A consultation with the Permanent Representatives to the EU of the concerned third countries should be considered.
- The impact assessment **should include a fundamental rights impact assessment**, including, but not limited to, the rights to data protection and privacy.

On **the question of interoperability**, the study recommends the following:

- The LIBE Committee should consider **putting on hold the examination of the ETIAS proposal** until **policy orientations, guidelines and possible legislation on**

¹ Point 16 of the Agreement states: 'The Commission may, on its own initiative or upon invitation by the European Parliament or the Council, complement its own impact assessment or undertake other analytical work it considers necessary'.

interoperability have been tabled and adopted and until such time as **the co-legislators make a final decision on the proposal for a Regulation establishing the EES**.

- Alternatively, as part of a comprehensive impact assessment accompanying the proposal for an ETIAS Regulation, **the LIBE Committee should request the European Commission to include a specific explanation of interoperability**, including the legal provisions that shall govern interoperability, which model will be used and how it may be embedded in ETIAS.

The study foregrounds **specific recommendations on ETIAS screening rules and the watchlist**, which potentially constitute **particularly severe infringements on fundamental rights**:

- **ETIAS screening rules are supplemental rather than essential to the other measures involved in ETIAS's functioning**. In the meantime, data mining and profiling form a **particularly serious interference with the rights to data protection and privacy**. As such, **the LIBE Committee should consider establishing ETIAS without the ETIAS screening rules**.
- Alternatively, before considering the establishment of ETIAS screening rules, the LIBE Committee should request the European Commission, in concert with the European Border and Coast Guard Agency (EBCG) when appropriate, to submit, as part of a comprehensive ETIAS impact assessment, **an explanation of the provenance, substance and functioning of the algorithm and risk indicators** that will be used in ETIAS screening rules.
- Should the co-legislators eventually find the establishment of ETIAS screening rules relevant, **the LIBE Committee should consider including a suspension and a sunset clause for the measure in the ETIAS Regulation**. These would have the following effect: 1) the use of ETIAS screening rules would be **suspended**, pending review by the EDPS and the FRA together with the EBCG, should appeals related to decisions made on the basis of the screening rules increase beyond a threshold to be determined by the co-legislators or should the functioning of the screening rules be considered less than optimal by the relevant national authorities; and 2) a **sunset clause foreseeing the full and definitive shutdown of ETIAS screening rules** should the review, undertaken by the EDPS, FRA and EBCG upon suspension, be concluded negatively.
- The ETIAS watchlist is a supplemental rather than an essential part of the ETIAS proposal. In the meantime, it raises questions regarding the relationship with the EU counter-terrorism watchlist under Common Position 2001/931/CFSP and the reliance on information obtained through international cooperation. As such, **the LIBE Committee should consider establishing ETIAS without the ETIAS watchlist**. Alternatively, **the LIBE Committee should consider including a suspension and a sunset clause for the ETIAS watchlist** on the model suggested for the ETIAS screening rules.
- The oversight mechanism for the ETIAS screening rules and watchlist does not involve the intervention of independent or EU bodies other than the European Commission, ETIAS Central Unit and Europol. **The ETIAS Central Unit is effectively expected to self-monitor the impact of ETIAS screening rules on fundamental rights and privacy and data protection**. Furthermore, the ETIAS Screening Board does not include any independent or EU body other than Europol and ETIAS National Units. Additionally, **there is no oversight or monitoring mechanism involved in Europol's implementation of the ETIAS watchlist**. The LIBE Committee should consider amending the relevant Articles in the ETIAS proposal (Articles 7, 9, 28 and 29) to provide, at the very least, for

the systematic involvement of the EDPS and FRA on matters of fundamental rights, including discrimination, the right to data protection and the right to privacy.

Regarding fundamental rights compliance, finally, the study recommends:

- A **human rights impact assessment needs to be carried out before the proposal can be considered compliant with fundamental rights**. Taking into consideration **the requirement made recently by the European Parliament in its 13 December 2016 Resolution that fundamental rights should be part of the impact assessment of all legislative proposals in the European Union**, the LIBE Committee should recommend that such an impact assessment should **be carried out by an independent expert or body not involved in the design of the proposal**, with full involvement and support from the EDPS and the FRA.
- An impact assessment should **take into account the following issues**, among others, when assessing the necessity and proportionality of the proposed measures:
 - Why is ETIAS necessary and proportionate in addition to existing Passenger Name Record (PNR) and Advanced Passenger Information (API) frameworks?
 - What is the purpose of the individual data points requested and how do they support the **proposal's** legitimate aims?
 - Why should visa-exempt ETIAS applicants provide more data than applicants for a Schengen visa going through the VIS system?
 - If the purpose is screening before entry, what is the reason for retaining the data after the initial authorisation is granted? Why was a five-year retention period chosen?
 - Which agencies shall have access to the data and for what exact purpose? In particular, will intelligence services have access to ETIAS?
 - Why is it necessary to provide access to ETIAS data from the outset to law enforcement authorities and Europol? Under what conditions shall this access take place?
 - Will it be necessary for law enforcement authorities and Europol to have access to the full set of ETIAS data?
- The data required and the questions to be asked should be **reconsidered given the high risk of profiling based on protected characteristics**.
- The reasons for and the scale of the potential for interoperability in the proposal need to be explained with reference to the principles of legality, necessity and proportionality.

2. INTRODUCTION

2.1. Context of the study

On 16 November 2016, the European Commission adopted 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 (hereafter ETIAS proposal).² The ETIAS proposal is the latest initiative following the April 2015 adoption by the European Commission of the European Agenda on Security, the April 2016 adoption of a proposal for the establishment of the Entry-Exit System (EES), and the September 2016 Commission Communication on 'Enhancing security in a world of mobility'.³

The ETIAS proposal foresees that **all travellers to the Schengen area not subject to visa requirements** shall be obliged to **obtain authorisation prior to their departure** through an online application. The travel authorisation requirement does not concern EU citizens, holders of a valid residence permit or a local border traffic permit, among others, but applies to third-country nationals enjoying the right of free movement who do not hold a residence card, including third-country nationals who are family members of a Union citizen and to whom Directive 2004/38/EC applies. The delivery of an authorisation to travel under the ETIAS scheme is conditional upon the automated processing (comparison) of applicant personal data held in

- 1) existing information systems, such as the Schengen Information System (SIS), the Visa Information System (VIS), Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), the EES, Eurodac, the European Criminal Records Information System (ECRIS), and the Interpol Travel Documents Associated with Notices database (TDAWN);
- 2) the ETIAS-specific watchlist established by the ETIAS proposal; and
- 3) specific risk indicators.

The system will automatically issue a travel authorisation when the automated processing does not report a hit, while one or several hits will result in the application being processed manually by ETIAS National Units (based on the traveller's declared intended first country of entry). The proposal also foresees access to the personal data held in the ETIAS system by law enforcement and Europol for the purpose of countering terrorism and serious and organised crime.

As such, the ETIAS proposal displays four notable features:

- It continues the trend, most recently exemplified by the adoption of the EU PNR Directive and the examination of the proposal to establish the EES (awaiting Parliament first reading at the time of writing) of increasing the **reliance on mass**

² European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*. COM(2016) 731 final, 16.11.2016.

³ European Commission (2015), *The European Agenda on Security*. COM(2015) 185 final, 28.4.2015; European Commission (2016), *Proposal for a Regulation of the European Parliament and of the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*. COM(2016) 194 final, 6.4.2016; and European Commission (2016), *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*. COM(2016) 602 final, 14.9.2016.

data processing for the purpose of border control and countering terrorism and serious and organised crime.⁴

- It expands and formalises the reliance on **automated processing, interoperability** between information systems, and **data mining** and **profiling** characterised as 'risk assessment' in both the EU PNR directive and the ETIAS proposal.
- It follows the precedent set, among others, by VIS and possibly EES, of granting **law enforcement access to applicant data from the outset**.
- It **constitutes a significant interference** with fundamental rights, including, but not limited to, the right to private life and the right to the protection of personal data.

These four features are further compounded by the fact that, much like EU-PNR and EES, the ETIAS proposal has a rather chequered history. The introduction of an EU travel authorisation scheme for persons not subject to visa requirements was **first considered in the 2008 Commission communication on 'Preparing the next steps in border management in the European Union'**.⁵ The proposed measure was dubbed 'EU-ESTA' in reference to the Electronic System for Travel Authorization that US authorities eventually introduced in 2009 for travellers from countries participating in the Visa Waiving Program (VWP). In 2011 plans for EU-ESTA were discarded after the Commission communication on '**Smart borders – options and the way ahead**' raised doubts about the necessity of such a measure.⁶ At the time, the European Commission justified this decision by arguing that EU-ESTA's 'potential contribution to enhancing the security of the Member States would **neither justify the collection of personal data at such a scale** nor the financial cost and the impact on international relations'.⁷ Despite this assessment, and less than five years later, the European Commission announced its intention to return to this matter in its April 2016 communication on '**Stronger and Smarter Information Systems for Borders and Security**'.⁸

2.2. Questions, argument and organisation of the study

The most salient features of the ETIAS proposal and the uneven path of the idea of an EU-wide system of travel authorisation raise **three sets of questions** that need to be taken into consideration as the proposal is examined by the co-legislators:

- First, have there **been major documented changes** in the five years since the EU-ESTA option was first discarded that require the establishment of the ETIAS scheme now? This question concerns **the evidence basis** supporting the proposal and the **case for its necessity**.
- Second, how does ETIAS fit into the increasingly dense landscape of EU data processing schemes related to border control and the countering of terrorism and serious and organised crime? ETIAS is ostensibly a flanking measure to the EU visa policy, but some of the key features of the Commission proposal, especially automated processing, interoperability and profiling, blur the lines between the purported objectives of the measure, **making it difficult to assess the strict necessity and proportionality of the measure**, raising **further doubts about the lawfulness of the proposal**.

⁴ Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. OJEU L119/132, 4.5.2016.

⁵ European Commission (2008), *Preparing the next steps in border management in the European Union*. COM(2008) 69 final, 13.2.2008.

⁶ European Commission (2011), *Smart borders – options and the way ahead*. COM(2011) 680 final, 25.10.2011.

⁷ *Ibid*, p. 7 (emphasis added).

⁸ European Commission (2016), *Stronger and Smarter Information Systems for Borders and Security*. COM(2016) 205 final, 6.4.2016.

- Thirdly, **to what extent does the proposed measure interfere with fundamental rights**, including, but not limited to, the rights to privacy and data protection? To what extent is it **in conformity with EU and international law**?

In addressing these questions, this **study will demonstrate that the case for the necessity of ETIAS has not been made**. The focus on necessity follows the requirement laid out by the European Parliament in its Resolution of 29 October 2015, building on the ruling of the Court of Justice of the European Union (CJEU) of 8 April 2014 on data retention, that “the impact assessment of all law-enforcement and security measures involving the use and collection of personal data always includes a necessity and proportionality test”.⁹

In the meantime, the proposal’s focus on streamlining automated processing, interoperability and data mining and profiling has a potential impact on other policies related to border control and countering terrorism and serious and organised crime. As such, discussions on ETIAS need to be considered in the broader context of on-going discussions – **such as European Parliament resolutions over the last three years on mass surveillance and security** – about interoperability, the issue of data mining and profiling for security purposes and the infringement of such measures on fundamental rights, including the rights to privacy and data protection.¹⁰

This study will first examine the evidence basis of the ETIAS proposal (Section 2). It will then provide an examination of the relationship between the ETIAS proposal and the notion of interoperability (Section 3). It will finally develop a fundamental rights assessment of the ETIAS proposal (Section 4). On the basis of key findings, it will lastly provide a set of recommendations for consideration by the LIBE Committee (Section 5).

⁹ European Parliament (2015), *European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP))*. P8_TA(2015)0388, point 45.

¹⁰ See European Parliament (2014), *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*. P7_TA(2014)0230; P8_TA(2015)0388, op.cit.

3. THE ETIAS PROPOSAL: SCOPE, SUBSTANCE AND EVIDENCE BASIS

KEY FINDINGS

- Overall, **the case for the necessity of ETIAS has not been made.**
- **The ETIAS proposal is not accompanied by a Commission-produced impact assessment document** considering different policy options available to achieve the proposal's stated objectives or its relationship with other instruments in the same policy areas. As such, the proposal **does not conform to the European Commission's 'Better Regulation Guidelines' or the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.**
- **Due to the fact that the proposal accumulates objectives, it is difficult to determine either what parts are necessary or to what extent the measure is necessary in the first place.** A better assessment would be possible if the proposal were to clearly identify and prioritise the area of public policy to which it is intended to contribute primarily and the specific objectives it is designed to meet.
- The **same contractor, PricewaterhouseCoopers,** was asked to gather evidence **on EU-ESTA in 2011 and then in 2016 on ETIAS.** The **quality of furnished evidence is uneven, and the Commission's argument for the proposal is based at times on partial, ambivalent or inaccurate information.** As a result, some features of the proposal, such as the collection of IP addresses, are unjustified and unnecessary, while the necessity for a measure related to irregular migration and security targeting **specifically** visa-exempt third-country nationals is never fully established.
- Due to the volume of personal data it will process, ETIAS should be conceived of as a **platform for mining and profiling personal data** rather than a platform for issuing automated or manual travel authorisation decisions. The **ETIAS screening rules** aim to **identify persons who are otherwise unknown** to responsible authorities of the Member States **but are assumed to be of interest** for irregular migration, security or public health purposes. These persons are flagged not because of specific actions they have engaged in but because they display particular category traits. While not a data mining and profiling measure, the **ETIAS watchlist** is equally **future-oriented** by aiming to deny travel authorisation to individuals who authorities believe are likely to commit criminal offences in the future. Both measures, while **supplemental, rather than essential, to the core objectives of ETIAS,** constitute particularly severe infringements on fundamental rights.

3.1. From EU-ESTA to ETIAS: a measure with a chequered background

The introduction of an EU travel authorisation scheme for travellers not subject to visa requirements has been discussed for about ten years. The possibility of establishing an EU-ESTA was mentioned in passing in the communication on 'Preparing the next steps in border management in the European Union', adopted by the European Commission in February 2008. At the time, the measure was associated with border control and migration policy

rather than security, and the Commission suggested that EU-ESTA 'data could be used for verifying that a person fulfils the entry conditions before travelling to the EU, while using a **lighter and simpler procedure compared to a visa**'.¹¹ In its March 2009 resolution on the communication, however, the European Parliament **questioned 'whether the proposed system is absolutely necessary'** and asked for 'a thorough explanation of the rationale for it', expressing its conviction 'that close cooperation between intelligence services in particular is the right way forward, **rather than a massive collection of data in general**'.¹²

The professional services and consulting firm PricewaterhouseCoopers was commissioned to conduct a policy study, eventually published in February 2011, on EU-ESTA.¹³ The study considered four main options, including an EU-ESTA for all or only some visa-exempt third-country nationals, a combination of an EU-ESTA with electronic visas, or a gradual substitution of visa requirements by an EU-ESTA. One of the **report's key findings was that setting up an EU-ESTA requiring all visa-exempt third-country nationals to apply for a travel authorisation would not constitute a significant technical challenge but would present 'rather uncertain' security benefits, generate 'very tangible' costs and create a series of practical problems, including possible diplomatic tensions with third-country governments.**¹⁴ In particular, the report notes that **'no conclusive evidence was found in the course of this policy study to suggest that the system would make a significant contribution to enhancing their [the Member States] security, or at least one that could be perceived as justifying the collection and processing of personal data on the scale that would be required for an EU-ESTA and the investment it would represent'**.¹⁵

The concern expressed in the initial PwC study about the **strict necessity of EU-ESTA** was reflected in the Commission's own conclusions in the 2011 communication on 'Smart borders – options and the way ahead', which **discarded the establishment of an EU-ESTA** on similar grounds and **insisted instead that priority should be given to the smart borders package**. The communication outlined the possibility of returning to EU-ESTA but in line with the fourth option advanced by the contractor, namely as a **'contribution to the further development of the common visa policy'**, either in combination with electronic visas or the substitution of the visa requirement by an ESTA.¹⁶

The European Commission eventually returned to the matter five years later through the issue of security rather than the common visa policy. The first public reference to the current ETIAS proposal can be found in the April 2016 Commission communication on '**Stronger and Smarter Information Systems for Borders and Security**'. ETIAS is **presented as a tool to address the 'information gap' on visa-exempt third-country nationals arriving by land** for whom 'no information is available prior to their arrival at the EU's external border' (the purported 'gap' cannot be filled by either API or PNR data).¹⁷ The September 2016 Commission communication on '**Enhancing security in a world of mobility**' presents a more detailed overview of the foreseen measure, starting with the relevance of ETIAS for the common visa policy and in particular for visa liberalisation, before emphasising its relevance **as an 'additional layer of systematic control for visa-free country nationals [that] would be a valuable complement to existing measures to maintain and strengthen the security of the Schengen area'**.¹⁸ The ETIAS proposal, finally, is supported by a feasibility study from June

¹¹ COM (2008), 69 final, op. cit., p. 9.

¹² European Parliament (2010), *European Parliament resolution of 10 March 2009 on the next steps in border management in the European Union and similar experiences in third countries (2008/2181 (INI))*. OJEU, 2010/C 87 E/01, p. 4 (emphasis added).

¹³ PwC (2011), *Policy study on an EU Electronic System for Travel Authorization (EU ESTA)*. Brussels, 2010-1227/OV/fvh/ms/wb/ns.

¹⁴ Ibid., pp. 15-18 for the summarised analysis, pp. 281-285 for the full discussion.

¹⁵ Ibid., p. 18 (emphasis added).

¹⁶ COM (2011), 680 final, op. cit., p. 7.

¹⁷ COM (2016), 205 final, op. cit., p. 13.

¹⁸ COM (2016), 602 final, op. cit., p. 9.

to October 2016 and delivered on 16 November 2016 by the contractor PwC (which had already conducted the 2011 EU-ESTA study).¹⁹

The historical background to the current ETIAS proposal outlines **how rapidly the matter has pivoted**. In 2011 the European Commission considered, in line with what had been argued by the European Parliament, that **EU-ESTA was not a necessary measure and that priority should be given to smart borders, and especially EES**. Less than five years later, however, as **EES is being discussed by the co-legislators**, the European Commission is now **stressing 'the need to put in place a system that is able to achieve objectives similar to the visa regime, namely to assess and manage the potential irregular migration and security risks represented by third country nationals visiting the EU'**.²⁰ Given the significant rights implications, most notably in terms of privacy and data protection, the Commission should provide a clear explanation of the changes in circumstances in 2011 that makes the proposal justified and necessary.

3.2. Subject matter, scope and objectives of the proposal

The ETIAS proposal calls for the establishment of a centralised information system (warranting the choice for a Regulation rather than a Directive) that would gather and automatically process several categories of personal data **for all visa-exempt travellers to the Schengen area in order 'to determine whether their presence in the territory of the Member States does not pose an irregular migration, security or public health risk'** (Article 1). The outcome of this processing is the issuance or not of a travel authorisation, without which visa-exempt third-country nationals shall not be allowed to travel to the EU.

According to Article 2 of the proposal, the ETIAS Regulation would apply to:

- a) all nationals of third countries listed in Annex II to Council Regulation (EC) No 539/2001 who are exempt from the visa requirement for airport transit or intended stays in the territory of the Member States of a duration of no more than 90 days in any 180-day period;
- b) refugees and stateless persons residing in and holding a travel document from a third country listed in Annex II to Council Regulation (EC) No 539/2001 and who are exempted from the visa requirement pursuant to Article 4(2)(b) of that Regulation;
- c) third-country nationals who are family members of a Union citizen to whom Directive 2004/38/EC applies or of a national of a third country enjoying the right of free movement under Union law and who do not hold a residence card referred to under Directive 2004/38/EC.

Notable exclusions from the scope of the ETIAS Regulation include the following:

- 1) refugees and stateless persons or other persons who do not hold the nationality of any country residing in a Member State but who hold a travel document issued by that Member State;
- 2) third-country nationals who are members of the family of a Union citizen or third-country nationals who are members of the family of a third-country national enjoying the right of free movement under Union law, when these family members hold a residence card; and
- 3) holders of a local border traffic permit when they exercise their right within the context of the Local Border Traffic regime.

¹⁹ PwC (2016), *Feasibility Study for a European Travel Information and Authorisation System (ETIAS)*. Luxembourg: Publications Office of the European Union.

²⁰ COM (2016), 731 final, p. 2.

All in all, the Commission estimates that around **39 million travellers** would have their personal data processed through ETIAS by **2020** (see **Box 1** in **Section 2.4** for an **assessment of this calculation**). The ETIAS proposal is **thus meant to anticipate** an increase in visa-exempt traveller flows. The data processing listed in Article 4 of the ETIAS proposal would contribute to meeting the following specific objectives:

- 'a high level of security' by enabling a thorough security risk assessment of visa-exempt travellers;
- 'the prevention of irregular migration' by providing for an irregular migration risk assessment of applicants;
- 'the protection of public health' by providing for an assessment of whether the applicant poses a public health risk;
- enhancing the effectiveness of border checks;
- supporting the objectives of SIS related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet or specific checks;
- 'the prevention, detection and investigation' of terrorist offences or other serious criminal offences.

This list of specific objectives calls for three observations. First, there seems to be **a gap in reasoning in the proposal**. The identification of the problem and the objectives of the proposal are not logically connected. The **ETIAS proposal is justified by an anticipated increase in the numbers of visa-exempt travellers to the EU**. However, as the European Commission has argued in the past (for other initiatives such as the 'smart borders' legislative package), tackling increasing traveller flows could be seen as a **matter of facilitation** rather than **security**.²¹ There is, in fact, **no clearly explained logical connection in the ETIAS proposal between the problem addressed and the measure's objectives**.

Second, the explanation for the reasoning gap in the ETIAS proposal **appears to be the result of legislative inertia and path dependency** rather than a clearly demonstrated necessity for the system. Under his specific remit of data protection, the EDPS notes in his 6 March 2017 opinion that the ETIAS proposal continues a trend whereby 'migration management and security purposes are increasingly associated in the context of granting access to existing systems for law enforcement purposes ... building new information systems ... or extending the competences of an existing body'.²² In framing increased traveller flows across EU external borders as a matter of security rather than facilitation, the European Commission's **ETIAS proposal** extends a rationale it has recently adopted in its proposal for an EU PNR system and its revised proposal for EU smart borders.²³

Finally, the examination of the list of objectives of the ETIAS Regulation **speaks to a broader point, namely that the proposal accumulates objectives. This makes it difficult to ascertain what parts and to what extent the measure is necessary in the first place**. A clearer assessment would be possible if the proposal were to clearly identify and prioritise the areas of public policy it is intended to contribute primarily to and the specific objectives it is designed to meet.

²¹ See, in particular, the reasoning exposed in the Commission communications on border management and smart borders of 2008 and 2011, COM (2008) 69 final and COM (2011) 680 final, op. cit.

²² EDPS (2017), *EDPS Opinion on the Proposal for a European Travel and Information Authorisation System (ETIAS)*. Brussels, Opinion 3/2017, p. 7.

²³ The weakening of the facilitation objective in the 2016 smart borders proposal is documented in Julien Jeandesboz, Jorrit Rijpma and Didier Bigo (2016), *Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal*. Brussels: European Parliament, PE 571.381.

3.3. Substance of the measure

3.3.1. ETIAS structure

The ETIAS proposal foresees the establishment of an information system to:

1. allow and manage travel authorisation applications;
2. automatically screen applications against the data held in several other information systems (EU or international), an ETIAS-specific watchlist and ETIAS-specific risk indicators; and allow for the manual handling of applications rejected in the automated process; and
3. provide access for carriers, law enforcement services of the Member States, and Europol.

To do so, the **structure** of ETIAS consists of three parts (Article 5): the ETIAS Information System (ETIAS-IS), the ETIAS Central Unit (ETIAS-CU), and the ETIAS National Units (ETIAS-NUUs):

- The **ETIAS-IS** (Article 6) includes a Central System, a communication infrastructure so that the Central System can be securely connected to national border infrastructures of Member States (National Uniform Interface), and information systems making ETIAS interoperable. It further consists of the means for ETIAS to interact with applicants (public website and mobile app platform, email service, secure account service) and carriers (carrier gateway), and a web service through which the Central System can connect with the online services required for these interactions with applicants and carriers, including the payment intermediary and international systems (Interpol systems in particular). Finally, ETIAS-IS is comprised of software allowing ETIAS-CU and ETIAS-NUUs to process applications.
- The **ETIAS-CU** (Article 7) is hosted within the EBCG.
- The **ETIAS-NUUs** (Article 8) are competent authorities designated by the Member States. They interact with ETIAS-IS by examining and deciding travel authorisation decisions by means of a manual risk assessment on applications rejected by the automated application process. They interact with Europol and national law enforcement services for requests to consult ETIAS data. Finally, they interact with applicants in the event of an appeal of a negative travel authorisation decision.

The ETIAS structure mimics existing **centralised EU information systems** such as SIS or VIS. What is **notable**, however, is that it is the **first EU information system whose central unit shall be hosted and run by the EBCG**.

3.3.2. ETIAS as an application platform

On the one hand, then, **ETIAS is a platform allowing visa-exempt third-country travellers** (or intermediaries) **to apply** for a travel authorisation by **inputting their personal data** and **paying a €5 fee**. This is done through a public website and mobile app, which also provide applicants with an account service to input additional information and/or documentation, if necessary.

The data applicants (Article 15) must provide is **wide-ranging, including the following:**

1. biographical data, including such things as **the applicant's nationalities** (if more than one) and **the first name(s) of the applicant's parents**;
2. data concerning the travel document;
3. contact details (home address, or at least city and country of residence), email and phone number;
4. socioeconomic data (education level and field, current occupation);
5. Member State of first entry;

6. in the case of applications filled in by a person other than the applicant, biographical details of that person, details of the firm or organization, contact details of the intermediary and relationship to the applicant; and
7. answers to a set of specific questions related to whether the applicant has been subject to any disease with epidemic potential or other infectious or contagious parasitic diseases; his or her criminal convictions; any stays in a specific war or conflict zone over the last ten years and the reasons for the stay; and whether the applicant has been subject to any decision requiring him or her to leave the territory of a Member State or any other country or any return decision issued over the last ten years.

In addition to the active submission of data by the applicant, the ETIAS-IS **will collect the IP address from which the application was submitted**. There is, however, **no explanation** as to **why the IP address should be collected**. The 2016 PwC ETIAS feasibility study notes that collecting IP addresses could be used to geo-locate applicants at the time of application, to run **checks against a list of known 'malicious' IP addresses**, or to **'identify third-parties submitting applications on behalf of travellers'**.²⁴ However, the Commission contractor also notes that IP addresses are not necessarily reliable for these purposes and recommends **that the 'relevance and added value' of such data collection 'be further assessed before deciding in favour of collecting and processing it'**.²⁵

3.3.3. ETIAS as an automatic and manual data processing platform

On the other hand, ETIAS is a platform for **automatically and manually processing** the data applicants submit.

All data submitted to ETIAS is subject to automated processing. This processing takes place **within** the ETIAS central system, which creates an application file after checking that all of the required fields have been filled in and that the travel authorisation fee has been paid. Upon creation of the file, all personal data provided by the applicant is recorded and stored in the system. The ETIAS Central System also checks whether the applicant has an existing application file and, if so, creates a link between applications. After the application file is created, the ETIAS Central System compares the relevant data to the data present in records, files or alerts registered within **nine different information systems** (Article 18): the ETIAS Central System itself, SIS, EES, VIS, Eurodac, ECRIS, Europol data, SLTD and TDAWN (both Interpol systems). It should be noted that when the Commission published the ETIAS proposal (and at the time of writing), the EES legislative proposal was still under discussion by the co-legislators.

If **no hit** is reported, the ETIAS Central System automatically issues a travel authorisation and notifies the applicant. If **a hit is reported**, including if the applicant has responded positively to any of the specific questions asked during the application process, the application is forwarded and **manually assessed by ETIAS-NUs**. If there is a hit but the Central System cannot certify that the data recorded in the application corresponds to the data triggering a hit, the Central System automatically consults the ETIAS-CU.

Manual processing by the ETIAS-CU (Article 20) involves verifying whether the data recorded in the application file indeed corresponds to the data triggering a hit. If this is not the case, the ETIAS-CU will delete the false hit from the application file and the ETIAS Central System will automatically issue a travel authorisation. If the data corresponds or a doubt remains, the application will be manually assessed by ETIAS-NUs (Article 22).

The ETIAS-NUs are responsible for manually processing applications that have triggered one or several hits or ones for which a doubt remains after examination by the ETIAS-CU. The responsible ETIAS-NU is that of the Member State of first entry indicated by the applicant. In

²⁴ PwC (2016), *Feasibility Study*, op. cit., p. 27.

²⁵ Ibid., p. 28.

these cases, they are *in fine* responsible for issuing or refusing a travel authorisation, possibly after requesting (by email) additional information or documentation from the applicant. Manual processing entails the responsible ETIAS-NU having access to the application file (and linked application file(s) if any) and to the hits triggered during the automated processing. The decision-making process in the ETIAS-NU manual processing is as follows:

- if the hit involves the **applicant's travel document as having been** reported lost, stolen or invalidated in the SIS or Interpol SLTD or the applicant having been subject to a refusal-of-entry alert recorded in the SIS [Article 18(2) (a) to (c)], the outcome is systematically **the refusal of a travel authorisation**;
- if the hit concerns other matters, listed in Article 18(2)(d) to (m) as well as 18(3) to (55), the ETIAS-NU conducts a security, health or irregular migration risk analysis to decide whether to issue a travel authorisation.

The responsible ETIAS-NU consults the authorities of other Member States (Article 24) when these authorities were responsible for entering the data that triggered a hit in SIS, VIS, Eurodac, or EES, or when the applicant is found to be subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant. This process is meant to enable the responsible Member State authorities to provide a reasoned positive or negative opinion on the application, which is subsequently recorded in ETIAS.

The outcome of the automated or manual processing of data is immediately notified to the applicant via the email service. Information about the outcome is added in the ETIAS file. Should the outcome be negative [Article 32(2)], the notification includes a reference to the authority that refused the travel authorisation, the grounds for refusal, and information on the appeal procedure. Applicants can also appeal in cases where a travel authorisation is annulled or revoked. Appeals [Article 31(2)] are conducted in the Member State that took the decision on the application and in accordance with the national law of that Member State. Information to the applicant on the procedure to be followed is provided by the ETIAS-NU of the responsible Member State.

3.3.4. ETIAS as a platform for accessing personal data: carriers and law enforcement access

ETIAS should thirdly be understood as a platform for **accessing personal data**. Besides the authorities responsible for handling the functions of the system (ETIAS-CU and ETIAS-NUs, Europol), the ETIAS proposal foresees access to ETIAS data for **private entities (at this stage carriers)** and **public bodies (at this stage border authorities at the external borders and law enforcement authorities of the Member States and Europol)**. When considering ETIAS as a platform for accessing personal data, an additional nuance needs to be stressed. One must indeed distinguish **between access for the simple purpose of verifying whether travellers are in possession of a travel authorisation**, and **access to the contents submitted** by travellers. The first case concerns carriers and border authorities of the Member States, while the latter concerns access by Member State law enforcement authorities and Europol.

Carrier access is established **for the purpose of verifying that third-country nationals subject to the travel authorisation requirement possess a valid travel authorisation** [Article 39(1)] prior to boarding. Access is organised through a carrier gateway over the internet. Consultation of the ETIAS Central System is permitted for carriers using the machine-readable zone of the travel document. Carriers are **exempt from the obligation to verify the possession of a valid travel authorisation where it is technically impossible to do** so because of a failure of the ETIAS-IS or for other reasons outside their control.

Public authority access falls into two categories. Access by **border authorities at the external borders** is allowed 'for the sole purpose of verifying whether the person has a valid travel authorisation' [Article 41(1)]. Access takes place at the time of crossing the EU's

external borders. When it comes to access **for law enforcement purposes**, the ETIAS proposal **continues a trend initiated with VIS and recently continued through the smart borders/EES proposal**, namely providing access to designated Member State law enforcement authorities and Europol to an immigration and border control information system **from the outset** rather than after an evaluation or assessment period.²⁶ Law enforcement access is allowed 'in order to prevent, detect and investigate terrorist offences or other serious criminal offences' [Article 43(1)]. For this to happen, **all** the conditions listed in Article 45 must be met, including necessity, the existence of reasonable grounds, and the fact that the requested information could not be obtained through prior consultation of all relevant national databases and Europol data.

Law enforcement access to the ETIAS Central System is two-tiered. **The first stage involves a hit/no hit search**, limited to searching with specific data items: biographical details, travel document number, home address, email address, phone number and IP address. These items can be combined with three-search criteria to narrow the search: nationality, sex, and date of birth or age range. **In the event of a hit**, the requesting national law enforcement authority may access the data referred to in Article 15(2) (a) to (g) and (j) concerning such things as biographical data, contact details, travel document information and Member State of first entry. **Access to data concerning the applicant's current occupation and applicant answers to questions related to criminal history, stay in a specific war or conflict zone over the last ten years and reasons thereof** [Article 15(2)(i) and (4)(b) to (d)], and decisions requiring the applicant to leave or return decisions **must be justified through a reasoned electronic request subjected to an independent verification**. Likewise, Article 46(1) stipulates that Europol may request access to data stored in the ETIAS Central System on the basis of a reasoned electronic request sent to the ETIAS Central Unit. Europol requests are subject to prior verification by the EDPS, and access to data referred to in Article 15(2)(i) and 15(4)(b) to (d) is only given 'if consultation of the data was explicitly requested by Europol' [Article 46(3)].

3.3.5. ETIAS as a future-oriented, data mining and profiling platform: the ETIAS screening rules and watchlist

Due to the volume of personal data it will process, ETIAS should be conceived of as a **platform for mining and profiling personal data** rather than a platform for issuing automated or manual travel authorisation decisions. In the ETIAS proposal this concerns the establishment of two specific schemes: **ETIAS screening rules** (Article 28) and the **ETIAS watchlist** (Article 29).

The **ETIAS screening rules** are defined as 'an algorithm enabling the comparison between the data recorded in an application file of the ETIAS Central System and specific risk indicators pointing to irregular migration, **security or public health risk**' [Article 28(1)]. An algorithm is a problem-solving procedure; in this case, it is **automated** because it is embodied in a **set of rules that a machine follows in order to reach a particular goal**. The goal, here, is **fundamentally different from the automated screening achieved by allowing ETIAS to search for hits in other information systems**. In the latter case, the goal is to verify whether visa-exempt travellers **are known and reported for documented reasons** by the responsible authorities of the Member States. The **aim of ETIAS screening rules**, however, is **to identify persons who are unknown** to responsible authorities of the Member States but **are assumed to be of interest for irregular migration, security or public health purposes** due to fact that they **display particular category traits**.

The rules would be applied to a dataset consisting of the following:

²⁶ As was originally foreseen, for example, in the initial, 2013 smart borders legislative package. See European Commission (2013), *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*. COM(2013) 95 final, 28.2.2013; Julien Jeandesboz, Didier Bigo, Ben Hayes and Stephanie Simon (2013) *The Commission's legislative proposals on Smart Borders: their feasibility and costs*. Brussels: European Parliament, PE 493.026.

- statistics generated by EES (on 'abnormal' rates of overstayers and refusals of entry) and ETIAS (abnormal rates of refusal of travel authorisation and 'correlations' between information collected through the application form and overstay or refusals of entry); and
- 'information' concerning specific 'risk indicators' on security or threats, rates of overstayers and refusals of entry, or 'specific public health risks'. Migration and security risk information is provided by Member States. Information on public health risk, as defined in Article 2(21) of the Schengen Borders Code, is provided by the European Centre for Disease Prevention and Control.

The 'risks' to be assessed through ETIAS screening rules are not presented in detail the proposal but will be specified through delegated acts that the ETIAS Regulation empowers the Commission to adopt [Article 28(3), referring to Article 78]. The ETIAS-CU would be tasked with establishing specific risk indicators combining some of the data collected through ETIAS, including age range, sex, nationality, country and city of residence, education level, and current occupation [Article 28(4) (a) to (d)]. The ETIAS proposal mirrors the semantics used in the EU PNR Directive by referring to this process as 'assessment'.²⁷ Yet there are good reasons to consider that ETIAS screening rules are best understood as a procedure for **data mining** and **profiling**.²⁸

- **Data mining** is usually understood as 'a procedure by which large databases are mined by means of algorithms for patterns of correlation between data'.²⁹ This is precisely how the ETIAS proposal foresees the use of personal data in the ETIAS Central System. The **term 'correlation' is important** here, reminding us of the fact that **that data which might be related does not indicate causality or reason**.³⁰ The fact that data can be put in relation in a given dataset does not mean that the behaviour of the subjects whose data is being processed or the degree of interest that they represent will be the same.
- **Profiling** is defined in Article 4(4) of the EU General Data Protection Regulation (GDPR) as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.³¹ The GDPR considers profiling problematic when it comes to the right to data protection: Article 22(1) give data subjects the **general right not to be subjected** to it, with exceptions listed in Article 22(2). **ETIAS screening can therefore be characterised as profiling** insofar as the personal data of travellers is subjected to automated processing [by means of the algorithm referred to in Article 28(1)] in order to evaluate whether they present certain features that are assumed to be correlated with certain **security, migration or health 'risks'**.

In this respect, it is reasonable to argue that it is **misleading** to **present this particular aspect of ETIAS as 'screening rules'**. The personal data involved **is not simply screened** against existing lists of known individuals 'of interest' but is **mined** and **profiled** for the purpose of **identifying previously unknown persons** whose characteristics happen to be correlated to indicators deemed relevant.

The second screening scheme established by the ETIAS proposal is the **ETIAS watchlist**. Unlike ETIAS screening rules, which are a set of procedures for **identifying persons previously unknown**, the ETIAS watchlist is **a list of persons**. The watchlist will include 'persons who are suspected of having committed or taken part in a criminal offence', in other

²⁷ Directive (EU) 2016/681, op. cit.

²⁸ Technically, data mining is the first stage of a 'profiling operation'. See Jean-Marc Dinant et al. (2008), *Application of Convention 108 to the profiling mechanism*. Strasbourg: Council of Europe, T-PD(2008)01, 11.01.2008, pp. 3-5.

²⁹ Mireille Hildebrandt (2008), 'Defining Profiling: A New Type of Knowledge?'. In *Profiling the European Citizen: Cross-Disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth, Leiden: Springer, pp. 17-45, at p. 19.

³⁰ Ibid.

³¹ GDPR Article 2(3) states: 'For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98'.

words, **persons who are connected to a pre-existing criminal offence**, and ‘persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences’, in other words, **persons who have not yet committed a criminal offence but are suspected of being likely to do so in the future**. The ETIAS watchlist will be established on the basis of the following:

- information ‘related to terrorist offences or other serious criminal offences provided by Member States’; and
- information obtained through **international channels**, namely the United Nations list of war criminals and ‘information related to terrorist offences or other serious criminal offences obtained through international cooperation’.

Although the ETIAS watchlist consists of the names of persons, in contrast to the ETIAS screening rules that aim to **identify** persons, it is important to note that both are **future-oriented**. Both schemes, in other words, support decision-making on who is authorised to travel to the EU based on what a traveller **might do**, not only what he or she **may have done**. Finally, while ETIAS-CU, that is the **EBCG**, is responsible for establishing ETIAS screening rules, **Europol** is responsible for establishing the watchlist.

Furthermore, the ETIAS proposal leaves a number of questions open regarding the presentation, explanation and establishment of the ETIAS screening rules and watchlist. Regarding the **necessity** of the **ETIAS screening rules**, the European Commission provides no justification as to why, **in addition to automated screening against other EU information systems**, the data held in ETIAS should be subjected to data mining and profiling. The question here is **whether this is proposed for a particular reason or need to act or simply because the volume of data ETIAS will hold happens to allow such processing**. In the latter case, the ETIAS proposal would **embrace profiling by default**.

Likewise, the **necessity** of the **ETIAS watchlist** is unclear. With regard to counter-terrorism, the EU already maintains a counterterrorism watchlist based on Council Common Position 2001/931/CFSP of 27 December 2001 (hereafter CP 931 list) and the UN Security Council Resolution 1373 of 13 September 2001.³² There are at least three unanswered questions here:

- What is the relationship between the ETIAS watchlist and the CP 931 list? **What would the ETIAS watchlist add that is not on the CP 931 list?** As discussed in the next point, the ETIAS watchlist would include names of persons associated with serious and organised crime offences, whereas the CP 931 list is concerned exclusively with terrorism. At the same time, however, **the explanatory statement attached to the ETIAS proposal does not consider the relationship between the two lists when it comes to terrorism (including risks of duplication or mismatch)** and does not discuss the added value of the ETIAS watchlist or options other than the watchlist. This is especially important given that the **Court of Justice of the European Union (CJEU) has questioned the validity of including individuals in the CP 931 list without providing individual, specific and concrete reasons for inclusion**.³³ The CJEU has ruled in the well-known **Kadi cases** that UN Security Council Resolutions should not enjoy primacy over EU law; EU rules implementing UN Security Council Resolutions can be reviewed given that the protection of fundamental rights forms part of the foundations of the EU legal order. In that respect, the Grand Chamber has found that the rights of defence, particularly the right to be heard and of effective judicial review, are not adequately respected when the persons included in the list have not been communicated the evidence used against them to justify the restrictive measures imposed on them or have not been afforded the right to be informed of that evidence within a reasonable period of time after those measures were enacted.

³² Council Common Position of 27 December 2001 on the application of specific measures to combat terrorism. OJEC L344/93, 28.12.2001.

³³ Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Commission and United Kingdom versus Yassin Abdullah Kadi (No. 2)* [2013].

- The phrasing of ETIAS Regulation Article 29(2)(b) and (c) suggests that the ETIAS watchlist would also operate as a watchlist for 'serious criminal offences'. What is the relationship here with, for instance, alerts in the SIS related to these issues? **One would expect a discussion of the lawfulness of such a measure** given that the CP 931 watchlist, by contrast, derives its legitimacy from the fact that it implements a UNSC resolution.
- Lastly, what is the evidence basis underpinning listing decisions on the ETIAS watchlist? The provision of Article 29(2)(c) referring to information obtained through international cooperation is particularly problematic **given the CJEU rulings in the Kadi cases**. There is, on the other hand, no explanation as to why this would be necessary and as to how such information may be vetted by Europol.

3.3.6. Who has authority over ETIAS, and who has oversight? The role of EU agencies and bodies

Given the significant impact of the ETIAS proposal, it is important to map out who would have authority over the foreseen system. This includes **examining and assessing the mechanisms for oversight envisaged in the proposed legislation** in line with recent resolutions from the European Parliament, whose 13 December 2016 resolution states that 'effective democratic oversight of **security measures is essential**'.³⁴ The proposed ETIAS Regulation would give a mandate to three EU agencies: the EBCG to establish and ensure the functioning of the ETIAS-CU and to define ETIAS screening rules; the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) to develop and operationally manage the system; and Europol to participate in the definition of ETIAS screening rules and to manage the ETIAS watchlist.

The mandate given to eu-LISA (Article 63 and 64), relating to both the development and technical management of ETIAS, falls within the remit of **that agency's founding Regulation**. The mandate given to the EBCG (Article 65) **signals the growing role this agency is currently being granted in matters related to internal security and countering terrorism and serious and organised crime**, in accordance with Article 4(a) of the EBCG Regulation defining European integrated border management.³⁵ The EBCG is responsible for the automated processing of applications in the ETIAS system [Article 65(1)(b)], but among **the key features of the EBCG's mandate** is that the agency shall **host** two key bodies for the functioning of ETIAS:

- The **ETIAS Central Unit** (Article 7) is a 24/7 service tasked with ensuring that the data stored in the system is correct and up-to-date. Its remit also includes verifying applications for travel authorisations rejected by the automated process. It is further responsible for defining, testing, implementing, evaluating and revising the risk indicators for ETIAS screening rules. Finally, ETIAS-CU is the audit body for the processing of applications in ETIAS and the implementation of Article 28 provisions (ETIAS screening rules), **including 'regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection'** (emphasis added).
- The **ETIAS Screening Board** (Article 9, ETIAS-SB) is composed of representatives of each ETIAS-NU and Europol. The ETIAS-SB is **an advisory body consulted by the ETIAS-CU** on defining, evaluating and revising specific risk indicators for the ETIAS screening rules and the implementation of the ETIAS watchlist [Article 9(2)(a)(b)].

Concerning **Europol** (Article 67): besides providing the agency with access to ETIAS data, the key outstanding feature of the ETIAS proposal is providing Europol the mandate to establish the ETIAS watchlist (Article 29). The ETIAS Regulation also gives **the European**

³⁴ European Parliament (2016), *European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015 (2016/2009(INI))*. P8_TA-PROV(2016)0485, point M.

³⁵ Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation EC^o No 2007/2004 and Council Decision 2005/267/EC, OJEU L 251/1, 16.9.2016.

Commission a mandate, through the adoption of delegated acts, to specify the irregular migration, security or public health risks required to implement the ETIAS screening rules [Article 28(3)].

When considering organisational authority over ETIAS, **oversight over the screening rules and watchlist should be considered key areas of concern**. Given the future-oriented data mining and profiling components involved, these measures are likely to impact millions of third-country travellers. For **ETIAS screening rules**, the oversight mechanism over the 'rules' themselves (that is, the algorithm) and the 'risk indicators' is rather weak. There **is no oversight regarding the algorithm** to be used by the EBCG. Oversight by an authority other than the European Commission, Europol or the EBCG **with regard to the 'risk indicators'** is contained in **Recital (51) of the ETIAS proposal**. Since these indicators are adopted by means of a delegated act by the Commission, Recital (51) states (with reference to the Interinstitutional Agreement on Better Law-Making of 13 April 2016) that 'to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts'.³⁶ Article 78 further specifies the conditions under which this power is exercised and how it can be revoked. In the meantime, the **ETIAS-CU is charged with auditing its own implementation of Article 28, including the impact of ETIAS screening rules on fundamental rights**. This provision means that the **ETIAS-CU and the EBCG are given the responsibility to self-monitor** the operation of ETIAS screening rules. **No separate authorities or other EU bodies are involved** since the ETIAS Screening Board only consists of representatives from Europol and ETIAS-NUs. The same observation applies to the ETIAS watchlist, which **Europol is given the sole responsibility to implement**, with no possible oversight from the European Parliament or the Council: since the implementation does not involve delegated acts, no oversight from independent authorities or other EU bodies is possible.

3.4. Assessing the case for ETIAS: evidence basis and demonstrated necessity of the measure

Assessing the evidence basis for ETIAS requires considering and answering three separate questions. Firstly, how was evidence collected by the European Commission in preparing the proposal and what quality of evidence was available? Secondly, to what extent does the available evidence support or contradict the policy option eventually adopted by the Commission? Finally, are there alternative measures to the chosen policy option? It is only after examining these issues that the case for the necessity and proportionality of the proposed measure can be assessed.

3.4.1. The evidence gathering process for the ETIAS proposal

It is first important to stress that the **ETIAS proposal is not accompanied by a Commission-produced impact assessment document** considering different policy options available to achieve the proposal's stated objectives or its relationship with other instruments in the same policy areas. The EDPS has made the same observation with regard to the lack of a data protection impact assessment, which he notes is a 'fundamental prerequisite'. **This has recently been confirmed by the European Parliament, whose 13 December 2016 Resolution states 'that fundamental rights should be included as part of the impact assessment for all legislative proposals'**.³⁷ The conclusion of the EDPS's opinion with regard to data protection aspects is likely to apply more generally here, namely that the lack of an impact assessment document 'does not make it possible to fully

³⁶ Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making of 13 April 2016, OJEU L 123/1, 12.5.2016.

³⁷ P8_TA-PROV(2016)0485, op. cit., point 10.

assess the necessity and proportionality of ETIAS as it is currently proposed'.³⁸ According to the 'Better Regulation Guidelines' adopted by the European Commission in May 2015, an impact assessment is not a systematic requirement: adjustments can be made in cases where there 'may be a **political imperative** to move ahead quickly, an **emergency** that requires a rapid response, or a **need to abide to specific timeframes set in legislation**'.³⁹ In the case of the ETIAS proposal, this does not seem to hold:

- The **Commission does not seem to consider the situation an emergency**, since the measure is presented as anticipating a situation that could arise **after 2020**.
- There is no binding timeframe set in the legislation.
- There is **political momentum** due to the rapid adoption of the European Agenda on Security, the communications of April and September 2016 on border security in response both to the tragic series of attacks in EU Member States since the beginning of 2015, and political tensions over the refugee crisis. At the same time, **ETIAS is one of many measures** considered, proposed and adopted in relation to these matters, so **its status as a political imperative may well have to be substantiated further in order to justify the lack of a documented impact assessment effort**.

In the meantime, the Commission's 'Better Regulation Guidelines' stress that an impact assessment 'is **required** for Commission initiatives that are **likely to have significant economic, environmental or social impacts**'.⁴⁰ This commitment from the European Commission to the co-legislators is enshrined in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.⁴¹ A **measure concerning all visa-exempt travellers to the EU and envisaging the mass, automated processing of their personal data** might be considered to fall within this category.

Most of the evidence provided in the explanatory statement of the ETIAS proposal, secondly, comes **from three main sources**: the February 2011 **PwC study** on EU-ESTA, the October 2014 **PwC 'Technical Study on Smart Borders'** and the November 2016 **PwC feasibility study** on ETIAS.⁴² It is important to note that the latter is **not an impact assessment but a feasibility study**: its **focus** is understandably **on whether ETIAS is feasible**, not on **what its impact would be**. The Commission indicates that additional consultations took place with interested parties, including HLEG, representatives of the passenger carrier industry, and EU Member States with land borders.⁴³ From the point of view of evidence gathering, then, a first observation here is that **all the impact assessment work has been undertaken by a single contractor**, who additionally was asked to assess the **feasibility** of ETIAS, **not its impact**. While PwC's past work for the European Commission on EU-ESTA and likeminded proposals suggest that it may have some expertise in the area of technology consulting, the contractor may not be a specialist in human rights. It is understood that the European Commission informally consulted FRA and the EDPS. In his opinion on ETIAS, however, the EDPS notes that 'due to the very tight deadline and the importance and the complexity of the proposal, it was not possible to provide a meaningful contribution at that time'.⁴⁴ Further consultation with other relevant stakeholders such as the FRA, civil society and experts would help to establish a clearer picture of the **proposal's** potential impact.

3.4.2. Quality of evidence for the ETIAS proposal

The assessment of the evidence gathering process for the proposal is compounded by the fact that the **quality of evidence does not always appear to be of the highest**

³⁸ Opinion 3/2017, op. cit., p. 7.

³⁹ European Commission (2015), *Commission Staff Working Document: Better Regulation Guidelines*. SWD(2015) 111 final, p. 4 (emphasis added).

⁴⁰ Ibid., p. 17 (emphasis added).

⁴¹ Interinstitutional Agreement of 13 April 2016 on Better Law-Making, op. cit., point 13.

⁴² PwC (2014), *Technical Study on Smart Borders – Final Report*. Luxembourg: Publications Office of the European Union.

⁴³ COM (2016), 731 final, p. 16-17.

⁴⁴ EDPS (2017), *EDPS Opinion*, op. cit., p. 6.

standard. Box 1 below provides an example on the reported number of travellers affected by the measure. **This is relevant because, as the Commission notes, it is essential to demonstrating the necessity of the measure:** 'These figures **demonstrate the need** to put in place a system that is able to achieve objectives similar to the visa regime, namely to assess and manage the potential irregular migration and security risks represented by third country nationals visiting the EU'.⁴⁵

Box 1: How many people would be affected by the proposed ETIAS measure?

In the explanatory statement accompanying the ETIAS proposal, the Commission reports the following figures: '**1.4 billion people** from around 60 countries' can benefit from visa-free travel to the EU today, with 'an expected increase of **30%** in the number of visa exempt third country nationals crossing the Schengen borders **by 2020**, from **30 million in 2014** to **39 million in 2020**'.⁴⁶

To ascertain the necessity of the ETIAS measure, first, the figure of 1.4 billion third-country nationals benefitting from visa-free travel to the EU would have to be contextualised. **This is not the actual number of travellers coming into the EU today.** The figure appears to be an approximation provided by the contractor for the ETIAS feasibility study, with PwC reporting a figure of **over 1.2 billion** visa-exempt third-country nationals as of October 2016.⁴⁷ This is, in fact, the **total population of the countries** listed in Annex II to Council Regulation (EC) No 539/2001. These are, indeed, all **potential** visa-exempt travellers, but there is no evidence to determine what proportion of this total population would be **actual** travellers.

A similar exercise can be performed for the figure reported in the ETIAS proposal of 30 million crossings of the EU external borders by visa-exempt third-country nationals in 2014, expected to increase to 39 million in 2020. It is important to underline that there is **currently no separate, systematic recording of border crossings by visa-holding and visa-exempt third-country nationals.** As such, the figure **does not come from the feasibility work conducted for the ETIAS proposal** but from a study undertaken (again by PricewaterhouseCoopers) on another proposed measure, the 'smart borders package'.⁴⁸ The figure is an **estimate based on a seven-day data gathering exercise (18-26 May 2014)** by all current Schengen Member States and four non-Schengen EU Member States. The results of this data gathering were **extrapolated for a full calendar year**, and an annual growth rate of 4.2% was used to **further extrapolate estimates** for 2020 (and up to 2025). The contractor, without further elaboration, reports that this growth rate was 'based on consultation with various sources'.⁴⁹

The difficulty of generating appropriate and accurate evidence should be acknowledged. In parallel, however, the difficulty of ascertaining the actual number of people who would be affected by ETIAS remains; **whether the increase in this number makes the measure necessary** should be addressed before considering its adoption.

⁴⁵ COM (2016), 731 final, p. 2.

⁴⁶ Ibid., p. 6 (emphasis added).

⁴⁷ PwC (2016), *Feasibility Study*, op. cit., p. 9.

⁴⁸ PwC (2014), *Technical Study*, op. cit., pp. 20-22.

⁴⁹ Ibid., p. 20.

Another issue for the quality of evidence supporting the demonstrated need for ETIAS concerns the **scope of the evidence gathering conducted by the contractor**. As reported **by PwC** in the **2016 feasibility study**, the following elements were considered outside the scope of the study:

- other policy options than ETIAS in its current form, **including the 'use of existing systems for the purpose'**;
- **'detailed legal and fundamental rights analysis** (high-level/principles only)';
- with regard to border-crossing processes, the issue of second-line border checks and differences of control requirements for specific border-crossing points;
- with regard to advantages and disadvantages for stakeholders, a Member-State by Member-State impact assessment.⁵⁰

It is not possible to establish whether these limitations were included in the initial terms of reference of the feasibility study or whether they are the result of a subsequent exchange of views between the Commission and the contractor. In the meantime, the first two scope limitations indicate the difference between a feasibility study and an impact assessment for the purpose of evidence-based policymaking. **An impact assessment on a measure that both the contractor and the Commission had previously agreed should be shelved because it would entail a significant interference in fundamental rights would be expected to include, at a minimum, a fundamental rights analysis.**

In addition, **the lack of impact assessment means that the co-legislators, other stakeholders and the general public may not necessarily receive the appropriate information as to whether other options than the scenario apparently favoured by the European Commission are available.** As discussed in **Box 2** below, even within the parameters identified by the European Commission, **the ETIAS proposal bundles together a set of measures that are supplemental to one another rather than essential**; these measures could be envisaged as alternative policy options.

Box 2: Considering alternative ETIAS policy options

As it currently stands, the ETIAS proposal combines a set of measures that are supplemental rather than essential to one another. As discussed above, one can distinguish between, firstly, ETIAS as a platform for individuals to apply for a travel authorisation and for processing and accessing application data, and, secondly, ETIAS as a platform for mining and profiling the personal data submitted as part of the application. As such, removing the provisions regarding ETIAS screening rules and the ETIAS watchlist would not compromise the functioning of ETIAS as an authorisation platform where the data of visa-exempt third-country nationals is checked against existing information held in other EU information systems. Likewise, ETIAS could function as an authorisation platform without law enforcement access, except for access by border authorities at the external borders [Article 41(1)].

The policy options for ETIAS could be broken down as follows.

Option 1: ETIAS without the ETIAS screening rules, the ETIAS watchlist, and Europol and law enforcement access [save for border authorities under the current Article 41(1)]. This option would have the advantage of allowing for further data minimisation, since some items of biographical and socioeconomic data as well as the collection of the IP addresses would be mostly useful for data mining and profiling purposes. Sub-options to be

⁵⁰ PwC (2016), *Feasibility Study*, op. cit., p. 119. Emphasis added in excerpts below.

considered here could involve removing health-related questions. This would minimise the severity of the infringement upon fundamental rights as well.

Option 2: ETIAS without screening rules or the ETIAS watchlist but with Europol and law enforcement access. In this case, the possibility of data minimisation mentioned above would still exist. This option would remove some of the issues raised by the ETIAS watchlist outlined above.

Option 3: ETIAS without the ETIAS screening rules, but with the ETIAS watchlist and Europol and law enforcement access. The ETIAS screening rules, as argued above, are essentially a procedure to mine and profile the personal data of applicants and, as such, they constitute a particularly severe interference with the right to data protection and the right to privacy. Option 3, together with Option 1 and Option 2, would limit the extent of this interference.

Option 4: ETIAS with the ETIAS screening rules, watchlist and law enforcement access. This is the current, single option in the proposal by the European Commission. It would still be conceivable, in this option, to remove the provisions for law enforcement access, although Europol would have to be granted some kind of access due to their responsibility for creating and maintaining the ETIAS watchlist.

3.4.3. Questions requiring further evidence to establish necessity in the ETIAS proposal

Because of these gaps, it is impossible to assess whether the policy option proposed by the Commission is supported by sufficient evidence. Likewise, it is not possible to assess alternative options, **including the 'no ETIAS' option**, because these are not examined or mentioned either by the contractor or by the explanatory statement of the ETIAS proposal. It is, however, possible to outline several key questions that require further evidence and discussion related to the **measure's objectives and the problems** it is expected to address.

First, what is the evidence that third-country nationals **present a particular irregular migration risk**? The rationale for the ETIAS proposal highlights concerns that visa-exempt third-country nationals constitute an irregular migration risk because at the present time they are not subject to any check prior to their journey (unlike visa-holding third-country nationals, who are subject to a risk assessment in the visa application procedure). The ETIAS proposal states that in 2014 **about '286,000 third-country nationals were refused entry at the external borders of the EU-28'**, with a fifth of these rejections coming from the lack of a valid visa and the rest **due to 'a negative assessment of the migration and/or security risk represented by the third-country national'**.⁵¹ Yet as PwC reported in a footnote in the 2016 ETIAS feasibility study, **'reliable information** distinguishing between visa-holder and visa-exempt third-country nationals is **not available'**.⁵² In other words, it is **not possible to determine how many of the 286,000 third-country nationals mentioned by the ETIAS proposal are visa-exempt travellers** and whether they represent **a sizeable enough share of this group to make the measure strictly necessary**. The figures reported by Frontex/EBCG in its 2016 annual risk analysis report show, on the other hand, the following:

- Most **illegal border crossings** concern third-country nationals who are **not visa exempt**.
- **Out of the top ten nationalities for which refusals of entry** were reported at the external borders in 2015, **24% of all refusals of entry** came from five countries listed in Annex II to Council Regulation (EC) No 539/2001 (Albania, Serbia, Bosnia and

⁵¹ COM (2016), 731 final, op. cit., p. 3.

⁵² PwC (2016), *Feasibility Study*, op. cit., p. 10 (emphasis added).

Herzegovina, Brazil); **45%** of all refusals of entry came from six countries if the Ukraine were added to that list of five.⁵³

- The **top ten nationalities** for which **detections of illegal stay** were reported, however, **do not include any country listed in Annex II to Council Regulation (EC) No 539/2001**.
- Commenting on the granting of visa-free travel to Colombian and Peruvian nationals, in the meantime, Frontex registers no particular concern, stressing that **'the risks arising from a visa waiver for Colombian and Peruvian citizens will likely remain modest and concern mostly drug trafficking and trafficking in human beings. As in other visa liberalisation cases, passenger flow and refusals of entry are likely to increase'**.⁵⁴ It stands to reason that visa liberalisation leads to increased traveller flows and a correlated increase in the number, but not necessarily proportion, of refusals of entry, but **it is unclear from the evidence submitted by the Commission that this constitutes a problem making ETIAS necessary**.⁵⁵

The **strict necessity** of adopting, out of a primary concern with irregular migration, a measure as far-reaching in terms of data processing as ETIAS is therefore, based on the evidence currently provided by the European Commission and its contractor, **unclear and in need of further demonstration**.

Second, what is the evidence that visa-exempt third-country nationals **present a particular security risk when it comes to terrorism or serious and organised crime**? The rationale for ETIAS is that there is an 'information gap' on this group of travellers. **An 'information gap', however, does not constitute a security risk per se**. References to this information gap serve to make the case for the necessity of ETIAS as a whole and for justifying law enforcement access. Setting up ETIAS, according to the European Commission,

will reinforce EU internal security in two ways: first, through the identification of persons that pose a security risk before they arrive at the Schengen external border; and second, by making information available to national law enforcement authorities and Europol, where this is necessary in a specific case of prevention, detection or investigation of a terrorist offence, or other serious criminal offences.⁵⁶

The explanatory memorandum of the ETIAS proposal refers to the 'series of terrorist attacks' that the EU has faced in recent years **but fails to provide any concrete evidence that visa-exempt third-country nationals are of particular concern in countering terrorism (or serious and organised crime)**. While it is logical that ETIAS data might in some cases **prove useful** for law enforcement services, the **strict necessity** of the measure with regard to the objective of enhancing the security of EU citizens is **unclear and remains to be demonstrated**.

With regard to both irregular migration and security risks, the European Commission notes in the explanatory statement of the ETIAS proposal that both Europol and EBCG risk assessments 'confirm the existence of these risks from both an irregular migration and from a security point of view'.⁵⁷ **This statement is not accurate** in the sense that **neither EBCG nor Europol have provided evidence to the effect that visa-exempt third-country nationals are of particular concern in their operations**. As demonstrated above, the EBCG risk assessment is inconclusive with regard to irregular migration. **Europol's European Union Terrorism Situation and Trend Report 2016, cited as a source by the European Commission, does not record a particular concern with visa-exempt**

⁵³ On 2 March 2017, EU ambassadors have confirmed on behalf of the Council the agreement that had been reached between the Maltese Presidency and the European Parliament on visa-free travel for Ukrainian citizens for short stays. See Council of the EU (2017), *Visas: Council confirms agreement on visa liberalisation for Ukrainians*. Press Release 98/17, 02.03.2017.

⁵⁴ FRONTEX (2016), *Risk Analysis for 2016*. Warsaw: FRONTEX, 3.2016, p. 22.

⁵⁵ All figures taken and calculated from the annexed tables in FRONTEX (2016), *Risk Analysis for 2016*, op. cit.

⁵⁶ COM (2016), 731 final, op. cit., p. 4.

⁵⁷ Ibid., pp. 3-4.

third-country travellers but rather with EU nationals identified as 'foreign terrorist travellers' to Syria and Iraq. It **also explicitly stresses that while 'some terrorist incidents have been identified involving terrorists who have made use of migratory flows to enter the EU', there is 'no concrete evidence to date that terrorist travellers systematically use the flow of refugees to enter Europe', continuing to add that there is no documented link between (irregular) migration and terrorism.**⁵⁸

Third, **would ETIAS constitute a facilitation measure** for third-country nationals? Travel facilitation is presented in the 2016 ETIAS feasibility study as a 'secondary purpose' of the measure (irregular migration and security being the primary purposes) and is part of the rationale detailed by the European Commission for ETIAS.⁵⁹ The measure would constitute 'a significant improvement for travellers compared to the current state of play' because travellers 'would have a reliable early indication of admissibility into the Schengen area'. As such, ETIAS would also 'substantially reduce the number of cases of refusals of entry at the border crossing points' because it is assumed that travellers who have not received an authorisation will not undertake a journey. **This claim contradicts the findings of the previous 2011 PwC study on EU-ESTA**, which states that 'the system would impose a constraining pre-travel requirement upon travellers previously not submitted to any such requirement ... unless the implementation of an EU-ESTA would be accompanied by a lightening or even lifting of border checks'.⁶⁰ Since the overall functioning of ETIAS is similar to the policy option analysed by the contractor in 2011, **there is no reason to consider that the original assessment should be different today**. Furthermore, and as indicated above, **there is no evidence that visa-exempt third-country nationals are more or equally likely than visa-holding third-country nationals to be refused entry at the EU's external borders**, which makes it difficult to endorse the framing of ETIAS as a facilitation measure. Finally, if we consider ETIAS as a 'visa-light' authorisation procedure, there is **no evidence that persons who have no authorisation or have not been authorised to travel are less likely to undertake their journey than people who do not hold a visa or whose visa has expired or been annulled**. For example, a 2011 report by the United States Government Accountability Office (GAO) found that in 2010:

- about **2 percent** (364,086 travellers) **of all passengers travelling under the VWP 'were boarded without verified ESTA approval'**
- for those boarding without verified ESTA approval, 'no ESTA application had been recorded' for 99.8 percent, while the remaining 0.2 percent (648 travellers) had been denied an ESTA.⁶¹

Fourth, does ETIAS constitute **a risk for the international relations of the EU**? The issue is not actually addressed in the ETIAS proposal. The 2011 study on EU-ESTA, however, refers in passing to the fact **that such a system could end up 'creating a risk for the EU's international relations'**.⁶² This is particularly the case given the insistence, documented above, that ETIAS is needed in a context where visa liberalisation is expanding. What ETIAS purports to do is to introduce a visa-like, albeit a visa-light, procedure for travellers who had not faced such requirements before. The introduction of ETIAS in relation to the expansion of visa liberalisation may well suggest **that the EU considers the newly visa-exempt travellers as less trustworthy than nationals of countries who have traditionally benefitted from such a provision**. This appears to be especially the case as visa liberalisation is extended to less affluent parts of the world. **In order to strengthen the evidence basis on the necessity of ETIAS, it would therefore be relevant to consult**

⁵⁸ Europol (2016), *European Union Terrorism Situation and Trend Report 2016*. The Hague: European Police Office, p. 7 (emphasis added).

⁵⁹ COM (2016), 731 final, op. cit., p. 4.

⁶⁰ PwC (2011), *Policy study*, op. cit., p. 200.

⁶¹ GAO (2011), *Visa Waiver Program: DHS Has Implemented the Electronic System for Travel Authorization, but Further Steps Needed to Address Potential Program Risks*. GAO-11-335, 4.2011, p. 18.

⁶² PwC (2011), *Policy Study*, op. cit., p. 291.

with relevant EU services, in particular the EEAS, and with third-country diplomatic representations to the EU.

4. ETIAS: STREAMLINING INTEROPERABILITY IN THE SECURITY UNION

KEY FINDINGS

- The ETIAS proposal **does not foresee detailed rules** on how interoperability will be ensured, which model will be preferred and how it may be embedded in ETIAS.
- The implications of interoperability to the fundamental rights of individuals will be magnified in comparison to the current compartmentalisation of databases; the **specific purpose(s) for which a system was set up will be nullified**; and there is a risk of **extensive profiling**, as authorities may be able to compile a profile of travellers on the basis of information from different systems, with the result that individual rights and supervision may be more difficult to be exercise.
- The forthcoming ETIAS Regulation foresees, **without a proper and necessary impact assessment** of the privacy and data protection implications, the introduction of interoperability of existing and new large-scale information systems **through the back door**.

4.1. Interoperability of information systems: a walk down memory lane

A key component of the ETIAS proposal is its interconnection with other information systems, or in EU terms, its **interoperability** with existing (but arguably also future) law enforcement and border management information systems. This is not a new concept, as debates on interoperability first started in the aftermath of 9/11,⁶³ with a key issue being whether the then-negotiated VIS could be linked or incorporated into SIS.⁶⁴ After the Madrid bombings, the European Council's Declaration on combating terrorism invited the Commission to submit proposals for enhanced interoperability between SIS II, VIS and Eurodac. The Commission has defined **interoperability as the 'ability of information and communication (ICT) technology systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge'**.⁶⁵ However, details on the legal aspect for the interoperability of databases have rarely been mentioned, making the concept a technical rather than a legal or political matter.⁶⁶

While interoperability has been discussed for years, albeit in a sporadic manner, there have been few concrete proposals on the subject.⁶⁷ Since the Paris attacks on 13 November 2015, connecting 'data pots' has gained fresh impetus. The European Council's Conclusions of 18 December 2015 clearly refers to the need to ensure interoperability of all relevant systems

⁶³ Council, Document 13176/01 (24.10.2001).

⁶⁴ European Commission (2001), *Development of the Schengen Information System II*, COM(2001) 720 final, 18.12.2001, p. 8.

⁶⁵ European Commission/IDABC (2004), *European Interoperability Framework for Pan-European e-Government Services* (Luxembourg: Office for Official Publications of the European Communities), p. 5.

⁶⁶ For a critique, see Paul De Hert and Serge Gutwirth (2006), 'Interoperability of Police Databases within the EU: An Accountable Political Choice?', *International Review of Law Computers & Technology*, 20: 1-2 (March-July): 21-35; and EDPS, 'Comments on the Communication of the Commission on interoperability of European databases', 10.03.2006, at

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf; accessed 17 March 2017.

⁶⁷ See, for instance, Council, Document 6975/10 (01.03.2010), point 20, p. 7.

to ensure security checks.⁶⁸ After the Brussels events on 24 March 2016, Justice and Home Affairs Ministers adopted at their extraordinary meeting a Joint Statement which treated interoperability as a matter of urgency.⁶⁹ Indeed, in its Communication on stronger and smarter borders, the Commission identified four different models of interoperability. These correspond to a gradation of convergence among the systems:

- a single search interface to query several information systems simultaneously and to produce combined results on one screen;
- interconnectivity of information systems, so data registered in one system may automatically be consulted by another system;
- establishment of a shared biometric matching service in support of various information systems; and
- common repository of data for different information systems (core module).

While the political drive to interconnect existing and forthcoming systems is evident, there has been no impact assessment on privacy and data protection.

Instead, a High Level Expert Group on Information Systems and Interoperability (HLEG) has been set up to address the legal, technical and operational aspects of the different options, including the necessity, technical feasibility and proportionality of available options and their data protection implications.⁷⁰ The emphasis on interoperability is clear: the sub-group dealing with interoperability has already met three times, whereas the sub-groups on existing or new systems have met a total of three times.⁷¹ The HLEG final report was released on 5 May 2017, whereby the aim of ensuring interoperability is scrutinised extensively.⁷² In particular, it is explicitly stated that it is necessary and technically feasible to work towards the development of a European search portal (option 1), a shared biometric matching service (option 3) and a common identity repository (option 4). Option 2 involving interconnectivity of systems is envisaged to be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system.⁷³ Taking into account the discussions prior to the release of the final report, this finding comes as no surprise, however, it is striking that interoperability is now a given, and the convergence between immigration –or, in EU terms, border management- systems and security databases are merged in a confusing manner.

In the meantime, Member States have agreed in the Roadmap to enhance information exchange and information management by implementing the first option as a matter of priority, with the remaining options to be discussed in the medium and long term.⁷⁴ With the undertone for future development all too apparent, a convergence between criminal law and immigration control systems seems to be in the making. Although the Roadmap refers to all information systems in the Area of Freedom, Security and Justice related to both immigration and law enforcement, it explicitly states that the interlinkages between all different information exchange schemes will be **highlighted, which 'will contribute to ensuring the cooperation between the authorities and agencies ... and the interoperability between information systems'**.⁷⁵ It must be noted that the latter is already embedded in the EES and revised Eurodac proposals, despite the lack of an impact assessment and a comprehensive evaluation of the necessity and proportionality of such interoperability. On the one hand, the EES proposal prescribes interoperability between the EES and the VIS in the form of direct communication and consultation.⁷⁶ Such interconnection is meant to enable border control authorities using the EES to consult the VIS for a series of functions such as a) retrieving and

⁶⁸ Council, Document EUCO 28/15 (18.12.2015), point 3.

⁶⁹ Council, Document 7371/16 (24.03.2016), point 5.

⁷⁰ Commission Decision of 17 June 2016 setting up the High Level Expert Group on Information Systems and Interoperability (2016), OJ C257/3.

⁷¹ Interim report by the chair of HLEG (December 2016), p. 2.

⁷² Final report by the HLEG (May 2017).

⁷³ Ibid. p. 40.

⁷⁴ Council, Document 9368/1/16 (6.06.2016), p. 5; also see Council, Document 7711/16 (12.04.2016).

⁷⁵ Council, Document 9368/1/16 (6.06.2016), p. 4.

⁷⁶ For a discussion on interoperability prior to the EES proposal of 2013, see Council, Document 13801/13 (19.09.2013).

importing visa-related data to create or update the individual file, including in cases where a visa is annulled, revoked or extended; b) verifying the authenticity and validity of a visa or whether the conditions of entry are met; c) verifying whether a visa-exempt third-country national has been previously registered in the VIS; and d) verifying the identity of a visa holder through fingerprinting. Furthermore, border control authorities using the VIS may be able to directly consult EES data when examining visa applications, whereas visa authorities may be able to update the visa-related data in the EES in the event that a visa is annulled, revoked or extended.⁷⁷ On the other hand, the revised Eurodac shall be established in a way that allows for future interoperability with other databases without, however, explaining the model that may be adopted.⁷⁸ In both cases, the proposals seem to pre-empt future developments without a proper assessment of their impact. As a matter of fact, the Commission is set to adopt a proposal specifically on interoperability by late June 2017. At the same time, a Communication addressing the HLEG final report is also expected to be released.

4.2. Interoperability in the ETIAS proposal: inserted through the backdoor with minimum scrutiny

The proposal on ETIAS fits well within this worrying trend of interoperability for information systems, with the 2016 PwC Feasibility Study calling the proposed database **'a catalyst for greater interoperability of information systems in the area of borders and security'**.⁷⁹ With the proposal requiring the automated processing of existing border management and law enforcement information systems, the 'general principle [is] that ETIAS is built on the interoperability of information systems to be consulted (EES, SIS II, VIS, Europol data, Eurodac and ECRIS) and on the re-use of components developed for those information systems, the EES in particular'.⁸⁰ This link between the EES and ETIAS is particularly interesting in that both systems are primarily targeted at monitoring the movement and assessing the risk of visa-exempt third-country nationals, who currently do not fall within the remits of any operational large-scale database. It is true that the EES will also register the entry and exit of visa holders, however, the primary target is to fill **in the 'information gap'** that exists through the lack of centralised information for visa-exempt nationals. To that end, the connectivity is reflected in Article 10, which justifies interoperability as a means **'to enable carrying out the risk assessment'**. However, **the proposal does not specify any rules on how interoperability will be ensured, which model will be preferred and how it may be embedded in ETIAS.** The lack of detailed rules on interoperability seems to counter the **legality principle (the 'in accordance with law' criterion)**, as individuals may not be able to foresee how their data may be used in the future and for what purposes. **The proposal's** vague and laconic wording seems to foster the idea that the policy choice may be to adapt information systems in the future on the basis of the US model so as to fully interconnect the systems through the introduction of a common data repository. A few more details are provided in the feasibility study, which states that ETIAS shall contribute to stages (i), (ii) and (iv) outlined in the Commission communication on stronger and smarter information systems for borders and security.⁸¹ In this respect, it is stated that the ETIAS will allow simultaneous queries across all relevant European systems in the field of border management **and security and international databases. Importantly, 'this component could be reused by Member States in the future, thus realizing the occurrence of the "Single search interface" ambition'**.⁸² Furthermore, in line with the idea of exploiting the systems already in place, ETIAS will allow for interconnectivity. However, greater convergence can also be seen with the EES. As noted in the **proposal's explanatory memorandum**, the EES and ETIAS, which are designed to insert double-monitoring of visa-exempt third-country nationals, would share

⁷⁷ Commission, 'EES proposal of 2016', recital 13 and article 7.

⁷⁸ Commission, 'Eurodac proposal of 2016', p. 5.

⁷⁹ PwC (2016), *Feasibility Study*, p. 59.

⁸⁰ COM (2016), 731 final, p. 15.

⁸¹ PwC (2016), *Feasibility Study*, p. 59

⁸² Ibid.

a common repository of personal data of third-country nationals. Additional data from the ETIAS application (namely residence information, occupational and educational status, answers to background questions and IP address) and the EES entry-exit records would be separately stored but linked to a shared and single identification file.⁸³ There is no reference as to the possibility of the border guards not to see the whole content of the single identification file, therefore, it appears that the border guards shall be able to simultaneously see and consult the data stored both sets of personal data.

Although the Commission underlines that **'this approach is fully in line with the interoperability strategy proposed in its Communication on a Stronger and Smarter Information Systems of April 2016'**, it must be stressed that **interoperability between systems is essentially inserted through the back door, since no proper assessment of the fundamental rights concerns** (in relation to privacy and data protection, in particular, but also discrimination) **has been conducted so far. The delivery of a detailed impact assessment has been substituted by the work of the HLEG, which was set up to implement EU strategy rather than question its necessity and proportionality or assess its potential impact.** On the specific point of interlinking the EES and ETIAS, it must be further highlighted that the proposal entails a remarkable fast-forward to the fourth stage of interoperability, thus bypassing the previous stages. Given that the previous stages of interoperability have not been implemented, tested or evaluated yet, the lack of an impact assessment, both in relation to the ETIAS and the issue of interoperability as such, raises even greater concerns. Even the HLEG, in its interim report of December 2016, states that the necessity and proportionality of introducing a common repository of data are still undetermined. It proposes to **'explore, together with the European Data Protection Supervisor and the Fundamental Rights Agency, the data-protection implications of the establishment of a common repository of data'**.⁸⁴ In the case of ETIAS, this pronouncement undoubtedly sits at odds with putting the model in practice, questioning all the more the policy choices in the ETIAS proposal.

Ensuring the interoperability of ETIAS in a rather intrusive form **is likely to pre-empt the staging of discussions on the data protection implications of interoperability in relation to other information systems.** It may well **undermine the work currently undertaken by HLEG** in coordination with the EDPS and FRA and **eventually legitimise the principle of interoperability without proper scrutiny.** The ETIAS thus becomes a Trojan horse: not only does it introduce what may be a further layer of mass-scale information collection and further processing of data from visa-free third-country nationals, it may also have significant general implications for interoperability in the long term. The interconnection of systems, even if they were established for different purposes and with specific legal bases, may become the norm. This is a genuine risk rather than rhetoric; the introduction of specific features in proposed information systems was heavily influenced by the fact that existing ones had already incorporated those features. This can be seen with law enforcement access to immigration databases, whereby access by law enforcement authorities and Europol to the VIS seems to have influenced the decision to grant access by law enforcement authorities to Eurodac and the EES (and now ETIAS in its proposed form), to say nothing of the routine registration of biometric identifiers (fingerprints and photographs).

The **proposal's explanatory memorandum** claims that this feature will have significant savings for the set up and operation of ETIAS.⁸⁵ At the same time, there is no reference to the far-reaching implications of interoperability on the protection of fundamental rights, particularly privacy and data protection. Similarly, as highlighted above, the feasibility study on ETIAS is not geared towards analysing the compliance of the system with fundamental rights but proposes technical solutions to ensure the fulfillment of the aims of interoperability as

⁸³ COM (2016), 731 final, p. 15.

⁸⁴ High Level Expert Group, Interim Report, p. 11.

⁸⁵ Ibid.

prescribed by the Commission.⁸⁶ Therefore, interoperability seems to be considered a merely technical matter, thus demonstrating years after its original conceptualisation that it remains depoliticised.

Nevertheless, interoperability could be seen as the first step towards a gradual transition from a compartmentalised system of independent databases to a single EU information system. This would go counter to the paradigm of compartmentalisation, which was originally preferred as a policy option in order to ensure the protection of fundamental rights, particularly privacy and data protection. Furthermore, interoperability significantly enhances the EU's monitoring powers by nullifying the limited purposes for which databases were set up. **In that sense, interoperability 'disrespects the importance of separated domains and cuts through their protective walls', violating the purpose limitation principle, one of the core principles of data protection law.**⁸⁷ National authorities may be able to **draw very precise conclusions on the private lives of individuals whose data are inserted in the system, although these persons would not have been able to foresee the potential use of the collected information.** For instance, the level of integration between the EES and ETIAS envisaged in the proposed Regulation seems to suggest that a wide range of personal information from visa-exempt travelers shall be made available to national border and migration authorities (especially the ETIAS-NUs), national law enforcement authorities, the EBCG Agency and Europol. This goes beyond the list of prescribed data in either the EES or the ETIAS Regulation. Making EES and ETIAS interoperable to the extent that there is a common repository of personal data leads to the emergence of what is essentially a separate third database holding a variety of information on visa-exempt applicants ranging from biographical data, biometrics, occupational status, education, IP address and passport information. Furthermore, through the aggregation of information from different systems within ETIAS, the latter database becomes a powerful system combining a wealth of existing information on individuals.⁸⁸ In this respect, the nature and purpose of existing information systems may significantly change without a proper evaluation and with minimal scrutiny and transparency. Furthermore, existing and future databases may surely be **'instrumentalised'** as tools for the fulfillment of purposes related to ETIAS, namely conducting extensive profiling and automated data processing, even though the existing information systems expected to be interoperable with ETIAS are not meant to be used for profiling. On the contrary, these databases were set up for specific objectives unrelated to extensive profiling, which was not even foreseeable when the systems were originally established. As the EDPS has correctly pointed out, Eurodac in its current version is meant to assist the Dublin system; it is not meant to assist in the identification of immigration risks.⁸⁹ In addition, the pending proposals to amend the legal basis of existing systems (SIS II, Eurodac, ECRIS) or create new ones (EES) also provide for specific purposes that are not identical to the ones of the ETIAS system. Indeed, Eurodac and the EES are considered, at least on paper, directly security-related and security-oriented. In this respect, ETIAS may further legitimise and entrench the intertwinement of migration and security. Moreover, these systems contain millions of personal data points from a wide range of individuals, from perfectly legitimate travelers to **asylum seekers, which at the time of the data's collection were not collected for the purpose of conducting profiling on visa-exempt travelers.**

Another issue that emerges in the case of interoperability may be that individual rights, particularly the right to information, will be more difficult to exercise. Rules in relation to access rights need to be set out in order to ensure that national authorities not entitled to have access to a particular database shall not be granted access. Due to divergent rules regarding several aspects, such as retention periods, interoperability may lead to significant revisions in information systems with a view to aligning different modalities for the sake of

⁸⁶ PWC (2016), *Feasibility Study*, pp. 59-62.

⁸⁷ De Hert and Gutwirth (2006), 'Interoperability of Police Databases', *op. cit.*, p. 7. The purpose limitation principle is enshrined in Article 5(1)(b) of the General Data Protection Regulation.

⁸⁸ EDPS, 'Comments on the Communication of the Commission on Interoperability of European Databases' (n1536), p. 4.

⁸⁹ EDPS (2017), *EDPS Opinion*, p. 18.

efficiency. As the EDPS has already suggested, the blurring of the boundary between immigration control and criminal databases may also require amendments in relation to the legal bases.⁹⁰

In light of the above, an impact assessment addressing the issue of interoperability in a comprehensive manner is essential before proceeding with negotiations on the ETIAS proposal. Some of the key questions that need to be clarified before further progressing are the following:

- How will it be ensured that authorities lacking access to a set of personal data shall not be able to access a particular information system?
- How will individual rights be enforced, particularly since ETIAS will operate on the basis of data already stored in the system?
- How will the purpose limitation principle be ensured?
- Given the possibility that ETIAS data will not be stored for five years, how will the common repository model of interoperability work in practice?

⁹⁰ Ibid.

5. THE ETIAS PROPOSAL: A FUNDAMENTAL RIGHTS ASSESSMENT

KEY FINDINGS

- The proposal would **amount to a significant interference with human rights**, in particular the right to private life and the right to data protection, but the justification and necessity of the interference has not been clearly explained.
- The proposal is not accompanied by a specific **fundamental rights** or minimal **data protection impact assessment**.
- It is **impossible to assess the proportionality** of the measure as **the need to be met has not been clearly expressed**; there is no indication that alternative, less intrusive options have been considered; and the **effectiveness of the proposal has not been demonstrated**.
- The range of collected data, combined with the wide scope for its use, give rise to concerns that the proposal may lead to **profiling**, with **potentially discriminatory consequences**.
- The broad scope of information requested from applicants seems unnecessarily intrusive and interferes with the right to dignity.

The Commission has outlined the **potential impact** of ETIAS on a **wide range of fundamental rights**:

The proposed Regulation has an impact on fundamental rights, notably on right to dignity (Article 1 of the Charter of Fundamental Rights of the EU); right to liberty and security (Article 6 of the Charter), respect for private and family life (Article 7 of the Charter), the protection of personal data (Article 8 of the Charter), right to asylum (Article 18 of the Charter) and protection in the event of removal, expulsion or extradition (Article 19 of the Charter), the right to non-discrimination (Article 21 of the Charter), the rights of the child (Article 24 of the Charter) and the right to an effective remedy (Article 47 of the Charter).⁹¹

Although the potential issues have been identified, **no fundamental rights impact assessment has been carried out**. In the absence of a comprehensive impact assessment, **there is no substance to the proposal's assertion that it is compliant with fundamental rights**.

The main issues highlighted in this analysis are the right to respect for private life [Article 7 of the Charter of Fundamental Rights (CFR) and Article 8 of the European Convention on Human Rights (ECHR)], the right to the protection of personal data (CFR Article 8), and related concerns around the prohibition of discrimination (CFR Article 21, ECHR Article 14 and Article 2 of the Convention on the Rights of the Child (CRC)). But the **general principles discussed regarding legality, necessity and proportionality apply to all the rights that the Commission has identified as being impacted upon by the proposal**.

For the purposes of EU Institutions, the CFR is of paramount importance. The EU is not a signatory to the ECHR or the CRC, but **Member States implementing the proposal are**

⁹¹ COM (2016), 731 final, p. 19.

separately bound by their ECHR and CRC obligations. The **European Court of Human Rights (ECtHR) has made it clear that Member States cannot circumvent their ECHR obligations when implementing EU law.**⁹² In interpreting the CFR, the jurisprudence of the ECtHR and the ECJ may be relevant. Therefore, this analysis will consider both CFR and ECHR requirements for human rights compliance.

5.1. Interference with fundamental rights

The collection and storage of personal data on the scale envisaged in the ETIAS proposal clearly amounts to an interference with the right to private life under the CFR and the ECHR. **The ECtHR has held that the 'mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8'.**⁹³ This means that there is an interference with the right regardless of how the data is later used. Access to the data by law enforcement and others amounts to a further interference.⁹⁴ An interference is established regardless of whether the collected data is sensitive or not.⁹⁵

As the activities proposed amount to an interference with fundamental rights, including the right to private life, to be lawful the proposal must fulfil the tests of legality, necessity, proportionality and non-discrimination. It is important to recognise that the issue is not restricted to access or use of data. To comply with human rights law, the collection, storage and use of the data acquired under ETIAS must **in every case** fulfil those requirements as set out by the CFR and ECHR.

5.2. In accordance with the law

The proposal is for a Regulation to establish the ETIAS in law. On the face of it, this would fulfil the requirement **that an interference must be 'in accordance with the law'**. But human rights law requires that **the law should be sufficiently 'clear and precise'**, providing adequate guidance to guard against arbitrary interference with rights.⁹⁶ Some areas of the proposal currently lack the requisite precision and clarity.

For example, Article 10 of the proposal on Interoperability with other information systems states:

Interoperability between the ETIAS Information System and other information systems consulted by ETIAS such as the [Entry/Exit System (EES)], the Visa Information System (VIS), the Europol data, the Schengen Information System (SIS), [the Eurodac] and [the European Criminal Records Information System (ECRIS)] shall be established to enable carrying out the risk assessment referred to in Article 18.

There is no limit on the apparent scope of interoperability, which makes it very difficult to understand and identify the exact scale of this provision in practice. Without a clearer **explanation of what 'interoperability'** means, a comprehensive list of systems, or a clear definition of the type of system that ETIAS could consult, this provision is likely to fail the test of legality.

⁹² See, for instance, *Sharifi and Others v. Italy and Greece*, App no. 16643/09, EUR. Ct. H.R. Second Chamber, Judgment of 21 October 2014, para 232.

⁹³ *S. and Marper v the United Kingdom*, ECHR (2008) 1581, paragraph 67.

⁹⁴ *Leander v Sweden*, ECHR (1987), Series A, no. 116, at paragraph 48. Joined Cases C-293/12 (*Digital Rights Ireland*) and C-594/12 (*Kärtnner Landesregierung*), EU:C:2014:238, paragraph 35. Hereafter referred to as *Digital Rights Ireland*.

⁹⁵ *Österreichischer Rundfunk and Others*, EU:C:2003:294, paragraph 75; *Digital Rights Ireland*, EU:C:2014:238, paragraph 33.

⁹⁶ AG Mengozzi in *Opinion 1/15*, EU:C:2016:65, paragraph 193, with reference to *Fernández Martínez v Spain*, CE:ECHR:2014:0612JUD005603007, paragraph 117.

Another area of concern is Article 15.4, which includes a broad range of sensitive issues an applicant may be asked to answer as part of the application process, such as health and criminal convictions. The content and format of those questions are delegated to the European Commission. But the proposal is unclear about the exact purpose or scope of those questions, so it could be argued that the proposal as currently drafted is not sufficiently clear and precise. Given the sensitive nature of issues such as health and criminal convictions and the capacity for these questions to interfere with the inviolable right to dignity, the lack of specificity here needs to be addressed.⁹⁷

5.3. Necessity and purpose

Compliance with human rights law requires the proposed regulation to be necessary for a legitimate purpose in a democratic society. The CFR states that any limitations must respect the essence of the rights and freedoms and can only be made '[s]ubject to the principle of **proportionality ... 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'.⁹⁸

The **proposal's explanatory memorandum** asserts: '**Both from a migration and from a security point of view, there is a clear necessity to conduct prior checks in order to identify any risks associated with a visa-exempt visitor travelling to the Schengen Area**'.⁹⁹ While both migration and security concerns could be legitimate aims for interfering with the right to private life, the vague conflation of the two issues makes it difficult to assess exactly why the proposal is necessary. In his opinion, the EDPS stresses that 'while there might be synergies between migration and internal security, these are two different areas of public policy with distinct objectives and key actors'.¹⁰⁰ **The broad notion of 'any risks'** is also insufficiently clear to explain the **proposal's** necessity. It should be noted, particularly in the context of migration, that the ECtHR has found that the hallmarks of a democratic society **are** 'pluralism, tolerance and broadmindedness'.¹⁰¹ Before the proposal progresses, more work is required to clarify the exact need it is designed to meet. A desire to fill in the information gaps between other systems is not enough.

The proposal sets out the rationale for ETIAS in the following terms:

ETIAS will be an automated system created to identify any risks associated with a visa-exempt visitor travelling to the Schengen Area. Countries like the USA, Canada and Australia already use similar systems and consider these as an essential part of their security frameworks – as a result, these systems are now familiar to many Europeans.¹⁰²

Yet Australia, Canada and the USA are not governed by European human rights law. Familiarity with the systems used in those countries is not an argument for the necessity or legality of such a system in the European framework. The levels of privacy and personal data protection differ significantly in the European/EU system, so the existence of such practices in other countries does not make ETIAS necessary in the EU context. There is a real need to explain what makes the ETIAS proposal necessary, as opposed to just desirable or possible.

⁹⁷ CFR, Article 1, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

⁹⁸ CFR, Article 52.1, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.

⁹⁹ COM (2016), 731 final, p. 3.

¹⁰⁰ EDPS (2017), *EDPS Opinion*, p. 8.

¹⁰¹ See, for instance, *Lustig-Prean and Beckett v. The United Kingdom* (Applications nos. 31417/96 and 32377/96), Judgment of 27 September 1999, paragraph 80.

¹⁰² COM (2016), 731 final, p. 3.

5.4. Proportionality

The European Court of Justice has stated that:

Due regard to the principle of proportionality also derives from the Court's settled case-law¹⁰³ to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary.¹⁰⁴

Following a feasibility study commissioned in 2007, the Commission concluded in 2011 that the scheme should not move forward **'as the potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations'**.¹⁰⁵ This implies that the scale of the proposal was not deemed proportionate to the aims at that time and that it was not judged strictly necessary. There is no detailed explanation as to why that position has changed now. An assessment of the proportionality of the proposal requires a clear articulation of the needs it is designed to meet. The EDPS has underlined the fact that a data protection impact assessment is a prerequisite for assessing compliance; without one, it is impossible to fully assess the necessity and proportionality of the proposal.¹⁰⁶ An impact assessment should take into account the following considerations, among others, when assessing the proportionality and necessity of the measures proposed:

- What is the purpose of the individual data points requested and how do they support the **proposal's** legitimate aims?
- Why is ETIAS necessary and proportionate in addition to existing PNR and API frameworks?
- Why should visa-exempt ETIAS applicants provide more data than applicants for a Schengen visa going through the VIS system?
- If the purpose is screening before entry, what is the reason for retaining data after the initial authorisation is granted? Why was a five-year retention period chosen?
- Which agencies will have access to the data and for what exact purpose? In particular, will intelligence services have access to ETIAS?
- Why is it necessary to provide access to ETIAS data from the outset to law enforcement authorities and Europol? Under what conditions will this access take place?
- Will it be necessary for law enforcement authorities and Europol to have access to the full set of ETIAS data?

Pressing ahead with the proposal in the absence of a risk assessment runs the very real risk that these issues will ultimately need to be clarified through costly litigation before the ECJ. We therefore recommend that an impact assessment on fundamental rights with a focus on privacy and data protection should be completed before the proposal progresses.

The UN Special Rapporteur highlighted some challenges and worrying trends related to privacy and data protection in a recent report:

Increasingly, **personal data ends up in the same 'bucket'** of data which can be used and re-used for all kinds of known and unknown purposes. This poses critical questions

¹⁰³ Judgments of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C 73/07, EU:C:2008:727, paragraph 56; of 9 November 2010, *Volker und Markus Schecke and Eifert*, C 92/09 and C 93/09, EU:C:2010:662, paragraph 77; the *Digital Rights* judgment, paragraph 52, and of 6 October 2015, *Schrems*, C 362/14, EU:C:2015:650, paragraph 92.

¹⁰⁴ Judgment in *Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen* and *C-698/15 Secretary of State for the Home Department v Tom Watson and Others*, Judgment of 21 December 2016.

¹⁰⁵ COM (2011), 680 final, p. 7.

¹⁰⁶ EDPS (2017), *EDPS Opinion*, paragraph 13.

in areas such as requirements for gathering data, storing data, analysing data and ultimately erasing data.¹⁰⁷

The ETIAS proposal would seem to be an example of this worrying trend. If it is to progress, it should, at a minimum, be revised to clarify exactly for what purposes data can be used or re-used and highlight how that is reflected in the arrangements for the gathering, storing, analysing and erasing of data in the system.

5.5. Discrimination

Although the **proposal's explanatory memorandum and the Proposed Regulation assert that** there would be no discrimination, the choice of requested data from applicants and the provisions on screening raise serious concerns about the potential for both direct and indirect discrimination. The CFR, the CRC and the ECHR prohibit discrimination. CFR Article 21.1 states: 'Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited'. In relation to the prohibition on discrimination in the ECHR, the ECtHR has clarified that 'a difference of treatment is discriminatory if it has no objective and reasonable justification, that is, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised'.¹⁰⁸ CRC Article 2.2. **provides that** "States Parties shall take all appropriate measures to ensure that the child is protected against all forms of discrimination or punishment on the basis of the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members."

The CRC also provides a right of family reunification. CRC Article 10 provides that "applications by a child or his or her parents to enter or leave a State Party for the purpose of family reunification shall be dealt with by States Parties in a positive, humane and expeditious manner. States Parties shall further ensure that the submission of such a request shall entail no adverse consequences for the applicants and for the members of their family.....A child whose parents reside in different States shall have the right to maintain on a regular basis, save in exceptional circumstances personal relations and direct contacts with both parents...." **It is unclear from the proposal how this right will be guaranteed in a way** that does not discriminate against children in the EU with a parent or parents from countries covered by the ETIAS scheme.

The wide scope of data requested, along with the sensitive nature of the topics for questioning included in Article 15 of the proposal, raise concerns about the potential for discrimination. The ECtHR has **accepted that health could be a 'status' for the purpose** of the prohibition on discrimination in Article 14.¹⁰⁹ There is a risk that, in the absence of clear reasoning for questions on public health and the type of diseases that could be covered, this could result in unlawful discrimination based on things like HIV status. Such discrimination could also affect vulnerable children either because of their health status or the health status of their parents. It should be noted that the CRC contains specific protections for disabled children¹¹⁰ **and for children's access to the highest standards of health and to facilities of treatment**¹¹¹ that could be affected by the proposal where children and their families are travelling to the EU for the purposes of medical treatment. Questions regarding public health and epidemic risks may also be discriminatory unless there are protective measures in place for EU

¹⁰⁷A/HRC/34/60, at <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21321&LangID=E>, paragraph 20.

¹⁰⁸ Religionsgemeinschaft der Zeugen Jehovas v Austria, Application no. 40825/98, (2008) [87].

¹⁰⁹ V.A.M. v. Serbia, Application no. 39177/0 (2007).

¹¹⁰ CRC Article 23

¹¹¹ CRC Article 24

nationals at risk, as public health measures targeting only non-EU nationals would not be effective and therefore disproportionate.

The wide scope of questions on criminal convictions, not only on serious offences but 'for any offence in any country' is also a concern from a proportionality and discrimination perspective.¹¹² The EU is founded on the principles of human rights and equality, but those principles are not necessarily reflected in the criminal codes of non-EU countries. Criminal convictions could include minor infractions and offences committed when the applicant was a minor. They could also include convictions for offences that would not be criminalised in the EU now, such as matters related to sexual orientation, adultery, religious belief or freedom of expression. Even convictions related to an issue like abortion, on which EU Member States take very different stances, could be included within the scope of this provision. To require an applicant to respond to this type of question could have a disproportionate and discriminatory impact on some groups of people, going to the heart of the right to dignity.¹¹³ The current drafting seems disproportionate and arbitrary. If there really is a need to request information about criminal convictions, careful thought needs to be given as to what type of criminal convictions shall be clarified and under what circumstances this information needs to be requested.

The issues relating to the data required and the potential questions are compounded by Article 28 of the proposal on ETIAS screening rules:

4. Based on the risks determined in accordance with paragraph 2, the ETIAS Central Unit shall establish the specific risk indicators consisting of a combination of data including one or several of the following:

- (a) age range, sex, current nationality;
- (b) country and city of residence;
- (c) education level;
- (d) current occupation.

5. The specific risk indicators shall be targeted and proportionate. They shall in no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sexual life or sexual orientation.¹¹⁴

The assertion that the risk indicators shall be targeted, proportionate and non-discriminatory seems to contradict the contents of the list of indicators, many of which are essentially prohibited grounds for discrimination. Profiling on age, sex and nationality for an unspecified range of risks would clearly have a discriminatory effect. Although nationality may be taken into account in immigration decisions, it should be recalled that the ETIAS proposal will only apply to nationalities not subject to visa requirements in any event. Using the country and city of residence as a risk factor in this context could give rise to indirect discrimination since it would amount, in many cases, to risk profiling based on ethnic or social origin, religion, or membership of a national minority. Preventative risk profiling based on this type of general data rather than a concrete risk shown by, for example, information of a specific security risk linked to a conviction for particular offences or intelligence relating to a concrete security risk is unlikely to be considered lawful.¹¹⁵ It may also be counter-productive and add to a sense of ostracisation in groups who feel discriminated against as a result.

¹¹² ETIAS Proposal, Article 15.4.b.

¹¹³ CFR, Article 1.

¹¹⁴ ETIAS Proposal, Article 28.5.

¹¹⁵ See for example German Constitutional Court ruling 1 BvR 518/02

The prohibition on discrimination in European human rights law applies not only to the list of **prohibited grounds but to 'any other status'** or a combination of different grounds for distinction.¹¹⁶ Requiring information on education and professional status for screening is of concern, both for its potential to discriminate against people because of their socio-economic status but also because of the potential impact on people such as journalists, lawyers and human rights defenders and the consequent interference with other rights such as freedom of expression and association. It is unclear exactly what the point of requiring this data is, and the broad and ill-defined notion of risk in the proposal means it could give rise to arbitrary, disproportionate and discriminatory decisions.

¹¹⁶ ECHR, Article 14 ECHR. See Rory O'Connell (2009), 'Cinderella comes to the Ball: Article 14 and the right to non-discrimination in the ECHR', *Legal Studies: The Journal of the Society of Legal Scholars* 29:2 (2009): 211-229. O'Connell notes: 'Article 14 is not limited to distinctions based on "suspect grounds" typically used to express prejudice, but can cover any arbitrary distinction. This means that purely arbitrary distinctions are not permitted. It also means that the ECtHR does not have any problems dealing with claims that raise "intersectional" issues, i.e. do not neatly raise one particular ground for distinction, but raise more than one ground'.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1. Conclusions

The study asked three questions regarding the ETIAS proposal:

- Have there **been major documented changes** over the last few years that require the establishment of the ETIAS scheme?
- How does ETIAS fit into the increasingly dense landscape of EU data processing schemes related to border control and the countering of terrorism and serious and organised crime?
- Thirdly, **to what extent does the proposed measure create an interference with fundamental rights**, including but not limited to the right to privacy and data protection? To what extent is it **in conformity with EU and international law**?

Answering these questions is complicated by the fact that the European Commission has not attached a standalone impact assessment document but has relied upon a feasibility study done by external contractor PricewaterhouseCoopers to demonstrate the necessity of ETIAS.

Notwithstanding these complications, the study shows that **the central justification for ETIAS** advanced by the European Commission is the **anticipated increase in the number of visa-exempt third-country nationals** from 30 million in 2014 to 39 million in 2020 and the fact that so far visa-exempt persons are not monitored to the same extent as visa-holding travelers – the so-called **'information gap'**. The ETIAS proposal, however, provides **no concrete evidence that this 'information gap' constitutes a security threat**. As such, the study finds that there is a mismatch between the identification of the problem, an increase in the number of visa-exempt travelers, and the steps to address it; the problem logically calls for facilitation measures but ETIAS is almost exclusively security-related.

This study argues that the **gap in logic and reasoning** is paralleled in **an evidence basis of uneven quality**. Over the last five years, the European Commission has relied on a single contractor, PricewaterhouseCoopers, for evidence gathering on EU-ESTA/ETIAS. As the study demonstrates, the terms of reference for the latest study undertaken by the contractor (in 2016) are particularly restrictive. In addition, **the contractor's findings have fluctuated, without explanation, from one study to the next**, and the European Commission has **sidelined, without explicit reasons, the findings of its own contractor** regarding the necessity and justification for some of the measures envisaged in the ETIAS proposal.

As a result, the overall rationale for the establishment of ETIAS remains unclear, and the case for its necessity has not been made. This observation also **applies to specific features of the measure**. For example, why ETIAS should **store the IP addresses of applicants** or why the applicant questionnaire includes **entries related to health risks** have not been explained. For the former, at least, the feature runs contrary to the findings of the feasibility study undertaken by the **Commission's contractor**. Likewise, it is clear that the ETIAS screening rules and the ETIAS watchlist are supplemental rather than essential to the functioning of the system; the necessity for their inclusion in the proposal has not been discussed by the European Commission.

The numerous weaknesses in the case for ETIAS, in turn, are hard to ignore given that the study finds the **establishment of ETIAS would significantly affect the conduct of the EU's border and visa policy**. The ETIAS Regulation would establish a new automated data processing scheme for a category of travellers already under considerable scrutiny given the adoption of the PNR Directive (these travellers will be under even greater scrutiny if the EES Regulation is adopted by the co-legislator). As the study demonstrates, the proposal would further introduce through ETIAS screening rules **a procedure for the mining and profiling**

of the personal data of all visa-exempt third-country nationals. The proposal would also create another 'watchlist' whose legality and relationship to the existing EU counter-terrorism watchlist has not been considered by the European Commission. In addition, the ETIAS Regulation would preempt ongoing discussions about interoperability by introducing the notion into legislation before discussions over this matter are completed. This would be done without an assessment of important implications of interoperability, especially on the rights to privacy and personal data protection. As this study has shown, the ETIAS proposal constitutes a continuation of the Commission's efforts to introduce interoperability through the back door for information systems that up to now have been standalone and compartmentalised. This would be done with **limited scrutiny and minimal rules permitting individuals to ensure that they could foresee how their personal data could be used in the future.** Key principles of data protection law, such as purpose limitation, will become void of content, and the combination of data through different data pots will enhance the profiling capabilities of national competent authorities. By opting for such an approach, two main issues arise. The first is that the **persistent minimisation and marginalisation of the implications of interoperability** turns the issue into **a somewhat technical matter rather than a major shift in the operation and very nature of centralised databases.** The second is that the vagueness in the wording of the ETIAS proposal will allow for **constant upgrades, with the prospect that in the near-future an EU information system used for both law enforcement and border control purposes shall emerge** on the basis of the US model.

These findings, in turn, inform the assessment of the **fundamental rights aspects** of the ETIAS proposal. Although the proposal would amount to a **significant interference** with human rights, in particular the right to private life and the right to data protection, **the justification for and necessity of the interference has not been clearly explained yet.** It is **impossible to assess the proportionality of the measure, as the need to be met has not been clearly expressed;** there is no indication that **alternative, less intrusive options** have been considered; and **the effectiveness of the proposal has not been demonstrated.** The range of data collected and the wide scope for its use give rise to concerns that data may be used for profiling, with potentially discriminatory consequences. The broad scope of information requested from applicants seems unnecessarily intrusive and interferes with the right to dignity. The **current proposal, therefore, cannot currently be said to be genuinely compliant with fundamental rights.**

6.2. Recommendations

6.2.1. Points requiring clarification from the European Commission

The following are clarifications that the LIBE Committee could consider requesting from the European Commission when examining the proposal for an ETIAS Regulation.¹¹⁷

- On the necessity of the ETIAS proposal, the European Commission should clarify on what grounds it considers that **there has been a change in circumstances** justifying a return to the discarded EU-ESTA proposal. This issue concerns, in particular:
 - Beyond the fact that visa-exempt nationals are not monitored in the same way as visa-holding third-country nationals, the Commission should clarify the **evidence basis** on which it considers visa-exempt nationals **to pose a specific irregular migration risk.**
 - Beyond the fact that visa-exempt nationals are not monitored in the same way as visa-holding third-country nationals, the Commission should clarify the **evidence basis** on which it considers visa-exempt nationals **to pose a specific**

¹¹⁷ For instance, on the basis of Rule 130 of the Rules of Procedure of the European Parliament concerning questions for written answers to, among others, the European Commission.

security risk, particularly with regard to countering terrorism and serious and organised crime.

- A key issue identified in the study is the **absence of an impact assessment** from the European Commission. The Commission has relied exclusively upon a single contractor, PricewaterhouseCoopers, for **all** the evidence gathering and impact assessment for the ETIAS proposal. This concern is amplified by the fact that the Commission has used PwC as a key contractor in at least another major legislative file, the smart borders package. This matter concerns, in turn:
 - The reasons as to why the European Commission decided to not produce an impact assessment for the ETIAS proposal.
 - The reasons as to why the European Commission decided to **not produce a fundamental rights assessment and a data protection assessment** for the ETIAS proposal.
 - The **reasons as to why the European Commission chose to rely on the same contractor** for the 2011 and 2016 studies on EU-ESTA and ETIAS, as well as the contractual basis for this choice.
 - The **detailed costs** of the 2011 and 2016 policy and feasibility studies.
 - The **evidence of competence of the contractor** and possible sub-contractors justifying the systematic reliance on PwC.

6.2.2. Regarding impact assessment and necessity

- While there is a political momentum for the ETIAS proposal, the evidence-based case for the necessity of the measure has not been made. As such, the LIBE Committee should **insist that the ETIAS proposal comply with the European Commission's 'Better Regulation Guidelines'** and that the proposal be **accompanied by a full impact assessment**, together with a positive opinion of the European Commission Regulatory Scrutiny Board. **This request may be based on Point 16 of the Interinstitutional Agreement of 13 April 2016 on Better Law-Making**.¹¹⁸
- The impact assessment process **should give enough time for proper inter-service consultation within the European Commission and with other EU bodies**, including the EEAS, the EDPS, and the FRA.
- The impact assessment should clearly provide and state any **evidence that a) circumstances have changed sufficiently in the five years since the EU-ESTA initiative was abandoned to justify the necessity of ETIAS** and **b) that visa-exempt third-country nationals are of particular concern with regard to irregular migration and security risks**.
- The impact assessment should provide **an appropriate list of policy options**, including the **impact of 'no ETIAS'**, the possibility of establishing ETIAS with or without the ETIAS screening rules, the ETIAS watchlist, and Europol and law enforcement access, as well as **exploring further possibilities for data minimisation**, including the impact of not collecting IP addresses or health-related personal data.

¹¹⁸ Point 16 of the Agreement states: 'The Commission may, on its own initiative or upon invitation by the European Parliament or the Council, complement its own impact assessment or undertake other analytical work it considers necessary'.

- The impact assessment **should include an analysis of the effect on the EU's international relations**, in particular on third countries whose citizens currently benefit from visa exemption or are likely to do so in the foreseeable future. A consultation with the Permanent Representatives to the EU of the concerned third countries should be considered.
- The impact assessment **should include a fundamental rights impact assessment**, including, but not limited to, the right to data protection and the right to privacy.

6.2.3. Regarding interoperability

- The proposal for an ETIAS Regulation **foresees the implementation of interoperability between EU border control and security information systems before on-going high-level discussions on this issue have been completed**, and in particular before the HLEG has had the opportunity to deliver its 'interoperability package' (expected June 2017).
- In addition, the proposal for an ETIAS Regulation foresees interoperability between ETIAS and at least one other EU information system, **the EES, which the co-legislators are currently discussing**.
- The LIBE Committee should consider **putting on hold the examination of the ETIAS proposal** until such time as **policy orientations, guidelines and possible legislation on interoperability have been tabled and adopted** and until such time as **the co-legislators make a final decision on the proposal for a Regulation establishing the EES**.
- Alternatively, as part of a comprehensive impact assessment accompanying the proposal for an ETIAS Regulation, **the LIBE Committee should request the European Commission to include a specific explanation of interoperability**, including the legal provisions that shall govern interoperability, which model will be used and how it may be embedded in ETIAS.

6.2.4. Regarding the ETIAS screening rules and watchlist

- The provisions on the ETIAS screening rules introduce a new mechanism for **mining and profiling the personal data of visa-exempt third-country nationals** in EU border control measures. There is a **clear difference** between such a mechanism, which aims to single out persons previously unknown not for facts that they are associated with but because their individual characteristics meet certain category traits, and the other aspects of data processing in the ETIAS proposal, which consist in **verifying whether an individual traveller is already known (and for what facts) according to either the ETIAS watchlist or to other EU information systems**.
- **ETIAS screening rules are supplemental rather than essential to the other measures involved in ETIAS's functioning**. In the meantime, data mining and profiling form a **particularly serious interference with the rights to data protection and privacy**. As such, **the LIBE Committee should consider establishing ETIAS without the ETIAS screening rules**.
- Alternatively, before considering the establishment of ETIAS screening rules, the LIBE Committee should request the European Commission, in concert with the European Border and Coast Guard Agency (EBCG) when appropriate, to submit, as part of a comprehensive ETIAS impact assessment, **an explanation of the provenance,**

substance and functioning of the algorithm and risk indicators that will be used in ETIAS screening rules.

- Should the co-legislators eventually find the establishment of ETIAS screening rules relevant, **the LIBE Committee should consider including a suspension and a sunset clause for the measure in the ETIAS Regulation.** These would have the following effect: 1) the use of ETIAS screening rules would be **suspended**, pending review by the EDPS and the FRA together with the EBCG, should appeals related to decisions made on the basis of the screening rules increase beyond a threshold to be determined by the co-legislators or should the functioning of the screening rules be considered less than optimal by the relevant national authorities; and 2) a **sunset clause foreseeing the full and definitive shutdown of ETIAS screening rules** should the review, undertaken by the EDPS, FRA and EBCG upon suspension, be concluded negatively.
- The ETIAS watchlist is a supplemental rather than an essential part of the ETIAS proposal. In the meantime, it raises questions regarding the relationship with the EU counter-terrorism watchlist under Common Position 2001/931/CFSP and the reliance on information obtained through international cooperation. As such, **the LIBE Committee should consider establishing ETIAS without the ETIAS watchlist.** Alternatively, the **LIBE Committee should consider including a suspension and a sunset clause for the ETIAS watchlist** on the model suggested for the ETIAS screening rules.
- The oversight mechanism for the ETIAS screening rules and watchlist does not involve the intervention of independent or EU bodies other than the European Commission, ETIAS Central Unit and Europol. **The ETIAS Central Unit is effectively expected to self-monitor the impact of ETIAS screening rules on fundamental rights and privacy and data protection.** Furthermore, the ETIAS Screening Board does not include any independent or EU body other than Europol and ETIAS National Units. Additionally, **there is no oversight or monitoring mechanism involved in Europol's implementation of the ETIAS watchlist.** The LIBE Committee should consider amending the relevant Articles in the ETIAS proposal (Articles 7, 9, 28 and 29) to provide, at the very least, for the systematic involvement of the EDPS and FRA on matters of fundamental rights, including discrimination, the right to data protection and the right to privacy.

6.2.5. Regarding fundamental rights compliance

- A **human rights impact assessment needs to be carried out before the proposal can be considered compliant with fundamental rights.** Taking into consideration **the requirement made recently by the European Parliament in its 13 December 2016 Resolution that fundamental rights should be part of the impact assessment of all legislative proposals in the European Union,** the LIBE Committee should recommend that such an impact assessment **be carried out by an independent expert or body not involved in the design of the proposal,** with the full involvement and support from the EDPS and the FRA.
- An impact assessment should **take into account the following issues,** among others, when assessing the necessity and proportionality of the proposed measures:
 - Why is ETIAS necessary and proportionate in addition to existing PNR and API frameworks?
 - What is the purpose of the individual data points requested and how do they support the **proposal's** legitimate aims?
 - Why should visa-exempt ETIAS applicants provide more data than applicants for a Schengen visa going through the VIS system?

- If the purpose is screening before entry, what is the reason for retaining the data after the initial authorisation is granted? Why was a five-year retention period chosen?
 - Which agencies shall have access to the data and for what exact purpose? In particular, will intelligence services have access to ETIAS?
 - Why is it necessary to provide access to ETIAS data from the outset to law enforcement authorities and Europol? Under what conditions shall this access take place?
 - Will it be necessary for law enforcement authorities and Europol to have access to the full set of ETIAS data?
- The data required and the questions to be asked should be **reconsidered given the high risk of profiling based on protected characteristics**.
- The reasons for and the scale of the potential for interoperability in the proposal need to be explained with reference to the principles of legality, necessity and proportionality.

REFERENCES

- Council of the EU. 2017. *Visas: Council confirms agreement on visa liberalisation for Ukrainians*. Press Release 98/17, 02.03.2017.
- De Hert, Paul and Serge Gutwirth. 2006. 'Interoperability of Police Databases within the EU: An Accountable Political Choice?' *International Review of Law Computers & Technology* 20:1-2 (March-July): 21-35.
- Dinant, Jean-Marc et al. 2008. *Application of Convention 108 to the profiling mechanism*. Strasbourg: Council of Europe. T-PD(2008)01, 11.01.2008.
- EDPS. 2017. *EDPS Opinion on the Proposal for a European Travel and Information Authorisation System (ETIAS)*. Brussels, Opinion 3/2017.
- European Commission. 2016. *Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders*. COM(2016) 602 final, 14.9.2016.
- European Commission. 2016. *Proposal for a Regulation of the European Parliament and of the Council 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 of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*. COM(2016) 194 final, 6.4.2016.
- European Commission. 2016. *Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*. COM(2016) 731 final, 16.11.2016.
- European Commission. 2016. *Stronger and Smarter Information Systems for Borders and Security*. COM(2016) 205 final, 6.4.2016.
- European Commission. 2015. (2015) *Commission Staff Working Document: Better Regulation Guidelines*. SWD(2015) 111 final.
- European Commission. 2015. *The European Agenda on Security*. COM(2015) 185 final, 28.4.2015.
- European Commission. 2013. *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union*. COM(2013) 95 final, 28.2.2013.
- European Commission. 2011. *Smart borders – options and the way ahead*. COM(2011) 680 final, 25.10.2011.
- European Commission. 2008. *Preparing the next steps in border management in the European Union*. COM(2008) 69 final, 13.2.2008.
- European Commission. 2001. *Development of the Schengen Information System II*. COM(2001) 720 final, 18.12.2001.

- European Commission/IDABC. 2004. *European Interoperability Framework for Pan-European e-Government Services*. Luxembourg: Office for Official Publications of the European Communities.
- European Parliament. 2016. *European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015 (2016/2009(INI))*. P8_TA-PROV(2016)0485.
- European Parliament. 2015. *European Parliament resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens (2015/2635(RSP))*. P8_TA(2015)0388.
- European Parliament. 2014. *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*. P7_TA(2014)0230.
- European Parliament. 2010. *European Parliament resolution of 10 March 2009 on the next steps in border management in the European Union and similar experiences in third countries (2008/2181 (INI))*. OJEU, 2010/C 87 E/01.
- Europol. 2016. *European Union Terrorism Situation and Trend Report 2016*. The Hague: European Police Office.
- FRONTEX. 2016. *Risk Analysis for 2016*. Warsaw: FRONTEX. 3.2016.
- Government Accountability Office. 2011. *Visa Waiver Program: DHS Has Implemented the Electronic System for Travel Authorization, but Further Steps Needed to Address Potential Program Risks*. Washington, D.C.: GAO-11-335, 4.2011.
- Jeandesboz, Julien, Didier Bigo, Ben Hayes and Stephanie Simon. 2013. *The Commission's legislative proposals on Smart Borders: their feasibility and costs*. Brussels: European Parliament. PE 493.026.
- Jeandesboz, Julien, Jorrit Rijpma and Didier Bigo. 2016. *Smart Borders Revisited: An assessment of the Commission's revised Smart Borders proposal*. Brussels: European Parliament. PE 571.381.
- Hildebrandt, Mireille. 2008. 'Defining Profiling: A New Type of Knowledge?' In: *Profiling the European Citizen: Cross-Disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth. Leiden: Springer. 17-45.
- O'Connell, Rory. 2009. 'Cinderella comes to the Ball: Article 14 and the right to non-discrimination in the ECHR'. *Legal Studies: The Journal of the Society of Legal Scholars* 29:2 (2009): 211-229.
- PricewaterhouseCoopers. 2016. *Feasibility Study for a European Travel Information and Authorisation System (ETIAS)*. Luxembourg: Publications Office of the European Union.
- PricewaterhouseCoopers. 2014. *Technical Study on Smart Borders – Final Report*. Luxembourg: Publications Office of the European Union.
- PricewaterhouseCoopers. 2011. *Policy study on an EU Electronic System for Travel Authorization (EU ESTA)*. Brussels, 2010-1227/OV/fvh/ms/wb/ns.

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS **C**

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website:
<http://www.europarl.europa.eu/supporting-analyses>

PHOTO CREDIT: iStock International Inc.



ISBN 978-92-846-1074-7 (paper)
ISBN 978-92-846-1075-4 (pdf)

doi: 10.2861/919151 (paper)
doi: 10.2861/615043 (pdf)