



ETIAS Data Protection Impact Assessment (DPIA)

Handling instructions for the marking INTERNAL DAY-TO-DAY

- Distribution on a need-to-know basis.
- Not to be released outside of the information stakeholders.
- Not for publication.

Handling instructions for the marking SENSITIVE

- Distribution only on a strict need-to-know basis.
- Not to be released outside of the intended recipients. Any person who is not the intended recipient of this information must inform the sender.
- The same markings need to be used to reply to- or to forward this information.
- Not for publication.

Date of the DPIA, Validation/Sign-Off and Review

Document Control Information

Settings	Value
Project Name:	ETIAS Data Protection Impact Assessment
Corporate Record:	☐ Yes ☒ No
Record Reference ¹ :	Not available
Processing Operation Name:	ETIAS Data Protection Impact Assessment
Revision Status:	01_00_03
Sensitivity:	Sensitive
Issue Date:	14/06/2021

Document Approver(s)

Approver Name	Role	Approval Date	Signature
GARKOV Krum	eu-LISA Executive Director		
	eu-LISA Head of Operations Department		
	eu-LISA Head of Security Unit		

Document Reviewers

Reviewer Name	Role	Review Date
	eu-LISA – ETIAS Programme Manager	26.04.2021
	eu-LISA – Data Protection Officer	26.04.2021
	eu-LISA – Business Relations Management sector, Vice Chair of ETIAS AG	29.01.2021
	eu-LISA – Head of Business Relations Management sector, Chair of ETIAS AG	29.01.2021
	eu-LISA – Architecture Sector	29.01.2021
	eu-LISA – Head of Information Security and Assurance Sector	29.01.2021

¹ Record reference in the register of data processing activities (from either the data processing register of eu-LISA as controller or the register of categories of data processing operations of eu-LISA as processor).

Version History:

Version	Date	Author	Short Description of Changes
00_01_00	15/09/2020	Unisys TEAM	Submission for Review – 1 st round
00_02_00	22/01/2021	Unisys TEAM	Submission for Review – 2nd round
00_03_00	12/02/2021	eu-LISA DPO	The comments of eu-LISA DPO are included in section 10 'eu-LISA DPO Comments'.
01_00_00	08/04/2021	Unisys TEAM	Implementation of eu-LISA DPO comments. Chapter 11. "Addressing DPO comments" is included in the report The initial draft version of the excel file (ETIAS DPIA_sheets_v.00.00.01) is added as annex to the present report.
	22/04/2021	eu-LISA DPO	Minor additional comments provided
01_00_01	26/04/2021	Unisys TEAM	Section 4.5.2: elaborated on other parties consulted. Section 13: reworked Action Plan to reflect all mitigation measures.
	03/05/2021	eu-LISA DPO	Minor additional comments provided
01_00_02	28/05/2021	Unisys TEAM	Comment from DPO implemented in Executive summary; section 4.3.2.1 ; section 4.3.5.4. Action Plan reworked to clarify responsible, expected date and status.
01_00_03	14/06/2021	ETIAS Programme Manager	Integrated DPO comments and Addressing DPO comments into Annexes section

Table of Contents

Executive Summary	8
Terminology.....	14
1. Introduction.....	18
1.1. Structure of this DPIA.....	18
2. Reasons for this DPIA	20
3. DPIA Methodology.....	22
3.1. DPIA Team.....	23
3.2. Guidelines, tools, methodologies, standards and opinions used in the DPIA.....	23
3.3. Extension and limits of the DPIA: Identify what has been left out of scope of the assessment	27
4. General Description of the Data Processing Operation	29
4.1. Name and description of the data processing activity	30
4.2. Roles.....	32
4.3. General description of the data processing activity	34
4.4. Internal context of the data processing in the organization.....	46
4.5. External context of the organization and the data processing.....	48
4.6. Lawfulness of the data processing operation.....	49
5. Systematic Description of the Data Processing Operation.....	52
5.1. Detailed description of the purpose(s) and supporting assets	54
5.2. Flowchart.....	57
5.3. TCN Draft Application	58
5.4. TCN Submitting application.....	64
5.5. Automated processing	68
5.6. Manual processing	72
5.7. TCN requests access, rectification, completion or erasure of personal data, consent & abuse.	78
5.8. Watchlist management.....	84
5.9. Watchlist review.....	90
5.10. Access to the ETIAS Central System for Border control and law enforcement purposes.....	94
5.11. Carriers verification.....	101
5.12. European Border and Coast Guard Agency support to carrier or TCN.....	106
5.13. Interaction with other processes	109
6. Necessity and Proportionality Assessment.....	110
7. Identify and Assess Risks	119
7.1. Guiding questions on data protection principles	124
8. Measures to Mitigate Identified Risks.....	150
9. DS (Data Subjects) Comments (If Applicable)	154
10. Conclusions and Recommendations.....	155



11. Action Plan.....	157
12. ANNEXES	162
12.1. eu-LISA DPO Comments.....	162
12.2. Addressing DPO Comments.....	165
12.3. Knowledge base for the description of supporting assets	167
12.4. Knowledge base for likelihood and impact ratings.....	167
12.5. Identification of the risks.....	170
12.7. Knowledge base for possible risks and mitigation measures	171

Table of figures

Figure 1 TCN draft application flow	58
Figure 2 TCN Submission application flow	64
Figure 3 automated processing flow.....	68
Figure 4 manual processing flow.....	72
Figure 5 TCN requests access, rectification, completion or erasure of personal data, consent & abuse	78
Figure 6 Watchlist management.....	84
Figure 7 Watchlist review flow	90
Figure 8 Access for Border control and law enforcement purposes flow	94
Figure 9 Carrier verification flow.....	101
Figure 10 European Border and Coast Guard Agency support to carrier or TCN.....	106

Table of tables

Table 1 Mitigation measures.....	13
Table 2 Abbreviations and Acronyms.....	14
Table 3 Glossary	17
Table 4 Legal basis	21
Table 5 DPIA Team.....	23
Table 6 Legislative framework.....	25
Table 7 Implementing and Delegated acts	26
Table 8 Opinion and Guidelines	27
Table 9 Main Processing Operations	31
Table 10 Roles.....	34
Table 11 Processing operation.....	36
Table 12 Data subjects	38
Table 13 Data categories.....	41
Table 14 Recipients of the data	43
Table 15 International data transfers	45
Table 16 Legal basis and necessity for processing.....	50
Table 17 data flows	54
Table 18 supporting assets	56
Table 19 flowchart diagram symbols.....	57
Table 20 TCN Draft Application steps.....	59
Table 21 TCN Submitting Application steps.....	Error! Bookmark not defined.
Table 22 Automated Processing steps	69
Table 23 Automated Processing overview.....	72
Table 24 Manual processing	77
Table 25 TCN requests access, rectification, completion or erasure of personal data, consent & abuse steps.....	79
Table 26 TCN requests access, rectification, completion or erasure of personal data, consent & abuse overview	83
Table 27 Watchlist Management.....	85
Table 28 Watchlist Management overview	89
Table 29 Watchlist review.....	91
Table 30 Watchlist Review overview.....	93
Table 31 Access to the ETIAS Central System for Border control and law enforcement purposes	95
Table 32 Access to the ETIAS Central System for Border control and law enforcement purposes overview	100



Table 33 Carriers verification.....	102
Table 34 Carriers verification overview.....	105
Table 35 Carriers verification overview.....	107
Table 36 Interaction with other processes.....	109
Table 37 Necessity Assessment	115
Table 38 Proportionality Assessment.....	118
Table 38 Risk classification.....	119
Table 39 Risk rating.....	119
Table 40 Identified Risks.....	124
Table 41 Fairness analysis.....	127
Table 42 Transparency analysis.....	131
Table 43 Purpose limitation analysis	133
Table 44 Data minimisation analysis.....	136
Table 45 Data minimisation analysis	139
Table 46 Storage limitation -retention period analysis.....	142
Table 47 Security analysis.....	147
Table 48 Security risks first set.....	149
Table 49 Option to reduce or eliminate risk	153
Table 50 Conclusions and Recommendations	155
Table 51 Action plan	161
Table 52 Knowledge base for the description of supporting assets	167
Table 53 Knowledge base for likelihood and impact ratings	169
Table 54 Identification of the risks.....	170

Executive Summary

The European Travel Information and Authorisation System (ETIAS), is a large-scale information system, and one among the measures undertaken as part of the Smart Borders Package. After negotiations with the European Parliament and the Council, the ETIAS Regulation (EU) 2018/1240 was adopted on 12 September 2018 and entered into force on 9 October 2018.

ETIAS is expected to be operational by the end of 2022. Once fully implemented, it will enable the advanced authorisation of visa-exempt travellers when crossing the external borders and will in particular impose a new check to be performed by carriers to those who are travelling.

The expected number of travel authorisations request is approximately 80 to 110 million application requests per year following the Entry into Operations.

Due to the complexity of ETIAS processing activities, the definition of roles is one of the most complex part to identify. Following the regulation Frontex and Members States are involved as data controller for the processing of personal data in the ETIAS Central System and eu-LISA has been assigned from the legislator as both a data controller and data processor.

From EU perspective, European Border and Coast Guard Agency is to be considered a data controller in relation to the processing of personal data in the ETIAS Central System. While the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) is responsible for developing the system and is a data controller for the information security management.

This DPIA assesses the data protection risks identified with the design and development of ETIAS. It is a first study which will have to be complemented by synergetic contributions from FRONTEX and Member states to achieve an exhaustive assessment of all the risks related to the establishment of ETIAS.

The chosen approach for this exercise is to provide a general and systematic description of the entire system, and then focus the risk analysis on eu-LISA's responsibilities for design, development and information security management.

Given the importance of eu-LISA's responsibilities on the security management of the system, a security risk assessment is required, as foreseen by article 73 (3) (a) of the Regulation (EU) 2018/1240. This exercise is already on going in the framework of the analysis and design phase.

The aspects related to the testing phase are not in the scope of this DPIA, since they do not involve the use of personal data.

Following legal requirement (article 1, Regulation (EU) 2018/1240), the main purpose of the ETIAS is: "to enable consideration of whether the presence in the territory of Member States of third-country nationals exempt from the requirement to be in possession of a visa would pose a security, illegal immigration or high pandemic risk".

According to article 4 of Regulation (EU) 2018/1240, the objectives of ETIAS is to support competent authorities of Member States by: contributing to a high level of security; contributing to the prevention of illegal immigration; contributing to the protection of public health; enhance the effectiveness of border checks; supporting the objectives of SIS; contributing to the prevention, detection and investigation of terrorist offences or of other serious criminal offences; contribute to the correct identification of persons.

This DPIA has been carried out following the relevant European regulations framework and data protection authorities' guidelines. This assessment focus on actual or potential data protection risk to third country nationals and legal compliance risks, predominantly in relation to the EU GDPR, based on ETIAS regulation and on delegated and implementing acts available.

Outcome

The outcome of the assessment shows 21 risks. Based on four levels of risks, negligible/limited/significant/maximum, 16 out of 21 risks were identified as high risks (significant). After the mitigation measures proposed in chapter 8 the residual risks are reduced in a range between negligible and limited (low risk).

Taking into account the safeguards, security measures and controls to mitigate the risks, the processing of personal data does not represent a high risk to the rights and freedoms of natural persons and the processing of personal data will be carried out.

Nevertheless, eu-LISA will inform EDPS of the analysis and conclusion of this DPIA.

The table below shows the risks initially identified as high and the residual risk rating²:

	Risk	Initial Rating	Residual Rating
R1	To be able to save a draft, applicants shall provide their email address. Where the applicant e-mail address is not validated at the early stage of Data collecting, the hyperlink could be sent to a different person. Two-factors authentication as proposed by IA 2 using only mail address is not appropriate.	9- Significant	3- Limited
R2	The Store location of TCN application draft is not clearly defined by regulation or current architecture document.	9- Significant	3- Limited
R4	Since the contract between the Commission and the Payment provider is not finalized yet, it is impossible to assess if TCNs could exercise their rights before the transfer.	6- Significant	3- Limited
R5	TCN personal data (log Timestamp; IP address; Device information ³) could be collected without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.	6- Significant	2- Negligible
R6	TCN personal data (log Timestamp; IP address; Device information) could be stored without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.	6- Significant	2- Negligible
R8	Inadequate and incomplete information to the data subject on the processing activity, due to the fact that data subject is not aware about the transfer of his personal data to Ms competent authorities.	6 – Significant	4- Limited
R9	In the framework of the manual processing, during the hit verification process (article 4(g) of IA 8 Access, Amend, Erase),	9 – Significant	4- Limited

² This list includes identified high risks (Significant or more). Some risks (notably Risk 3; Risk 7; Risk 10; Risk 13 and Risk 14) are not included since their initial rating is already “limited” (see chapter 7, table 41)

³ These logs shall be stored in ETIAS storage location for a period of two years

	Risk	Initial Rating	Residual Rating
	National Units could export TCN's personal data. Possible lack of expert knowledge about data protection of the extracted personal data at the NUs level could have a negative impact on TCN fundamental rights (unlawful disclosure; processing beyond the purpose/without consent)		
R11	In the framework of the manual processing, usage of free text additional information given by the applicant can induce semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 27 of the Regulation; article 2 (3) (d) and (4), article 3, (3) and (4); article 4, (3); article 6 of the DA 7).	9 – Significant	4-Limited
R12	In the framework of the access, amend, erase request by the applicant, the usage of free text can induce semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 64 of the Regulation; article 4 (3) (b) of IA 13).	9- Significant	4- Limited
R15	In the framework of the request coming from TCN to amend/erase her/his personal data, there is a lack of clear and sufficient legal basis (or architecture information) concerning the storage location and retention period of these requests.	6- Limited	4- Limited
R16	Not appropriate use of the impact assessment tool by National competent authorities could lead to discrimination (generic research made in not-exact mode).	6- Limited	4- Limited
R17	At the time of drafting this DPIA the encryption protocol for "securing data in transit and at rest" is not defined yet. Resulting a possible unauthorized access to personal data.	9- Significant	3- Limited
R18	Technical deficiencies in the control of accesses through the carrier interface could allow unauthorized access to personal information.	6- Significant	3- Limited
R19	At the time of drafting this DPIA there is a lack of information concerning the technical or organizational process that could undermine the information integrity during the extraction data from the ETIAS DB to the Read-Only DB	6- Significant	3- Limited
R20	Following article 49, (2), immigration authorities querying EES could access additional categories of data by querying ETIAS central system. This information's go beyond the categories of data to be collected under the purpose of EES (details on family members and minors), Article 49, (3).	9 – Significant	3- Limited
R21	TCN Personal Data will be compared with specific risk indicators defined by the ETIAS Central Unit and ETIAS Screening Board art (7) (2) (c) and art (9)	9 – Significant	3- Limited



	Risk	Initial Rating	Residual Rating
	Wrong technical implementation, testing or maintenance of the risk indicators (as per art (74)) could lead to discrimination and profiling of the data subjects.		

Following the data protection risks assessment, the Mitigation measures identified to reduce or eliminate the high risks listed in Chapter 7 “Identify and Assess Risks” are:

		Mitigation measures
1	R1	Eu-LISA shall ensure that a technical solution is designed and developed to validate the e-mail address of the applicant at the early stage of the Data collection.
2	R2	Eu-LISA shall ensure the design and the development of a secure storage for data application Draft to enable the confidentiality, integrity and availability of the information contained to be respected. The security Risk assessment should include information on this asset.
3	R3; R4;	Eu-LISA shall ensure that all the legal requirements are implemented in order to enable that in the framework of the contract to be finalised between the commission and the payment service provider, only the unique identifier (ID) shall be transferred to the third parties (e.g. payment providers) in order to be processed in compliance with Data Protection regulation and principles.
4	R5, R6	Eu-LISA, after establishing whether the technical solutions make it possible to establish a link between the logs and the applicant, shall provide sufficient information about the processing of personal data on several levels, which is easily accessible to the data subjects.
5	R7	Based on the Train-the-Trainer approach, Eu-LISA shall provide all relevant information/training to raise the awareness of the Member States about the data relating to NUIs users stored in the CS.
6	R8	Eu-LISA shall ensure that the design of the “software for the purpose of manual processing of applications and for accessing and amending data for the purposes of appeals”, is implemented by including a disclaimer informing travelers that their data could be manually processed by competent authorities of one or more Member States. This will help to ensure the exercise of the right of appeal. (Article 4(1) of the IA 8 is an open list of specific functionalities)
7	R9	Eu-LISA shall share the outcomes of this assessment with Member States in order to raise awareness for them to elaborate mitigation measure at their level (e.g. authorized staff training)
8	R10	Eu-LISA shall ensure the design of a technical solution to fairly obtain the consent of data subject to the storage of logs of his/her authentication (Timestamp; IP address; Device information; Status of response) in the Central System. Eu-LISA shall also ensure the integrity of those log files.
9	R11; R12;	Eu-LISA shall ensure the development of all technical solutions to enable quality compliance of data entered by applicant or third party, in the free text space and limit as much as possible the use of free text as foreseen by legal basis (IA 1 Annex).
10	R13	Eu-LISA shall implement of all legal requirements, notably from AI 1 and his ANNEX, by ensuring that the applicant is informed prior to submission that no personal data should be included in the report and where personal data are nonetheless provided consents that the data will be redacted.
11	R14	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the data retention period in Central System of personal data related to the abuse reports, notably free text and supporting documents has the same duration as that foreseen for the personal data related to the application.
12	R15	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the storage location and the data retention period of applicant request concerning the access, rectification, completion, erasure of personal data, consent and abuse, are the same as those foreseen for the data related to the application.
13	R16	Eu-LISA shall deliver the training to MS competent authorities following the Train-The-Trainer approach on how the impact assessment tool will support Watchlist management.

14	R17	Eu-LISA shall ensure the design and the implementation of a secure encryption mechanism following best practices and requirement from legal basis to enable the integrity and the confidentiality of the data.
15	R18	Eu-LISA shall include the carrier interface in the scope of the Security Risk assessment and identify the appropriate measures which will ensure the confidentiality, integrity and availability of carrier interface and personal data that will be managed.
16	R19	Eu-LISA shall adopt all technical measures to ensure the integrity and the confidentiality of personal data in the extraction to the RODB
17	R20	Before giving an access to the information relating to the traveller's parental authority or legal guardian information ETIAS should validate that a prior search has been conducted in the EES under Article 26 of Regulation (EU) 2017/2226 and the search result indicates that the EES does not contain an entry record corresponding to the presence of the third country national on the territory of Member States.
18	R21	Eu-LISA shall adopt secure development standard during the development, testing and maintenance phases to guarantee that the risk indicators will be correctly developed and tested, as defined in article 7(c) article 33 and article 74(1).

Table 1 Mitigation measures

Terminology

a. Abbreviations and Acronyms

CS	Central System
CIR	Common Identity Repository
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECU	ETIAS Central Unit
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
ENU	ETIAS National unit
ETIAS	European Travel Information and Authorisation System
EBCGA (Frontex)	European Border and Coast Guard Agency
eu-LISA	European Union Agency for the Operational Management of Large Scale IT Systems in the Area of Freedom Security and Justice
ECHR	European Court of Human Rights
EUCJ	European Court of Justice
EUROPOL	European Union Agency for Law Enforcement Cooperation
GDPR	General Data Protection Regulation
IDA	Implementing and Delegated acts
MS	Member States
NUI	National Uniform interface
SLTD	Stolen and Lost Travel Document database (Interpol)
SIRENE	Supplementary Information Request at the National Entries
TCN	Third-Country National
TDawn	Travel Documents Associated with Notices database
TFEU	The treaty on the functioning of the European union
VE	Visa Exempt third country national
VIS	Visa Information System

Table 2 Abbreviations and Acronyms

b. Glossary

Accountability	Principle intended to ensure that the controller is in charge of ensuring compliance and being able to demonstrate that compliance. In the EUIs, the controller is legally speaking the 'Union institution, body, office or agency or the Directorate- General or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.
Adequacy decision	The European Commission may decide that a third country provides an adequate level of data protection. Transfers to adequate third countries do not require additional safeguards compared to transfers to recipients inside the EU. For more details, see chapter V of the Regulation.

Adequate safeguards	Measures for adducing an adequate level of protection when transferring personal data to third countries or international organisations, e.g. standard contractual clauses
Availability	Property of being accessible and usable upon demand by an authorized entity.
Border authorities	Border guard assigned in accordance with national law to carry out border checks as defined in point 11 of Article 2 of Regulation (EU) 2016/399
Carrier	Any natural or legal person whose profession it is to provide transport of persons (the Regulation (EU) 2016/399 – known also as Schengen Borders Code – Article 2).
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Control	In information security terminology, a measure that is modifying risk.
Data Controller	The data controller is the party that, alone or jointly with others, determines the purposes and means of the processing of personal data. The actual processing may be delegated to another party, called the data processor. The controller is responsible for the lawfulness of the processing, for the protection of the data, and respecting the rights of the data subject. The controller is also the entity that receives requests from data subjects to exercise their rights.
Data protection by design and by default	The principle that controllers must consider data protection both during the development and deployment and to have protective default settings (Article 27 of the Regulation).
Data Protection Authority (DPA)	Public authority charged for supervising the processing of personal data. The EDPS is the DPA for the EUIs.
Data Protection Impact Assessment (DPIA)	A structured process to manage the data protection risks of certain risky processing operations (Article 39 of the Regulation).
Data Protection Officer (DPO)	The DPO informs and advises the controller/EUI, EUI staff and data subjects on data protection issues and ensures, in an independent manner, the internal application of data protection rules in their EUI. DPOs are also the main contact point between EUIs and the EDPS. Every EUI has a DPO.
Data subject	Any natural person whose personal data you process, whether employed by your EUI or not.
ETIAS National Units	Competent authority as ETIAS National Unit designed by each Member State.
European Data Protection Board (EDPB)	The forum in which national DPAs, the EDPS and the European Commission cooperate to ensure consistent application of data protection rules throughout the EU. Replaced the WP29.
European Data Protection Supervisor (EDPS)	The Data Protection Authority for the EUIs (see the Regulation).
External borders	The Member States' land borders, including river and lake borders, sea borders and their airports, river ports, seaports and lake ports, if they are not internal borders.
General Data Protection Regulation	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

High epidemic risk	Means any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization (WHO) or the European Centre for Disease Prevention and Control (ECDC) and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.
Illegal immigration risk	Means the risk of a third-country national not fulfilling the conditions of entry and stay as set out in Article 6 of Regulation (EU) 2016/399
Lawfulness of processing	In order to lawfully process personal data, the processing has to fall under one of the situations listed in Article 5 of the Regulation, such as this being necessary for the performance of a task in the public interest assigned to a EUI by EU law.
Integrity	Property of accuracy and completeness
Operability	Principles of accessibility meaning that user interface components and navigation must be operable.
Perceivability	Principles of accessibility meaning that information and user interface components must be presentable to users in ways they can perceive.
Person responsible on behalf of the controller	Top management is accountable for compliance with the rules, but responsibility is usually assumed at a lower level ('person responsible on behalf of the controller' / 'controller in practice'). The business owner will in many cases be the responsible person.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1) GDPR). Data subjects may be identifiable directly (e.g. names) or indirectly (e.g. "a female Maltese Director-General in your EUI")
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR).
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Example: company organising an assessment centre for your EUI, based on an outsourcing contract
Profiling	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 that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) GDPR).
the Regulation	Regulation (EU) 2018/1240 (consolidated version 11/06/2019)
Right of information	Data subjects have the right to be informed about your processing of their personal data. Inform them by providing a data protection notice / privacy statement.
Right of access	Data subjects have the right to access their personal data held by a controller; some exemptions may apply (Article 17 of the Regulation (EU) 2018/1725)
Right of rectification	Data subjects have the right to rectify their personal data held by a controller when they are incorrect (Article 18 of the Regulation (EU) 2018/1725)

Right of erasure / right to be forgotten	Data subjects have the right to obtain erasure of their personal data held by a controller in some situations, such as when data are held unlawfully (Article 19 of the Regulation (EU) 2018/1725).
Risk	A possible event that could cause harm or loss or affect the ability to achieve objectives. Risks have an impact and a likelihood. Can also be defined as the effect of uncertainty on objectives.
Special categories of data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; processing of genetic data, biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation (Article 10 of The Regulation (EU) 2018/1725); data concerning criminal convictions and offences (Article 11 of The Regulation (EU) 2018/1725).
Supporting assets	Supporting Assets are physical components that support the processing of personal data. Supporting Assets include hardware (computers, removable storage media, hard drives, servers, workstations, etc.), software (operating systems, databases, business applications, etc.), networks, etc.
Third-country nationals	Any person who is not a Union citizen within the meaning of Article 20(1) TFEU and who is not covered by point 5 the Regulation (EU) 2016/399 (article 5).

Table 3 Glossary

1. Introduction

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereafter “eu-LISA”) is an EU Agency to provide a long-term solution for the operational management of large-scale IT systems, which are essential instruments in the implementation of the asylum, border management and migration policies of the EU. The Agency was established in 2011 by Establishing Regulation (EU) No 1077/2011 and started its activities on 1 December 2012. In 2018 eu-LISA was given a larger mandate which is detailed in Regulation (EU) 2018/1726.

The Agency currently manages Eurodac, the second generation Schengen Information System (SIS II) and the Visa Information System (VIS). Further to these, eu-LISA is developing the Entry/Exit System (EES), the European Travel Information Authorisation System (ETIAS) and the European Criminal Records Information System - Third-Country Nationals (ECRIS-TCN). These systems and the pre-existing ones are being built/adapted to ensure Interoperability - improved access to information stored in EU information systems and identity management at an EU level.

1.1. Structure of this DPIA

This assessment follows the structure of the eu-LISA’s DPIA template that is based on the EDPS’s Guidelines and the Article 29 Data Protection Working Party Guidelines. This structure is divided in chapters that are detailed below.

After enunciating the reasons to carry out this DPIA (Chapter 2 [Reasons for this DPIA](#)), this report outlines the methodology followed to describe the processing activities from a Data Protection perspective and assess Data protection risks (Chapter 3). For this purpose, this section carried on with the list of all the relevant documentation leading to a good understanding of the legal context. It was therefore firstly referred to with all the applicable regulations and secondly, to all the relevant guidelines and opinion of the EDPB and the EDPS while taking also into account specific documents from eu-LISA. At the end of Chapter 3, the extension and the limits of this DPIA were finally outlined.

In Chapter 4 “General Description of the Data Processing Operation”, this report identifies the role (controller, processor, sub-processors, recipients) of the different organisations/entities involved in the data processing along with the different data subjects, data categories and the legal basis for the processing. The internal and external context of the organisations affecting the processing activities were also detailed in this chapter.

In the next Chapter 5 “Systematic Description of the Data Processing Operation, the report shows in a more detailed way the different processing activities to highlight the processing operations step by step. For a good understanding of the system, in this part, the report details what are the data flows (i.e. where data comes from and where it goes), what are the assets supporting those data, how the different steps inside a sub processing are organised and especially what is the objective of each step. Those important points have been synthesised in different flowcharts for a better understanding and visualisation.

Then, Chapter 6 is dedicated to the assessment of the necessity and the proportionality of the processing activities. This analysis is made by referring to the ETIAS legal basis and to the information content in the ETIAS

[REDACTED]

feasibility study⁴, to the EDPS relevant guidelines⁵ and Opinion⁶ and to the principles issued from EUCJ and ECHR case law.

Chapter 7 “Identify and Assess Risks” shows the risks assessment based on an extensive analysis on Data protection principles. The eu-LISA template originally included this section in the annex; however, in order to clearly show the process and methodology underlying the analysis and assessment of data protection risks, this section include information regarding compliance with the Data Protection principles in the main part of the report.

In the following Chapter 8 “Measures to Mitigate Identified Risks”, the report addressed only the significant and maximum risks thanks to mitigation measures from this DPIA’s knowledge base mitigation measures, from the EDPS and EDPB recommendations.

Chapter 10 covers Conclusions and Recommendations including some specific recommendations to further mitigate those risks.

Finally an Action Plan was proposed (Chapter 11 “Action Plan”).

⁴ European Commission, Feasibility Study for a European Travel Information and Authorisation System (ETIAS) Final Report, 16 November 2016.

⁵ EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017

⁶ EDPS, Opinion 3/2017 EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS), 6 March 2017

2. Reasons for this DPIA

As a data processor in relation to the processing of personal data in the ETIAS Information System (art. 58 (1)), eu-LISAs' main responsibilities are to host the ETIAS Central System in its technical sites, define the design and technical development of the ETIAS Information System and ensure that the system is operated in accordance with the provisions of the Regulation, following technical specifications as adopted by euLISA's Management Board, subject to a favourable opinion from the Commission, in accordance with article 73 of the Regulation. Based on these provisions, the DPIA is carried out by eu-LISA – as a processor - serves as a tool to fulfil the principle of data protection by design and by default (DPbDD).

As a data controller in relation to information security management of the ETIAS Central System (art. 57 (1)), eu-LISA's main responsibility, shared with Member States ("ETIAS National Units") and Frontex ("ETIAS Central Unit"), is to take the necessary measures to ensure the security of the ETIAS Information System (art. 59). Based on art. 59, eu-LISA is considered to be joint controller with the Member States and Frontex regarding the security of processing of personal data. Following the requirements set up in art. 28 of Regulation 2018/1725, an arrangement between the joint controllers was not necessary because their respective responsibilities are determined by the Regulation to which the joint controllers are subject.

The ETIAS processing operations trigger the obligation to conduct a DPIA under Article 39 of Regulation (EU) 2018/1725, because the large-scale processing of special categories of personal data in ETIAS are "likely to result in high risks to the rights and freedoms of natural persons", without prejudice of other ETIAS data controllers' obligation to carry out their own DPIAs.

2.1. ☒ Processing included in a positive list provided by the EDPS - EDPS List (art. 39.4)

2.1.1. ☒ Exclusion databases

- ☒ Large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation)
- ☐ Internet traffic analysis breaking encryption (data loss prevention tools)
- ☐ e-Recruitment tools automatically pre-selecting/excluding candidates without human intervention

2.1. ☐ Positive threshold assessment - Criteria for high risks:

2.1.2. Scoring:

- ☐ Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting
- ☐ Automated-decision making with legal or similar significant effect
- ☐ Systematic monitoring
- ☐ Sensitive data or a highly sensitive nature
- ☐ Data processed on a large scale
- ☐ Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject
- ☐ Data concerning vulnerable data subjects

	☐ Innovative use or applying technological or organizational solutions that can involve novel forms of data collection and usage ☐ Preventing data subjects from exercising a right or using a service or a contract
2.1.3.	Threshold assessment document: ☐ Link: ☐ Annex:
2.2.	☐ Processing included in a negative list provided by the EDPS - EDPS List (art. 39.5) (If included in this list, a DPIA is not compulsory and would end here unless there are reasons to ground a DPIA. If so, detail these reasons in next checklist 'Decision of eu-LISA')
	☐ Management of personal files under Article 26 of the Staff Regulations as such ⁷ ☐ Standard staff evaluation procedures under Staff Regulations (annual appraisal) ☐ Standard 360° evaluations for helping staff members develop training plans ☐ Standard staff selection procedures ☐ Establishment of rights upon entry into service ☐ Management of leave, flexitime and telework ☐ Standard access control systems (non-biometric) ⁸ ☐ Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in public space)
2.2.	☒ Decision of eu-LISA (select the reason/s for this decision)
	☒ Generate knowledge and data protection culture in eu-LISA ☐ Analysis or audit of data processing activities of eu-LISA ☐ Improvement of the global process management of eu-LISA ☒ Systematic, methodical and documented control of the level of risk accepted in each data processing activity ☐ Exercise of accountability ☒ Embed privacy by design and other appropriate information security measures into the specification, design and build of systems and procedures ☐ Other:

Table 4 Legal basis

⁷ Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such.

⁸ E.g. badges to be swiped at entry points.

3. DPIA Methodology

The methodology adopted for the drafting of the ETIAS DPIA is fully aligned with the guidelines provided by the EDPS – [Accountability on the ground part I](#)⁹ and [part II](#)¹⁰, as amended in July 2019 - and by the Article 29 Working Party- [Guidelines on Data Protection Impact](#)¹¹. The approach adopted aims to respond to the specific characteristics of ETIAS, taking in account also the current situation and the potential future development of the System.

The structure of this assessment tends to answer to the following questions:

- Who does what?
- For what reason?
- How (with which means/support assets)?
- What do we collect?
- For how long?
- Who has access to personal data?
- What are the possible risks associated with each operation?
- What are the most appropriate mitigation measures to reduce or eliminate the identified risks?¹²

Thus, the general description of the system (Chapter 4) focuses on the roles (o), the internal (4.4) and the external (4.5) context, the lawfulness of the ETIAS processing operations. The systematic description shows in details, from a data protection perspective, the main steps of the processing activities (chapter 5). After the analysis of the necessity and proportionality of the processing activities (chapter 6 **Error! Reference source not found.**), risks related to each step are described and assessed in chapter 7. Finally chapter 8 lists and describes the mitigation measures proposed to reduce/eliminate the risks.

The DPIA is the result of a complex analysis process based on both legal and technical aspects. Given the early phase of the ETIAS design and development, the assessment is mainly focused on ETIAS regulation and implementing acts and the analysis is integrated with the technical elements currently available. In light of further development of the system new assessments may be required to update this DPIA.

⁹ EDPS, Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies. Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, v1.3 July 2019.

¹⁰ Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, v1.3 July 2019.

¹¹ Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 13 October 2017.

3.1. DPIA Team

Name	Role	Tasks
[REDACTED]	UNISYS – Project Manager	Advisor and reviewer
[REDACTED]	UNISYS – IT/Security specialist	DPIA Implementer
[REDACTED]	UNISYS – IT/Security specialist	DPIA Implementer
[REDACTED]	UNISYS – Data protection and Fundamental rights Consultant	Advisor/DPIA Implementer
[REDACTED]	UNISYS – IT/Security specialist	Reviewer
[REDACTED]	UNISYS – IT/Security specialist Data protection Consultant	Advisor
[REDACTED]	eu-LISA Project Manager Assistant	Advisor
[REDACTED]	eu-LISA – ETIAS Programme Manager	Advisor and reviewer
[REDACTED]	eu-LISA – Data Protection Officer	Advisor and reviewer
[REDACTED]	eu-LISA – DPO Assistant	Advisor
[REDACTED]	eu-LISA – Head of Information Security and Assurance Sector	Reviewer
[REDACTED]	eu-LISA Business Relations Management sector, Vice Chair of ETIAS AG	Reviewer
[REDACTED]	eu-LISA IT Officer – Architecture Sector	Reviewer
[REDACTED]	eu-LISA – Head of Business Relations Management sector, Chair of ETIAS AG	Reviewer

Table 5 DPIA Team

3.2. Guidelines, tools, methodologies, standards and opinions used in the DPIA

Both the descriptive and analytical parts of this report are based on the relevant legal framework of international law and EU law (3.2.1), on the relevant implementing and delegated acts (3.2.2), on the Opinions and Guidelines on DPIA principles and ETIAS in particular (3.2.3).

3.2.1. Legislative framework

No	ID	Title
1	Council of Europe	European Convention on Human Rights

No	ID	Title
2	Directive 2001/45/EC	Directive 2001/45/EC of the European Parliament and of the Council of 27 June 2001 amending Council Directive 89/655/EEC concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC)
3	2002/584/JHA	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States
4	Regulation (EC) No 767/2008	Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)
5	Regulation (EU) No 1077/2011	Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
6	2012/C 326/02	Charter of Fundamental Rights of the European Union
7	Regulation (EU) 2016/399	Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)
8	Regulation (EU) 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
9	Directive (EU) 2016/680	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
10	Regulation (EU) 2016/794	Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA
11	Regulation (EU) 2019/1896	Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624
12	Directive (EU) 2017/541	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
13	Regulation (EU) 2017/2226	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (also version consolidated on 11th of June, 2019)
14	Regulation (EU) 2018/1240	Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorization System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (consolidate version 11/06/2019)

No	ID	Title
15	Regulation (EU) 2018/1241	Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS)
16	Regulation (EU) 2018/1725	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
17	Regulation (EU) 2018/1725	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011
18	Regulation (EU) 2019/817	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA
19	Consequential amendment 2019/0001 (COD)	Proposal for a Regulation (EU) of the European Parliament and of the Council establishing the conditions for accessing the other EU information systems and amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxx [ECRIS-TCN]
20	Consequential amendment 2019/0002 (COD)	Proposal for a Regulation (EU) of the European Parliament and of the Council establishing the conditions for accessing other EU information systems for ETIAS purposes and amending Regulation (EU) 2018/1240, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861

Table 6 Legislative framework

3.2.2. Implementing and Delegated acts

Type	Act Name	The Regulation	Version Name	Version Date	Status
DA 1	Secure Account Service	Art. 6(4)	Final	22-02-2019	Final version considered.
DA 2	Verification Tool	Art. 31	Final	22-02-2019	Final version considered.
DA 3	Consent Tool	Art. 54(2)	Final	22-02-2019	Final version considered.
DA 4	Flagging	Art. 36(4)	Final	17-01-2020	Final version considered.
DA 5	Job Groups	Art. 17(3)	Final	06-05-2019	Final version considered.
DA 6	Payment Methods	Art. 18(4)	Final	21-10-2019	Final version considered.
DA 7	Content and Format of Add. Questions	Art. 17(5)	04-02-2020	04-02-2020	Act under circulation.

Type	Act Name	The Regulation	Version Name	Version Date	Status
DA 8	Screening Rules	Art. 33(2)	07-11-2019	07-11-2019	Act under discussion. The respective business processes and use cases represent a high-level approach.
IA 1	Report Abuse	Art. 15(5)	29-10-2020	29-10-2020	Final version considered.
IA 2	Public Website and App	Art. 16(10)	Final	23-03-2020	Final version considered.
IA 3	Format of Personal Data	Art. 17(9)	Final	16-08-2019	Act in written procedure.
IA 4	ETIAS Watchlist	Art. 35(7)	Final	01-03-2021	Act under discussion.
IA 5	Standard Form	Art. 38(3)	Final	10-05-2019	Final version considered.
IA 6	Operation of Carrier Gateway	Art. 45(2)	v00.42	18-11-2019	Act under discussion. The respective business processes and use cases represent a high-level approach.
IA 7	Carrier - Implementing Regulation	Art. 45(2)	To be released by COM	N/A	Act under discussion. The respective business processes and use cases represent a high-level approach.
IA 8	Access, Amend and Erase	Art. 73(3)(b)(i)(ii)	1_48_CT	31-10-2019	Act under discussion.
IA 9	Logs	Art. 73(3)(b)(iii)	Final	07-06-2019	Final version considered.
IA 10	Performance Requirements	Art. 73(3)(b)(iv)	v0.31	15-10-2019	Act under discussion.
IA 11	CAPs	Art. 73(3)(b)(v)	Final	07-06-2019	Final version considered.
IA 12	Central Repository	Art. 84(2)	v0_07	13-09-2019	This act is expected to be replaced by the IoP act for the CRRS.
IA 13	Data Quality Compliance	Art. 74(5)	v20	08-10-2019	Act under discussion.
IA 14	Query Tool	Regulation 2019/817	19-09-2019	19-09-2019	Act under discussion.
IA 15	Data Quality mechanisms	Regulation 2019/817	v0.9	15-09-2019	Act under discussion.
IA 16	UMF	Regulation 2019/817	0.1	18-09-2019	Act under discussion.

Table 7 Implementing and Delegated acts

3.2.3. Opinion and Guidelines

No	Author	Title
1	EDPS	Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies. Summary Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation (2.12.2018)
2	EDPS	Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit. (11.04.2017)
3	EDPS	Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019)
4	EDPS	Guidance on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects' rights (24.06.2020)
5	EDPS	Guidance Security Measures for Personal Data Processing Article 22 of Regulation 45/2001 (21.03.2016)
6	EDPS	Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA lists issued articles 39(4) and (5) of Regulation(EU) 218/1725
7	EDPS	Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). (24.04.2017)
8	EDPS	EDPS Opinion 3/2017 on the Proposal for a European Travel Information and Authorization System (ETIAS).(6.03.2017)
9	EDPS	Early Detection and Exclusion System Database (EDES-DB) Prior Checking Opinion Case 2016-0864 (4.10.2017)
10	EDPS	Formal comments of the EDPS on two proposals to establish the conditions for accessing other EU information systems for ETIAS purposes (13.03.2019)
11	ISO	ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment
12	Article 29 Data Protection Working Party	Guidelines on Data Protection Impact Assessment (DDPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679
13	Article 29 Data Protection Working Party	Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector
14	European Commission	Staff working document evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), Brussels, 8.9.2020 SWD(2020)174 final
15	European Parliament	The European Commission package of ETIAS consequential amendments Substitute impact assessment, December 2019

Table 8 Opinion and Guidelines

3.3. Extension and limits of the DPIA: Identify what has been left out of scope of the assessment

Following the guidance provided by the Article 29 Working Party and the EDPS, the approach taken in drafting

[REDACTED]

this evaluation aims to respond to the specific characteristics of ETIAS. Therefore, some precise methodological choices have been made to clearly define the scope and limits of the analysis, taking into account the current situation and the potential future development of the system.

DPIA is the result of a complex analysis process based on both legal and technical aspects. Given the early phase of the ETIAS development (the actual development of the system has not started yet). The assessment is mainly focused on ETIAS regulation and implementing/delegated acts and the analysis is integrated with the technical elements currently available. In light of further development of the system new assessments may be required to update this DPIA.

The presence of multiple joint controllers obliges to clearly set the boundaries of the analysis of the impact of processing activities on personal data, in order to let each controller, implement this report or perform his own DPIA. In particular, ETIAS DPIA focuses on the processing activities for which eu-LISA is responsible as data controller. However, the responsibility given by the EU legislator to eu-LISA to design and develop ETIAS requires that the description (general and systematic) of processing activities is comprehensive (Chapter 4 and 5).

The complementarity between ETIAS and EES, which translates, among other things, into sharing the IT infrastructure for dialogue with the Carriers, imposes another limitation. This report does not investigate the details of the analysis of the dialogue infrastructure (Carrier Gateway and Secure Web service/webmail) since these aspects are the subject of a specific DPIA commissioned in the framework of EES.

Furthermore, the analysis does not cover the processing of personal data within the framework of the test phase, since the data used are artificial and it would therefore be impossible to establish a violation of fundamental rights (Article 8 of the Charter of Fundamental Rights of the European Union).

Outside of Scope

1. Further technical developments not available during drafting and not defined yet by Implementing and delegated acts;
2. Responsibilities of National Units as Data Controller for ensuring data protection in the processing activities in ETIAS Central System which are not supported by the technical design under the scope of this DPIA;
3. Responsibilities of EBCGA/ETIAS Central Unit as Data Controller for ensuring data protection in the processing activities in ETIAS Central System which are not supported by the technical design under the scope of this DPIA;
4. Risk indicators for screening rules, since they shall be defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit after consultation of the ETIAS Screening Board;
5. Europol responsibility to ensure data protection in the framework of processing activities related to the watchlist and to the consultation of ETIAS Central System which are not supported by the technical design under the scope of this DPIA;
6. Dialogue infrastructures for carriers, since this topic falls on the scope of a dedicated DPIA;
7. Testing phase, since the approach is to use fake test data;
8. Interoperability components, since this topic falls on the scope of a dedicated DPIA;

4. General Description of the Data Processing Operation

In this chapter we will focus on the description of the data processing, taking into account the legal basis provided by the ETIAS The Regulation.

ETIAS system processes personal data of third country nationals exempt from the requirement to be in possession of a visa to enter the Schengen area. According to article 1 of The Regulation, the purpose of this processing is to enable consideration of “whether the presence of those third-country nationals in the territory of the Member States would pose a security, illegal immigration or high epidemic risk”. The process starts with the application made by a TCNS. A synthetic overview of the ETIAS system is reported in the following Figure 1 :

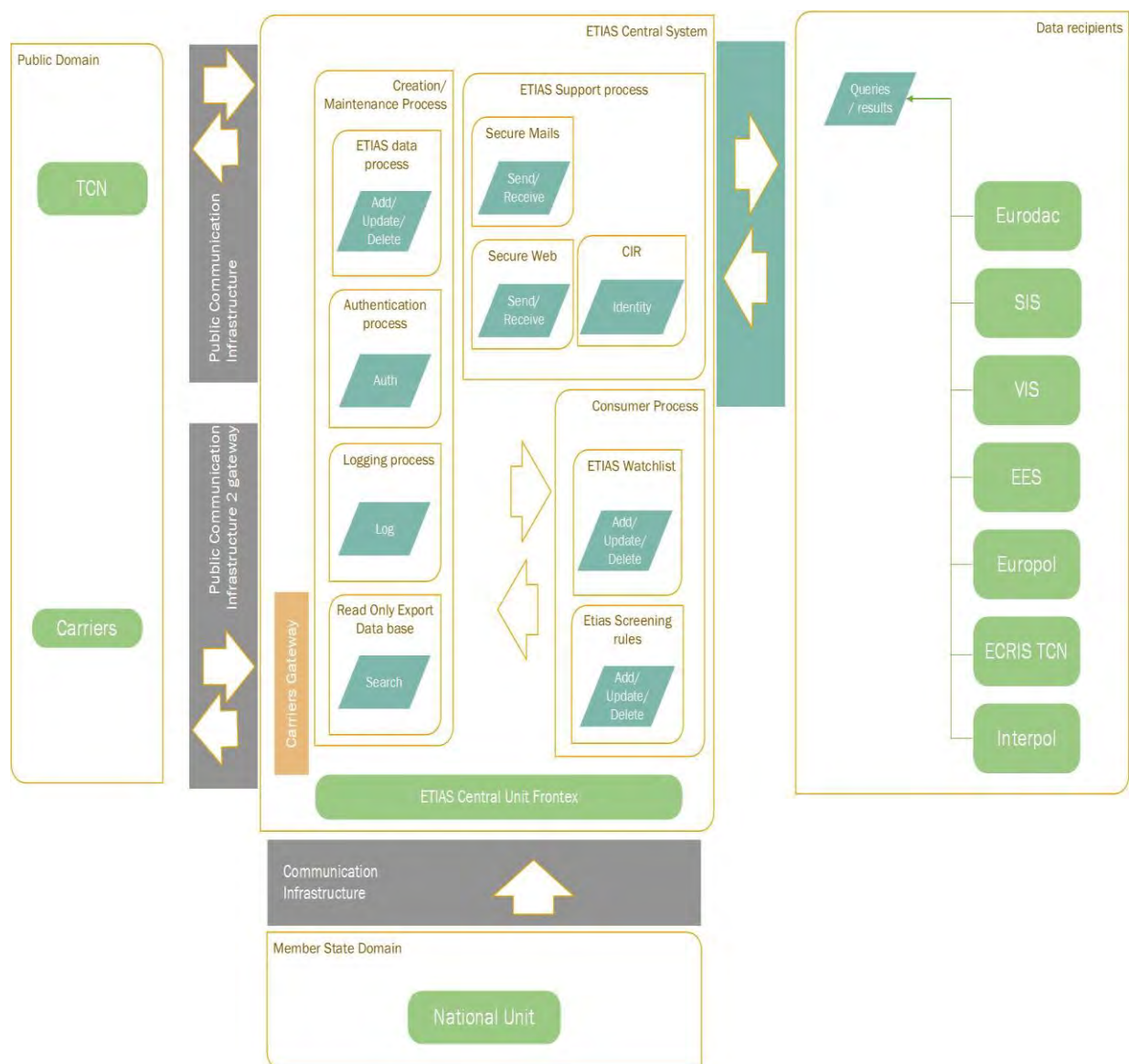


Figure 1 – ETIAS Synthetic overview

The nature of the data processing is automated, although, according to recital 24 of The Regulation, “whenever such comparison reveals that a correspondence (a ‘hit’) exists between any of the personal data or a combination thereof in the application and the specific risk indicators or the personal data either in a record, file or an alert in the above information systems or in the ETIAS watchlist, the application should be processed manually by the ETIAS National Unit of the Member State responsible. The assessment performed by the ETIAS National Unit should lead to the decision to issue the travel authorisation or not to do so”¹³.

4.1. Name and description of the data processing activity

Main Processing Operations			
	Name	Legal Base	Description
PA ₁	TCN Draft Application	Article 5(4) Implementing act Public Web Site	The process begins when TCN submits an application for a travel authorisation and fill an application form with the necessary data for this application, either on the public website or a mobile device application. Prior to submitting their application form, applicants shall be given the possibility to store, for a duration of up to 48 hours, the personal data entered.
PA ₂	Submitting application (TCN data collection)	Article 17; Article 19 ETIAS Regulation.	Upon submission, ETIAS will verify the TCN data by performing an Automated processing. If no hits are triggered, the travel authorisation is granted to the TCN and this information is communicated to him.
PA ₃	Automated Processing (Identifying hits in the application files)	Article 1; Article 22-23-25(2) ETIAS Regulation	Personal data of each applicant shall be automatically and individually processed by the ETIAS Central System to identify possible hit(s). In order to verify the application file against EU information systems, Europol and Interpol databases, the ETIAS Central System shall use the European Search Portal (ESP) to query those systems.
PA ₄	Manual Processing (in case one or more hits are reported)	Article 26-36(2)-36(3) ETIAS Regulation	Where the automated processing laid down in Article 20(2) to (5) has reported one or several hits, the application shall be processed manually by the ETIAS National Unit of the Member State responsible. Following the manual processing of the application, the ETIAS National Unit of the Member State responsible shall: (a) issue a travel authorisation; or (b) refuse a travel authorisation. In cases where there is doubt as to whether sufficient reasons to refuse the travel authorisation exist, the ETIAS National Unit of the Member State responsible shall have the possibility, including after an interview, to issue a travel authorisation with a flag

¹³ See also article 26 of The ETIAS Regulation.

			recommending to border authorities to proceed with a second line check.
PA 5	TCN requests access, rectification, completion or erasure of personal data, consent & abuse.	Article 64 ETIAS Regulation	ETIAS system has to guarantee, by design, rights of access, rectification, restriction, completion, erasure in relation to personal data of TCN.
PA6	Watchlist management	Article 34 ETIAS Regulation	ETIAS NUs and Europol shall introduce, amend or erase entry records in the ETIAS Watchlist based on the information related to terrorist offences or other serious criminal offences. Europol and Member States shall review and verify the continued accuracy of the data it entered to the ETIAS Watchlist regularly.
PA7	Watchlist review	Article 35(4) ETIAS Regulation	ETIAS NUs and Europol shall review and verify the continued accuracy of the data it has entered into the ETIAS watchlist regularly, and at least once a year.
PA8	Access to the ETIAS Central System for Border control and law enforcement purposes	Articles 50- 51- 52- 53 ETIAS Regulation	EU Authorities (EBCGA, Europol) and National competent authorities shall be able to consult the relevant personal data after submitting a consultation request
PA9	Carriers access for verification purposes	Article 45 ETIAS Regulation	Carriers, through the carrier gateway, get an 'OK/NOT OK' answer indicating whether or not the person has a valid travel authorization.
PA10	EBCGA support to carriers	Article 7 of the Commission implementing regulation for carrier article 7(2) m of the Regulation.	TCN and Carrier are able to ask for support to European Border and Coast Guard Agency.

Table 9 Main Processing Operations

4.2. Roles

4.2.1. Data Controller

4.2.1.1. Name and contact details

European Union Agency for the Operational Management of Large Scale IT System in the Area of Freedom, Security and Justice (eu-LISA)

Department : Security Unit

Legal Base:

- Article 57 of the Regulation:

"(...) In relation to information security management of the ETIAS Central System eu-LISA is to be considered a controller"

Responsibility: Information Security management

According to articles 59(1) and 69(1) eu-LISA is co-responsible with ETIAS Central Unit and National Units for security of processing

article 74(1) eu-LISA is responsible for technical Management of ETIAS

Email : eulisa-SECURITY@eulisa.europa.eu

4.2.1.2. Contact details of DPO

Email: dpo@eulisa.europa.eu

4.2.2. Joint Controller

4.2.2.1. ☐ N/A ☒ YES, fill in details below

European Border and Coast Guard Agency (EBCGA)

Department : ETIAS Central Unit

Email: Frontex@frontex.europa.eu

Legal Base :

- article 57(1) of The Regulation: *The European and Coast Guard Agency is to be considered a data controller in accordance with point (d) of article 2 of Regulation (EC) N. 45/2001 in relation to the processing of personal data in the ETIAS Central System*

Responsibility: Processing of personal data in ETIAS Central System

- article 75(1): *The European and Coast Guard Agency shall be responsible for*
 - the setting up and operation of the ETIAS Central System Unit and ensuring the conditions for the secure management of data stored in ETIAS*
 - the automated processing of applications and*
 - the ETIAS screening rules*

Contact details of DPO

Email: dataprotectionoffice@frontex.europa.eu

National Units

4.2.2.2. Legal Base :

- **article 57 (2)**

In relation to the processing of personal data in the ETIAS Central System by a Member State, the ETIAS National Unit is to be considered as controller in accordance with point 7 of Article 4 of Regulation (EU) 2016/679 (...).

Responsibility: Defining purpose and means of processing of personal data in ETIAS Central System by Member State

- **Article 35 – Responsibility and tasks regarding the ETIAS watchlist**

Responsibilities: Article 76 (1)

Each Member State shall be responsible for:

(a) the connection to the NUI;

(b) the organisation, management, operation and maintenance of the ETIAS National Units for the manual processing of applications for travel authorisation where the automated processing has reported a hit, as referred to in Article 26;

(c) the organisation of central access points and their connection to the NUI for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences;

(d) the management and arrangements for access of duly authorised staff of the competent national authorities to the ETIAS Information System in accordance with this Regulation and to establish and regularly update a list of such staff and their profiles;

(e) the set up and operation of the ETIAS National Units;

(f) entering data into the ETIAS watchlist related to terrorist offences or other serious criminal offences pursuant to Article 34(2) and (3); and

(g) ensuring that each of its authorities entitled to access the ETIAS Information System takes the measures necessary to comply with this Regulation, including those necessary to ensure the respect of fundamental rights and data security.

4.2.3. Data Processor/s and sub-processor/s of each processor

4.2.3.1. ☐ N/A ☒ YES, fill in details below and adapt as necessary to include all parties

4.2.3.2. Eu-LISA
Legal Base :

- **Article 58 (1), (2):**

1. eu-LISA is to be considered a processor in accordance with point (e) of Article 2 of Regulation (EC) No 45/2001 in relation to the processing of personal data in the ETIAS Information System.
2. eu-LISA shall ensure that the ETIAS Information system is operated in accordance with this Regulation

- **Article 45 (4) :** eu-LISA is responsible for security of Carriers gateway and personal data

contained in it and for process of extracting the personal data in the separate read-only database Responsibility 2 : Extracting personal data in the read-only data base • article 73: Responsibility of eu-LISA during the design and development phase • Article 74: Responsibility of eu-LISA following the entry in operation of ETIAS	
4.2.3.3.	Internal organisation(s)/entity(ies) ☒ N/A ☐ YES, fill in details below
4.2.3.4.	External organisation(s)/entity(ies) ☒ N/A ☐ YES, fill in details below Name and contact details Name of the organisation Address: Generic email Contract with the processor, or other legal act under EU or MS law ☐ Link: ☐ Attachment Contact details of DPO Email:
4.2.4.	Source/s of data – data providers
4.2.4.1.	MS and Europol In relation to ETIAS Watchlist personal data with the conditions and obligations as laid down in ETIAS Regulation.

Table 10 Roles

4.3. General description of the data processing activity

4.3.1. Processing operation

4.3.1.1. Description of the data processing

ETIAS provides to the Third Country National data collection tools (as website or mobile application) to allow applicant to create/amend/revoke a data file containing all information needed for their travel authorisation request.

Third Country National applies by filling in the online application form. The application files are

[REDACTED]

automatically processed by the ETIAS Central System which executes a detailed security check of each applicant to determine whether they would pose a security, illegal immigration or high pandemic risk. The personal data in the applications should be compared with the data present in a record, file or alert registered in an EU information system or database (the ETIAS Central System, SIS, the Visa Information System (VIS), the Entry/Exit System (EES), ECRIS-TCN or Eurodac), in Europol data or in the Interpol databases (the Interpol Stolen and Lost Travel Document database (SLTD) or the Interpol Travel Documents Associated with Notices database (TDAWN)). The personal data in the applications should also be compared against the ETIAS watchlist and screening rules (recital 23).

In case of automated processing reports one or several hits the ETIAS Central System automatically notifies the ETIAS Central Unit.

ETIAS Central Unit will perform an initial assessment to reject any false positives.

The ETIAS Central Unit should be responsible for verifying, in cases where the automated application process has reported a hit, whether the applicant's personal data correspond to the personal data of the person having triggered that hit.

Where a hit is confirmed or where doubts remain, the ETIAS Central Unit shall initiate the manual processing of the application. It shall ensure that the data it enters in the applications files are up to date and define, establish, assess ex ante, implement, evaluate ex post, revise and delete the specific risk indicators.

ETIAS Central Unit shall ensure that the verifications that are performed and their results are recorded in the application files. It shall also carry out regular audits of the processing of applications and of the implementation of the ETIAS screening rules, including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection.

ETIAS Central Unit shall furthermore be responsible for fulfilling a number of support tasks such as ensuring that the necessary notifications are sent and providing information and support. It should be operational 24 hours a day, 7 days a week.

Where the data does not match, and no other hit has been reported during automated processing, the ETIAS Central Unit deletes the false hit from the application file and the ETIAS Central System automatically issues a travel authorisation.

When the automated processing has reported one or several hits, the application will be processed manually by the ETIAS National Unit of the Member State responsible. This ETIAS National Unit shall have access to the application file and any linked application files, as well as to any hits triggered during the automated processing. The ETIAS Central Unit informs the ETIAS National Unit of the Member State responsible whether one or several other Member States or Europol were identified as having entered or supplied the data that triggered the hit.

When the ETIAS National Unit of the Member State responsible deems the information provided by the applicant in the application form to be insufficient to enable it to decide whether to issue or refuse a travel authorisation, it may request additional information or documentation from the applicant. The ETIAS National Unit of the Member State responsible shall request additional information or documentation upon the request of a Member State consulted (article 27 (1)).

Following the manual processing of the application, the ETIAS National Unit of the Member State responsible can issue the travel authorisation; or refuse it.

ETIAS also allows consultation by the designated authorities which are entitled to request consultation of data stored in the ETIAS Central System in order to prevent, detect and investigate terrorist offences or other serious criminal offences.

An operating unit submits a reasoned electronic or written request for consultation of a specific set of data stored in the ETIAS Central System to a central access point.

Upon receipt of the request, the central access point shall verify the fulfilment of the access conditions, including by checking whether each request for consultation of data is duly justified.

If the conditions for access are fulfilled, the central access point shall process the request. The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the operating unit that made the request in such a way that the security of the data is not compromised.

4.3.1.2. Purpose(s) of the data processing

The main purpose of the ETIAS data processing activity, according to Article 1 of The Regulation is :

To enable consideration of whether the presence in the territory of Member States of third-country nationals exempt from the requirement to be in possession of a visa would pose a security, illegal immigration or high pandemic risk.

According to article 4 of The Regulation the objectives of ETIAS are:

- Record new travel request by the third country national, including children and vulnerable people.
- Compare the personal data against EU information system to identify possible hit(s).

This will:

- Contribute to a high level of security
- Contribute to the prevention of illegal immigration
- Contribute to the protection of public health
- Support the objectives of SIS
- Contribute to the prevention, detection and investigation of terrorist offences or of other serious criminal offences
- Validate manually if there is a hit that is not a false positive. If needed, additional information can be request from the Third Country National.
- Give an access to Europol and to the Member State's law enforcement authorities.

4.3.1.3. Data processing for further processing

☒ N/A

☐ YES, if so specify the further purpose:

☐ Archiving in the public interest

☐ Scientific or historical research purposes

☐ Statistical purposes

Safeguards in place to ensure data minimisation:

☐ Pseudonymisation

☐ Any other, specify:

☐ Other further purposes, specify:

☐ Compatibility test result:

Table 11 Processing operation

4.3.2. Data subjects (list of categories of persons whose data are processed)

4.3.2.1. Internal to the organisation:

☐ N/A

☒ YES, data subjects:

Eu-LISA Staff - Operational management

The Regulation (article 69) eu-LISA shall keep logs of all data processing operations within the ETIAS Information System. Those logs shall include the staff member id having performed an access to the ETIAS Information system, however this information should be considered as business data and not personal.

4.3.2.2. External to the organisation:

☐ N/A

☒ YES, data subjects:

Applicant

As defined in the Regulation Article 2 ETIAS applies to the following categories of third-country nationals:

(a) nationals of third countries listed in Annex II to Council Regulation (EC) No 539/2001(6) who are exempt from the visa requirement for intended stays in the territory of the Member States of a duration of no more than 90 days in any 180-day period;

(b) persons who, pursuant to Article 4(2) of Regulation (EC) No 539/2001, are exempt from the visa requirement for intended stays in the territory of the Member States of a duration of no more than 90 days in any 180-day period;

(c) third-country nationals who are exempt from the visa requirement and who fulfil special conditions (letter (i) and (ii) of article 2 (1)

The Regulation (article 2) also defines a list of exclusion for this regulation:

(a) refugees or stateless persons

(b) third-country nationals who are family members of a Union citizen

(c) third-country nationals who are family members of a third-country national enjoying a right of free movement equivalent to that of Union citizens, under an agreement between the Union and its Member States on the one hand and a third country on the other, and who hold a residence card pursuant to Directive 2004/38/EC or a residence permit pursuant to Regulation (EC) No 1030/2002;

(d) holders of residence permits referred to in point 16 of Article 2 of Regulation (EU) 2016/399;

(e) holders of uniform visas;

(f) holders of national long-stay visas;

(g) nationals of Andorra, Monaco and San Marino and holders of a passport issued by the Vatican City State or the Holy See;

(h) nationals of third countries who are holders of a local border traffic permit issued by the Member States pursuant to Regulation (EC) No 1931/2006 of the European Parliament and of the Council (1) when such holders exercise their right within the context of the Local Border Traffic regime;

(i) persons or categories of persons referred to in points (a) to (f) of Article 4(1) of Regulation (EC) No 539/2001;

- (j) *third-country nationals holding diplomatic or service passports who have been exempted from the visa requirement pursuant to an international agreement concluded by the Union and a third country;*
- (k) *persons who are subject to a visa requirement pursuant to Article 4(3) of Regulation (EC) No 539/2001;*
- (l) *third-country nationals exercising their right to mobility in accordance with Directive 2014/66/EU (2) or (EU) 2016/801 (3) of the European Parliament and of the Council.*

Following article 17 of the Regulation, other Data subjects could be identified:

Commercial intermediaries authorised by the applicant

Article 17(2)m : "in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration".

Authorized person by the applicant

Article 17(2)m

Person exercising parental authority or legal guardianship

Article 17(2)k : "for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian"

Parents of the applicant

Article 17(2)a : " surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant"

Visited family members of the applicant in a conflict or war zone

DA 07, art. 3 (3); f)

The selection of multiple reasons and sub-reasons shall be possible. In case the applicant chooses the field "family visit", the applicant shall be presented with the following instruction: "Please provide first name, surname and residence of the indicated family member(s)." and shall be presented with a free text field.

Family member with whom the applicant has family ties (status of family member)

Article 17(2)l(ii) the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties;

Table 12 Data subjects

4.3.3.1. List of data categories which are processed (by category of data subject)

Personal Data for Visa Exempt third country national

The Regulation (article 17)

- surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant
- other names (alias(es), artistic name(s), usual name(s)) if any
- other nationalities
- type, number and country of issue of the travel document
- the date of issue and the date of expiry of the validity of the travel document
- the applicant's home address or, if not available, his or her city and country of residence
- email address and, if available, phone numbers
- education (primary, secondary, higher or none)
- current occupation (job group); where the application is subject to the manual processing in accordance with the procedure laid down in Article 26, the Member State responsible may in accordance with Article 27 request that the applicant provide additional information concerning his or her exact job title and employer or, for students, the name of their educational establishment;
- Member State of first intended stay, and optionally, the address of first intended stay
- for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian
- where he or she claims the status of family member referred to in point (c) of Article 2(1):
- his or her status of family member
- the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties
- his or her family ties with that family member in accordance with Article 2(2) of Directive 2004/38/EC
- in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration.
- in addition, the applicant shall provide answers to the following questions:
- whether he or she has been convicted of any criminal offence listed in the Annex over the previous 10 years and in the case of terrorist offences, over the previous 20 years, and if so when and in which country
- whether he or she has stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay
- whether he or she has been the subject of any decision requiring them to leave the territory of a Member State or of any third countries listed in Annex II to Regulation (EC) No 539/2001 or whether

they were subject to any return decision issued over the previous 10 years.

The ETIAS watchlist shall be composed of data consisting of one or more of the following items:

- surname
- surname at birth
- date of birth
- other names (alias(es), artistic name(s), usual name(s))
- travel document(s) (type, number and country of issuance of the travel document(s))
- home address
- email address
- phone number
- the name, email address, mailing address, phone number of a firm or organisation
- IP address
- If available: first name(s), place of birth, country of birth, sex and nationality.

Authorised staff (article 60; 70; 74 of the Regulation)

- the staff member ID.

4.3.3.2. Special categories of personal data

☒ N/A

☐ YES, list special categories of personal data¹⁴ which are processed (by category of data subject):

4.3.3.3. If applicable, indicate the reasons under article 10(2) allowing the processing of the special categories of data:

- a) ☐ the data subject has given explicit consent to the processing of those personal data for one or more specified purposes
- b) ☐ the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security
- c) ☐ the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent
- d) ☐ the processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade union aim
- e) ☐ the processing relates to personal data which are manifestly made public by the data subject
- f) ☐ the processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice is acting in its judicial capacity
- g) ☐ the processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the

¹⁴ Article 10(1) of The Regulation

right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

- h) ☐ the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or pursuant to contract with a health professional
- i) ☐ the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices
- j) ☐ the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union law

4.3.3.4. The data being processed contain sensitive data which fall(s) under article 11 'criminal convictions and offences':

☐ N/A

☒ Yes,

- list by category of data subject:

TCNs (Data subject):

Criminal records

- the basis for the processing has been laid down in the following Union law (please provide reference to the legal text):

The Regulation

Article 17 (4)

4. In addition, the applicant shall provide answers to the following questions:

(a) whether he or she has been convicted of any criminal offence listed in the Annex over the previous 10 years and in the case of terrorist offences, over the previous 20 years, and if so when and in which country; (b) whether he or she has stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay;

(c) whether he or she has been the subject of any decision requiring him or her to leave the territory of a Member State or of any third countries listed in Annex II to Regulation (EC) No 539/2001 or whether he or she was subject to any return decision issued over the previous 10 year

Article 23 (1)

For the purposes of point (e) of Article 4, the ETIAS Central System shall compare the relevant data referred to in points (a), (b) and (d) of Article 17(2) to the data present in SIS in order to determine whether the applicant is the subject of one of the following alerts: (a) an alert on missing persons; (b) an alert on persons sought to assist with a judicial procedure; (c) an alert on persons for discreet checks or specific checks

Article 43 (1)

1. The ETIAS watchlist shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence. (...)

Table 13 Data categories

4.3.4. Recipients of the data

4.3.4.1. Internally in eu-LISA:

☐ N/A

☒ YES, list recipients:

authorised staff member

Legal Base: the Regulation (article 69; 70)

“eu-LISA shall keep logs of all data processing operations within the ETIAS Information System. (...)”.

4.3.4.2. Outside eu-LISA (within EU/EEA):

☐ N/A

☒ YES, list recipients:

ETIAS Central Unit

Legal Base: The Regulation(article 13)

ETIAS NATIONAL UNIT

The Regulation(article 28)

Data subject, Commercial intermediary and Parental Authority/Legal Guardian

The Regulation(article 15)

Europol

Legal Base:

- **article 1 (2)**

may consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence.

Legal Base:

- **article 35 (1)**

Before Europol or a Member State enters data into the ETIAS watchlist, it shall:

(a) determine whether the information is adequate, accurate and important enough to be included in the ETIAS watchlist;

(b) assess the potential impact of the data on the proportion of applications manually processed;

(c) verify whether the data correspond to an alert entered in SIS.

- **article 1 Regulation UE 2018/1241**

Regulation (EU) 2016/794 is amended as follows:

(1) Article 4(1) is amended as follows:

(a) the following points are added: '

(n) manage the ETIAS watchlist in accordance with Articles 34 and 35 of Regulation (EU) 2018/1240 of the European Parliament and of the Council (*);

(o) enter data into the ETIAS watchlist related to terrorist offences or other serious criminal offences obtained by Europol, without prejudice to the conditions regulating Europol's international cooperation;

Border authorities

The Regulation(article 47 a, c, d(2); article 39(1); article 44(6)

Carriers

The Regulation(Art 13 (3); article 45; article 46)

Immigration authorities

The Regulation(article 49)

SIRENE office

The Regulation(article 23)

ECBGA

The Regulation(article 22)

European Data Protection Supervisor

The Regulation(article 67)

Table 14 Recipients of the data

4.3.5. International data transfers

4.3.5.1. Transfer outside of the EU or EEA:

☐ N/A, transfers do not occur and are not planned to occur

☒ YES, list recipient/s and country/ies to which the personal data is transferred:

- **Immigration Authorities**

The Regulation Article 65 (2)

By way of derogation from Article 49 of this Regulation, if necessary for the purpose of return, the immigration authorities may access the ETIAS Central System to retrieve data to be transferred to a third country in individual cases only where all of the following conditions are met:

(a) a prior search has been conducted in the EES in accordance with Article 26 of Regulation (EU) 2017/2226; and

(b) this search indicates that the EES does not contain data concerning the third-country national to be returned.

- **Carriers**

Carrier are by default outside of EU/EEA. The answer to the request made by Carriers in ETIAS Information System may be considered a personal data.

The Regulation Article 45 (2)

The ETIAS Information System shall, through the carrier gateway, provide the carriers with an 'OK/NOT OK/not applicable' answer indicating whether or not the person has a valid travel authorisation. If a travel authorisation has been issued with limited territorial validity in accordance with Article 44, the response provided by the ETIAS Central System shall take into account the Member State(s) for which the authorisation is valid as well as the Member State of entry indicated by the carrier. Carriers may store the information sent and the answer received in accordance with the applicable law. The OK/NOT OK answer shall not be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

4.3.5.2. Transfer to international organisation/s:

☐ N/A, transfers do not occur and are not planned to occur

☒ YES, list names of the international organisations to which the data is transferred:

- **Interpol**

The Regulation Article 65 (1)

1. Personal data stored in the ETIAS Central System shall not be transferred or made available to a third country, to an international organisation or to any private party with the exception of transfers to Interpol for the purpose of carrying out the automated processing referred to in points (b) and (l) of Article 20(2) of this Regulation. Transfers of personal data to Interpol are subject to the provisions of Article 9 of Regulation (EC) No 45/20

The Regulation Article 20 point 2(b)

"whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD;"

The Regulation Article 20 point 2(l)

"(l) whether the travel document used for the application corresponds to a travel document recorded in a file in TDAWN;"

4.3.5.3. Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision¹⁵

☒ Transfer subject to appropriate safeguards¹⁶, specify:

a) ☒ a legally binding and enforceable instrument between public authorities or bodies

b) ☐ standard data protection clauses adopted by the Commission

c) ☐ standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission

d) ☐ binding corporate rules, ☐ codes of conduct or ☐ certification mechanisms, where the processor is not a EU¹⁷

e) ☐ contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation

f) ☐ administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

4.3.5.4. Derogations from the prohibition of transfer of the data outside the EU¹⁸

☒ N/A

☐ YES, specify the condition that applies:

a) ☐ the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards

b) ☐ the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

c) ☐ the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

d) ☐ the transfer is necessary for important reasons of public interest

e) ☐ the transfer is necessary for the establishment, exercise or defence of legal claims

f) ☐ the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

g) ☐ the transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest

Table 15 International data transfers

¹⁵ Article 47 of The Regulation

¹⁶ Article 48(2) and 48(3) of The Regulation

¹⁷ EU Institution or body.

¹⁸ Article 50 of The Regulation

4.4. Internal context of the data processing in the organization

The European Commission first introduced the idea of a ETIAS in April 2016 in the Communication "Stronger and Smarter Information Systems for Borders and Security"¹⁹ and adopted the proposal²⁰ on 16 November 2016. After negotiations with the European Parliament and the Council the ETIAS Regulation (EU) 2018/1240 was adopted on 12 September 2018 and entered into force on 9 October 2018.

ETIAS, once fully implemented, will enable the advance authorisation of visa-exempt travellers when crossing the external borders and will in particular impose a new check to be carried out by carriers to those travellers.

While currently carriers only check whether visa-exempt travellers have a travel document, with ETIAS, carriers will also check whether they have a valid travel authorisation. Travellers will have to make an online application to obtain an ETIAS travel authorisation prior to travelling to the Schengen area. At check in, air and waterborne carriers, as well as carriers transporting groups overland by coach, will have to verify the status of the travel document required for entering the Schengen area, including verifying the validity of the ETIAS travel authorisation. The carrier will send a query to the carrier gateway and will receive an "OK/NOK" response. A carrier can still board a traveller that received a NOK answer at its own risk.

Following the regulation 2018/1240, eu-LISA is to be considered a data Controller "in relation to information security management of the ETIAS Central System" (article 57) and a data processor in relation to the processing of personal data in the ETIAS Information System eu-LISA" (article 58). Moreover, eu-LISA has the responsibility to design and develop the architecture of the system including its communication infrastructure. Due to this specific legal provisions, the EDPS has assigned to eu-LISA the responsibility to perform a DPIA²¹.

Therefore, it should be stressed that this DPIA report can help the European Border and Coast Guard Agency (EBCGA) and MS to identify risks related to the processing activities in which there are data controller. Thus, this document does not pretend to replace the specific risks assessments the EBCGA and MS must perform. Each actor should assess the specific data protection risks related to these data processing activities, based on their specific borders processing activities management in the light of the European regulations and their national implementation.

In order to give a comprehensive description of the ETIAS processing activity, useful to prepare the assessment of the data protection impact, it is important to highlight two main aspects which show the complexity of the internal context in the organization, according to The Regulation:

- the presence of multiple controllers (joint-controllers)
- the interactions with other EU Information systems

4.4.1. Joint controllers:

According to article 57 of the Regulation purpose and means of ETIAS data processing are determined by, at least, 3 different controllers. European Border and Coast Guard Agency and National Units are to be considered controllers in relation to the processing of personal data in the ETIAS Central System; National Units competent

¹⁹ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/communication_on_stronger_and_smart_borders_20160406_en.pdf

²⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A0731%3AFIN>

²¹ EDPS, Letter to eu-LISA DPO "ETIAS data protection impact assessment: preliminary guidance (case 2019-0495)", Brussels, 13th May 2020.

authorities are joint controllers in relation to the watchlist; eu-LISA is to be considered a controller in relation to information security management.

As stated by EDPS in its guidelines²², the coexistence of multiple controller should not have a negative impact on the protection of the fundamental rights of data subjects. Therefore, "the data subject may exercise his or her rights under the Regulation (EU) 2018/1725 in respect of and against each of the controller"²³.

In other words, the complexity of the internal organization laid down by the EU law, may not limit data subjects from exercising their rights under EUDPR, specifically regulated under Chapter III of Regulation (EU) 2018/1725 (such as the rights of access and rights to rectification, to erasure, to data portability and to object to data processing).

4.4.2. Interactions with other EU information systems

eu-LISA oversees providing multiple Information systems on behalf of the Member States (MS) that were deemed essential for the implementation of the asylum, border management and migration policies within the EU.

Currently managing the second-generation Schengen Information System (SISII), Eurodac (the Fingerprint data base for asylum applications) and the Visa Information System (VIS), eu-LISA also oversees the development of the Entry/Exit System (EES), the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN) and the European Travel Information Authorisation System (ETIAS).

Interoperability is a key component of the ETIAS data processing. This interoperability with other EU information systems should be enabled following the article 11 of The Regulation

According to recital (77), ETIAS Regulation was adopted "in order to integrate this Regulation into the existing legal framework and to reflect the necessary operational changes for eu-LISA and the European Border and Coast Guard Agency, Regulations (EU) No 1077/2011 (1), (EU) No 515/2014 (2), (EU) 2016/399, (EU) 2016/1624 (3) and (EU) 2017/2226 (4) of the European Parliament and of the Council should be amended".

Following article 11 of ETIAS Regulation, interoperability between the ETIAS Information System, other EU information systems and Europol data shall be established to enable the verification referred to in Article 20.

The personal data in the applications shall be compared with the data present in a record, file or alert registered in an EU information system or database (the ETIAS Central System, SIS, the Visa Information System (VIS), the Entry/Exit System (EES) or Eurodac), in Europol data (...).

Recital 58 of ETIAS regulation states that ECRIS-TCN would be automatically consulted when examining ETIAS applications. Therefore, the European Commission in its proposal stated that it was not necessary to further justify the necessity and proportionality of the extension of the scope of ECRIS-TCN²⁴. EU Agency for Fundamental rights (FRA) expressed serious concerns about using "ECRIS-TCN data for immigration law enforcement purposes outside of criminal proceedings"²⁵. EDPS correctly pointed out that the reference to ECRIS-TCN in Recital 58 of the ETIAS Regulation cannot be considered as sufficient to justify an expansion of

²² EDPS, EDPS Guidelines on the concepts of controller, processor and joint controllership under The Regulation (EU) 2018/1725, 7 November 2019, p. 30.

²³ Article 28 (3) of The Regulation (EU) 2018/1725.

²⁴ See The European Commission package of ETIAS consequential amendments Substitute impact assessment, December 2018 pp 18-22.

²⁵ FRA, 'Opinion of the European Union Agency for Fundamental Rights concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information System' (2015) 3

the ECRIS-TCN scope. Furthermore, article 20 of the ETIAS Regulation specifically – and exhaustively – lists the systems that ETIAS will query and for what reason. This list does not include the ECRIS-TCN.

This DPIA aims to highlight once more the position expressed by EDP: “broadening of the use of an existing system would be difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law”²⁶. However, it falls outside of the scope of this DPIA to make a judgement on the compliance of the legal basis with the data protection principles.

4.5. External context of the organization and the data processing

The external context of ETIAS plays a particularly important role given the complexity of this system in which multiple actors are involved in synergy.

The preparatory work for ETIAS is the result of interactions with actors outside the agency. To ensure the greatest possible effectiveness of the system and to adapt the design to the needs and requirements of external stakeholders, within the constraints imposed by the European legislator, eu-LISA has conducted and continues to conduct periodic consultations and negotiation processes mainly with the member states and other EU agencies involved in the operation of ETIAS.

Before explaining in detail how consultations with external actors have taken place so far and how they have been integrated into the drafting of this DPIA, it is also important to indicate which entities and organisations (other than EU institutions and member states) are involved in the functioning of ETIAS

4.5.1. External organizations/entities involved:

In the aim to achieve its scope, ETIAS data processing activities implies two main external (from EU) organizations/entities:

- Carriers and
- Interpol

• Carriers

The Use of ETIAS by carriers is defined by articles 45 and 46 of The Regulation: “[a]ir carriers, sea carriers and international carriers transporting groups overland by coach shall send a query to the ETIAS Information System in order to verify whether or not third-country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation”²⁷. All aspects related to the carrier gateway and the web services interface fall out of the scope of the present report, and are tackled by a specific DPIA performed in the framework of EES WS.

• Interpol

According to the article 12 of The Regulation, “[T]he ETIAS Central System shall query the Interpol Stolen and Lost Travel Document database (SLTD) and the Interpol Travel Documents Associated with Notices database (TDawn). Any queries and verification shall be performed in such a way that no information shall be revealed

²⁶

²⁷ Article 45(1) of The Regulation.

to the owner of the Interpol alert". Following article 65 of ETIAS Regulation, the transfer of personal data to Interpol for the purpose of carrying out the automated processing referred to in points (b) and (l) of Article 20(2), is the only exception to the ban of transferring personal data to a third country, to an international organisation or to any private party.

4.5.2. Consultation of other parties

Perform a DPIA is a joint exercise in which different and complementary expertise are required. That is why different actors involved in the design, have been consulted all along the preparation of this assessment. Internally to eu-LISA BRM, Architecture and Security sectors gave relevant contribution to this report.

The outcomes of consultation between eu-LISA and multiple external stakeholders have also been included as inputs in the drafting of the present report, especially from:

- Advisory Group (AG): Business Use Cases have been discussed and elaborated with the joint participation of Member State's representatives, Frontex (EBCGA) and Europol.
- Smart Borders Committee/ ETIAS Expert Group: eu-LISA supported EU Commission and Member States in elaborating the implementing acts and the delegated acts, which served as source for the stakeholder's requirements elicitation.
- Tender Technical Specifications (TTS): External contractors with expertise on design, security by design and data protection by design, supported eu-LISA for the elaboration of the ETIAS technical specifications. Member States were consulted and formally adopted these technical specifications after a favourable opinion of the Commission.
- Program Management Board (PMB), Management Board (MB) and Commission: Following article 73 (3) of ETIAS regulation, the ETIAS technical specifications have been adopted by eu-LISA's Management Board, after a favourable opinion from the Commission. eu-LISA's Management Board approval was supported by the Programme Management Board recommendation after their review of the ETIAS TTS.

4.6. Lawfulness of the data processing operation

4.6.1. Legal basis and necessity for processing

- 4.6.1.1. ☒ 5(1)(a) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body (a task attributed to your Agency by the legislation) (e.g. "Staff Regulations Article X, as implemented by eu-LISA implementing rules Article Y", instead of just "Staff Regulations")
- ☐ 5(1)(a2) Necessary for the management and functioning of the Agency (required for the functioning of the Agency. Not all processing operations required for the functioning of the Agency are explicitly mandated by legislation) (e.g. keeping an internal staff directory, access control)
- ☒ 5(1)(b) Necessary for compliance with a legal obligation to which the controller is subject; (a specific legal obligation to process personal data) (e.g. obligation to publish declarations of interest in an EU agency's founding regulation)
- ☐ 5(1)(c) Necessary for performance of a contract to which the data subject is party or in order

	to take steps at the request of the data subject prior to entering into a contract (this is rarely used by the EU institutions): ☒ 5(1)(d) The data subject has given consent to the processing of his or her personal data for one or more specific purposes (if persons have given free and informed consent) (<i>e.g. a photo booth on EU open day, optional publication of photos in the internal directory</i>) ☐ 5(1)(e) Necessary in order to protect the vital interests of the data subject or of another natural person (<i>e.g. processing of health information by first responders after an accident when the person cannot consent</i>)
4.6.1.2.	☒ In case the basis for the processing referred to in article 5(1)(a) and/or 5(1)(b) apply, the basis for the processing has been laid down in the following Union law (please provide reference to the legal text) 5(1) (a) : Articles 1 (4),7 and 19 (1) (II) of eu-LISA Regulation²⁸ 5(1)(b) : Article 6²⁹ and article 57 (1), 58 and 69 of ETIAS regulation 5 (1) (d) : Article 6 (2) (i) and 24 (6) (c) (ii), 54 (2) of ETIAS regulation as amended by DA 3; Article 6 (I) ETIAS regulation as amended by IA 2. Following the above mentioned legal provisions, for the purpose of facilitating a new application after the expiry of the validity period of an ETIAS travel authorisation, the application file may be stored in the ETIAS Central System for an additional period of no more than three years after the end of the validity period of the travel authorisation and only where, following a request for consent, the applicant freely and explicitly consents by means of an electronically signed declaration (consent tool).
4.6.1.3.	☒ [Elaborate on the Lawfulness of Special Categories of Personal data –if they are part of the data processing - according to Article 10 and 11] Following article 10 (g) of EULs DPR “The processing is necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.” Following article 11 EULs DPR, data relating to criminal convictions and offences must be also considered as sensitive³⁰. As defined in The Regulation Article (34.1) the ETIAS watchlist shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence. It must be considered as sensitive data. Usage of this special category of data is requested by The Regulation article (34 and 35), the ETIAS watchlist shall form a part of the ETIAS Central System, which is developed and managed by eu-LISA.

Table 16 Legal basis and necessity for processing

²⁸ Regulation EU 2018/1726.

²⁹ Article 6 of Regulation (EU) 2018/1240 states that eu-LISA shall develop the ETIAS Information System and ensure its technical management.

³⁰ Regulation EU 2018/1725 “Processing of personal data relating to criminal convictions and offences or related security measures based on Article 5(1) shall be carried out only under control of official authority or when the processing is authorised by Union law providing for appropriate safeguards for the rights and freedoms of data subjects”.

[REDACTED]

5. Systematic Description of the Data Processing Operation

More details concerning all the system functionalities are available in the ETIAS Architecture Document. From a data protection perspective, the data processing activities (PA) enabled by ETIAS' functionalities are defined as:

Data Flow ID	Name	Description	Steps
PA1	TCNDraft Application	Prior to submitting their application form, applicants shall be given the possibility to store, for a duration of up to 48 hours, the personal data entered.	1. Prerequisite 2. Application draft exist 3. Collect data 4. Transfer data 5. Generation of the hyperlink 6. Transmission of the hyperlink 7. Store Data (draft) 8. Store Data (log) 9. Transfer draft to central system 10. Use mail address for authentication 11. Access restriction 12. Draft Consultation 13. Draft Erasure
PA2	Submitting application (TCN data collection)	Processing and transfer when applying to obtain a travel authorisation for a TCN	1. Request Fee : 2. Transfer To payment service provider(s) 3. Check previous Application 4. Mail Notification 5. Store data 6. Automated Processing 7. Manual Processing (Human Hit Verification) 8. Store Decision 9. Mail decision Notification
PA3	Automated Processing (Identifying hits in the application files)	Automatically and individually process the application files	1. Transfer Data 2. Consolidated Result 3. Store Data

Data Flow ID	Name	Description	Steps
PA4	Manual Processing (in case one or more hits are reported)	Process the application file where a hit is reported in the automated processing	1. Retrieve hit information 2. Hit assessment (CU) 3. Transfer to Sirene Bureau 4. Hit assessment (NU) 5. Store Data (File For Extraction) 6. Collect Data (Additional) 7. Collect Data (Interview) 8. Decide on the hit 9. Store Logs
PA5	TCN requests access, rectification, completion or erasure of personal data, consent & abuse.	This data flow describes the different actions that a TCN is able to do using the web or mobile application:	1. Authentication: 2. Store Data (Auth) 3. Consent 4. Store data (Consent) 5. Remove data (Consent) 6. Report abuse 7. Collect Data (abuse) 8. Transfer abuse to Central Unit 9. Store Data (abuse) 10. Access, Rectification, Completion, Erasure 11. Collect Data (request) 12. Process Data (request) 13. Transfer data (Transfer Request To Central Unit) 14. Check Application Status
PA6	Watchlist management	How ETIAS NUs and Europol shall introduce, amend or erase new entry records in the ETIAS Watchlist	1. Prerequisite 2. Collect Data 3. Process Data 4. Store Data 5. Check Data & Delete Data 6. Check Notification & Automatic Notification
PA7	Watchlist review	Review and verify the continued accuracy of the data entered into the ETIAS Watchlist	1. Message from SIS 2. Compare SIS/Watchlist 3. Collect Data 4. Process Data 5. Store/Delete Data

Data Flow ID	Name	Description	Steps
PA8	Access to the ETIAS Central System for Border control and law enforcement purposes	How member state designated authorities, Europol and border authorities, shall be able to consult the ETIAS Central System	1. Prerequisite 2. Collect data for Law Enforcement 3. Restricting Access 4. Process Data 5. Transfer Data 6. Collect Data at Border 7. First Line Data Collection 8. Second Line Data Collection
PA9	Carriers access for verification purposes	Carriers verify if the person has a valid travel authorisation	1. Prerequisite 2. Collect Data 3. Process Data 4. Extract Data to Read Only Database 5. Store Data 6. Transfer Data to carriers
PA10	EBCGA support to carriers	TCN or Carrier is able to ask for support of ETIAS Central Unit	1. Collect data 2. Data processing 3. Store data

Table 17 data flows

5.1. Detailed description of the purpose(s) and supporting assets

Supporting asset ID	Supporting asset type	Short Description	Description
SuS1	Software	ETIAS Central System	Includes the ETIAS watchlist Art 6 (a)
SuS2	System	National Uniform Interface (NUI)	Common component to all member states allowing them to connect securely to the CU. Art 6 (b)
SuS3	System	Communication Infrastructure	The communication infrastructure between the ETIAS Central System and the NUIs which shall be secure and encrypted. Art 6 (c)

<i>Supporting asset ID</i>	<i>Supporting asset type</i>	<i>Short Description</i>	<i>Description</i>
<i>SuS4</i>	<i>System</i>	Secure Communication Infrastructure	A secure communication infrastructure between the ETIAS Central System other EU information systems and Europol. Art 6 (d), Art 11
<i>SuS5</i>	<i>Software</i>	Public website and an app for mobile devices	Main purpose of the website is to enable third-country nationals subject to the travel authorisation requirement to submit a travel authorisation application, to provide the data required in the application and to pay the travel authorisation fee and inform the public on all matters related to ETIAS. Art 6 (e), Art 16
<i>SuS6</i>	<i>Software</i>	Email service	Art 6 (f)
<i>SuS7</i>	<i>Software</i>	Secure account service	Enable applicants to provide any additional information or documentation required. Art 6 (g)
<i>SuS8</i>	<i>Software</i>	Verification tool	For applicants to check the status of their applications and to check the period of validity and status of their travel authorisations (valid, refused, annulled or revoked). This tool shall be made accessible via the dedicated public website or via the app for mobile devices. Art 6 (h), Art 31
<i>SuS9</i>	<i>Software</i>	Consent tool for retention period	A tool enabling applicants to give or withdraw their consent for an additional retention period of their application file; Art 6 (i)
<i>SuS10</i>	<i>Software</i>	Watchlist assessment tool	A tool enabling Europol and Member States to assess the potential impact of entering new data into the ETIAS watchlist on the proportion of applications that are manually processed; Art 6 (j)
<i>SuS11</i>	<i>System</i>	Carrier Gateway	Art 6 (K) Secure access to the carrier gateway, including the possibility to use mobile technical solutions, shall allow carriers to query ETIAS Information System prior to the boarding of a passenger. Art 45
<i>SuS12</i>	<i>Software</i>	Carrier Gateway Database	The carrier gateway shall make use of a separate read-only database updated daily via a one-way extraction of the minimum necessary subset of data stored in ETIAS Art 45 (4)

<i>Supporting asset ID</i>	<i>Supporting asset type</i>	<i>Short Description</i>	<i>Description</i>
<i>SuS13</i>	<i>Software</i>	Web Service	Secure web service enabling the ETIAS Central System to communicate with the public website, the app for mobile devices, the email service, the secured account service, the carrier gateway, the verification tool for applicants, the consent tool for applicants, the payment intermediary and the Interpol databases; Art 6 (l)
<i>SuS14</i>	<i>Software</i>	Software for applications processing and consulting	Software enabling the ETIAS Central Unit and the ETIAS National Units to process applications and to manage consultations with other ETIAS National Units and with Europol. Art 6 (m), Art. 26(3),(4),(6); 27(2),(8);37(3),40(3),42(7);29(2)
<i>SuS15</i>	<i>Software</i>	ETIAS Storage Location	Although no database is explicitly described in the regulation, Article 13 makes it implicit.
<i>SuS16</i>	<i>Software</i>	Watchlist Database	The ETIAS watchlist shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence
<i>SuS17</i>	<i>Personnel</i>	CU	ETIAS Central Unit's staff
<i>SuS18</i>	<i>Personnel</i>	NU	ETIAS National Unit's staff
<i>SuS19</i>	<i>System</i>	Internet Communication Infrastructure	Allowing TCN to communicate with ETIAS System.
<i>SuS20</i>	<i>System</i>	Draft Database	The application draft can be store for 48h, exact location is not defined in the regulation.

Table 18 supporting assets

5.2. Flowchart

Following data flow diagram symbols are used to describe the different step in a dataflow:

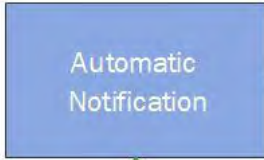
	Start point of the data flow. The different actors starting the data flows are included in the start symbol. Actor can be a timer for some data flow, ie when a central system needs to periodically execute a data flow. One data flow can have more than one start point.
	End of the data flow. When you are in a sub data flow at the end you return and continue the process to the parent data flow.
	Action Step, action or set of actions on or using personal data's
	Sub data flow, some data flow can trigger sub data flow, the current data flow is put on idle and wait that the sub data flow is finish to continue.
	Transfer of personal data to another actor(s).
	Notification to an actor including personal data. This notification process can be unsecure and are not under the control of EU-LISA ie send a mail to the TCN mail address.
	Personal data input or output point.
	Test, will redirect the dataflow to a specific path depending of some conditions.

Table 19 flowchart diagram symbols

Two main personal data paths exist in this dataflow, the first one is when the creation of the draft, the second one is for consultation, alteration, or erasure of an already existing draft. The difference between both is the restriction of the access to the personal data.

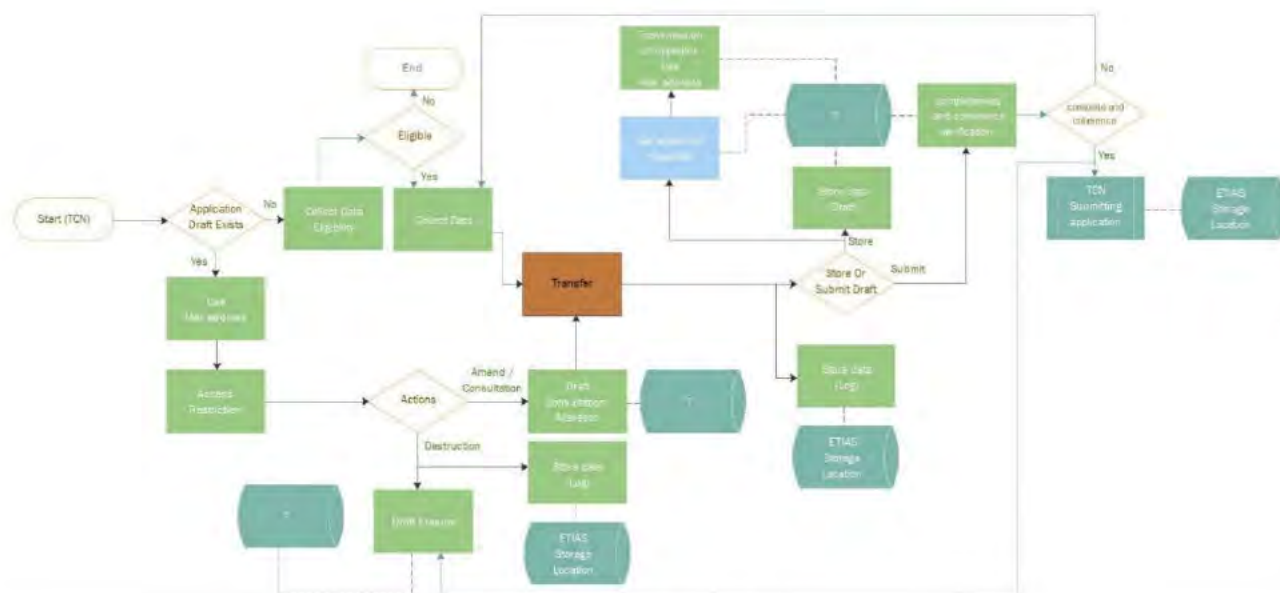


Figure 1 TCN draft application flow

TCN Draft Application steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	See 5.3.3	Usage of the public website or the app for mobile devices to submit a travel authorisation application form, and provide the data required in the application form to save a draft	SuS5 - Public website and an app for mobile devices SuS13 - Web Service
Transfer	See 5.3.4	Usage of internet to communicate the personal data to ETIAS	SuS19 – Internet SUS1 - ETIAS Central System SuS13 - Web Service
Generation of hyperlink	See 5.3.5	Generate a unique hyperlink used for access restriction of personal data.	SuS1 - ETIAS Central System?
Transmission of hyperlink	See 5.3.6	Communication of the hyperlink to the application requestor.	SuS6 – Email service
Store data Draft	See 5.3.7	Storage of the draft for 48h maximum.	SuS20 – Draft database
Store data log	See 5.3.8	Central system will store logs	SUS1 - ETIAS Central System SUS15 - ETIAS Storage Location
Transfer Draft to central system	See 5.3.9	Change and transfer the status of a draft to application request.	SUS1 - ETIAS Central System
Use mail address for authentication	See 5.3.10	Usage of mail address to authentication purpose.	SuS20 – Draft database SuS6 – Email service
Access restriction	See 5.3.11	Restrict the access to personal data saved in a draft.	SUS1 - ETIAS Central System
Draft consultation Alteration	See 5.3.12	Consult, alter or submit an existing draft application.	SuS5 - Public website and an app for mobile devices SuS13 - Web Service SuS19 - Internet
Draft Erasure	See 5.3.13	Erase draft at expiration or if requested by the application requestor.	SuS20 – Draft database

Table 20 TCN Draft Application steps

5.3.1. Prerequisite

The public website and the app for mobile devices shall comply with the principle of perceivability, operability, understandability and robustness as referred to in Directive (EU) 2016/2102 of the European Parliament and the Council.

5.3.2. Application draft exists

This step is a supporting operation to validate if the access request concerns a new application or an access to an existing draft.

5.3.3. Collect data Eligibility

Central System collect personal data as country to verify the applicant's eligibility to obtain an ETIAS travel authorisation according to his/her nationality through the eligibility matrix verification (e.g.: country is not applicable; applicant has diplomatic passport) and concludes the applicant is not in the scope of ETIAS.

5.3.4. Collect data

Using public website and the app for mobile devices as defined in the Regulation (EU) 2018/1240 (Article 16) "the third-country nationals subject will submit a travel authorisation application form, to provide the data required in the application form in accordance with Article 17 and to pay the travel authorisation fee".

Personal data of the applicant:

- surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, country of birth, sex, current nationality, first name(s) of the parents of the applicant
- other names (alias(es), artistic name(s), usual name(s)) if any
- other nationalities
- type, number and country of issue of the travel document
- the date of issue and the date of expiry of the validity of the travel document
- the applicant's home address or, if not available, his or her city and country of residence
- email address and, if available, phone numbers

Risk R1: By not doing any mail validation at this stage there are a risk of mistake in the mail address used in future authentication process. This can allow unauthorised access to private data. Two-factors authentication as proposed by IA 2 using only mail address is not appropriate.

- education (primary, secondary, higher or none)
- current occupation (job group); where the application is subject to the manual processing in accordance with the procedure laid down in Article 26, the Member State responsible may in accordance with Article 27 request that the applicant provides additional information concerning his or her exact job title and employer or, for students, the name of their educational establishment;
- Member State of first intended stay, and optionally, the address of first intended stay
- for minors, surname and first name(s), home address, email address and, if available, phone number of the person exercising parental authority or of the applicant's legal guardian
- where he or she claims the status of family member referred to in point (c) of Article 2(1):
- his or her status of family member
- the surname, first name(s), date of birth, place of birth, country of birth, current nationality, home address, email address and, if available, phone number of the family member with whom the applicant has family ties
- his or her family ties with that family member in accordance with Article 2(2) of Directive 2004/38/EC
- in the case of applications filled in by a person other than the applicant, the surname, first name(s),

[REDACTED]

name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration.

- In addition, the applicant shall provide answers to the following questions:
 - Whether he or she has been convicted of any criminal offence listed in the Annex over the previous 10 years and in case of terrorist offences, over the previous 20 years, and if so when and in which country
 - Whether he or she has stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay
 - Whether he or she has been the subject of any decision requiring them to leave the territory of a Member State or of any third countries listed in Annex II to Regulation (EC) No 539/2001 or whether they were subject to any return decision issued over the previous 10 years.

Regulation (EU) 2018/1240(article 17(6)) "Where the applicant answers affirmatively to any of the questions he or she shall be required to provide answers to an additional set of predetermined questions, The Commission shall adopt delegated acts to lay down the content and format of those additional questions and the predetermined list of answers to those questions.", "The applicant shall provide the additional information or documentation directly to the ETIAS National Unit of the Member State responsible through the secure account service referred to in point (g) of Article 6(2)"

COMMISSION DELEGATED DECISION specifying the content and format of the questions and laying down the additional set of predetermined questions pursuant to Article 17(5) and (6) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, this act establishes the format and contents of the questions and answers pursuant to Article 17(5) of Regulation (EU) 2018/1240 as well as the additional set of predetermined questions and answers pursuant to Article 17(6) of that Regulation

Subjects of the Question are concerning:

- Criminal offences to be declared in the application form pursuant to Article 17(4)(a)
- Stay in war or conflict zones to be declared in the application form pursuant to Article 17(4)(b)
- Decisions taken against the applicant to leave a territory or return to be declared in the application form pursuant to Article 17(4)(c)

To be able to save a draft, applicants shall provide their email address.

The security of the public website and mobile application are laydown in article 6 of the public website implementing act.

the public website and the app for mobile devices shall be designed and implemented to ensure, including as regards logging, the confidentiality, integrity and availability of the services and to ensure non-repudiation of transactions as referred to in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017¹² and apply at least the following application security principles.

5.3.5. Transfer

The transfer between the browser or mobile application of the applicant and the web services is using Internet, as defined in Article 6(3) web service shall to the extent technically possible share and re-use the hardware and

[REDACTED]

software components of the EES web service referred to in Regulation (EU) 2017/2226.

The ETIAS Central System, the NUIs, the web service, the carrier gateway and the communication infrastructure of ETIAS shall to the extent technically possible share and re-use the hardware and software components of the EES Central System, of the EES National Uniform Interfaces, of the EES web service and of the EES Communication Infrastructure referred to in Regulation (EU) 2017/2226.

A secure internet access to the web service is used in article 13 of the Regulation (EU) 2017/2226 and should be used for the transfer of TCN personal data.

5.3.6. Store or Submit Draft

Application requester can choose between save a draft or submit the current application to process.

5.3.7. Generation of the hyperlink

This step is a supporting operation in the case of creation of a new draft to generate a unique hyperlink as define in the implementing act Public Web Site article 5(5)(c). This hyperlink cannot be considered as a personal data but have a important role to restrict the access an existing draft and related personal data. This hyperlink is valid for 48h. but no information is for the moment provided of the retention place.

"(c) containing a unique hyperlink, valid for 48 hours, necessary for retrieving their application form containing their personal data."

5.3.8. Transmission of the hyperlink

When an applicant creates a draft, the draft system will send a mail as define in the implementing act Public Web Site article 5(4) and 5(5).

The mail will include a unique hyperlink, valid for 48 hours, necessary for retrieving their application form containing their personal data.

5.3.9. Store Data (draft)

Prior to submitting their application form, applicants shall be given the possibility to store, the personal data entered. Storage location are not clearly defined in the legal base.

Risk R2: As the store location for the draft application, who contain personal data, is not yet clearly defined, risk as: storage limitation, security, purpose limitation, fairness and purpose limitation can occur.

The storage of such data shall be compliant with Regulation (EU) 2018/1725.

5.3.10. Store Data (log)

During the collection phase (5.3.4) Central system will log Timestamp; IP address; Device information; these logs shall be stored for a period of two years and protected by appropriate measures against unauthorised access. No mention was found if a direct link can be done between the applicant draft and these logs.

5.3.11. Completeness and coherence verification

Central System performs a completeness and coherence verification on the mandatory data fields, following requirement describe in the implementing act on the mechanism, the procedures and the appropriate requirements for data quality compliance, pursuant to Article 74(5) of Regulation (EU) 2018/1240 of the European Parliament and of the Council.

5.3.12. TCN Submitting application

TCN application is submitted to the submit dataflow to process the application request.

5.3.13. Use mail address for authentication

Using the mail enter during the creation of the draft and when requesting the storing of their data, applicants shall receive an email:

- (a) confirming the storing of their data;
- (b) informing that the data will be stored for a maximum of 48 hours; and
- (c) containing a unique hyperlink, valid for 48 hours, necessary for retrieving their application form containing their personal data.

5.3.14. Access Restriction

In order to access their personal data entered in the application form prior to submission, applicants shall use a two-factor authentication.

The two-factor authentication shall consist of the following elements:

- (a) the unique hyperlink referred to in paragraph 5.3.7;
- (b) a unique code generated automatically upon each usage of the unique hyperlink.

The unique code shall be sent to the email address referred to in paragraph 5.3.4.

The unique code shall be usable once and shall expire after a short period of time. Sending a new unique code shall invalidate unique codes previously sent to the same applicant.

5.3.15. Draft Consultation Alteration

During the 48h, applicant can consult, alter and submit the draft, previous personal data stored in the draft is retrieve from the draft location.

5.3.16. Draft Erasure

The retention period for the draft is 48h, as define in the implementing act, will be stored for a maximum of 48 hours.

When a draft is submitted to the central system, the draft should be erased.

5.4. TCN Submitting application

This data flow defines the TCN data collection, and the data processing operation performed for the purpose of submitting the application for a travel authorisation. The process begins when a TCN intends to apply for a travel authorisation and fill an application form with the necessary data for this application, either on the public website or by the mobile device application. The systems will then check if the TCN pose a security issue, for instance in regard to illegal immigration or high epidemic risk, by means of an automated processing of the data against other EU databases. If no hit result from the automated processing, the travel authorisation is granted to the TCN and this information is communicated to the applicant. Otherwise, a manual processing of the data will be performed. The following diagram refers to ETIAS Regulation:

- 1) Article 17: Application form and personal data of the applicant
- 2) Article 19: Admissibility and creation of the application file

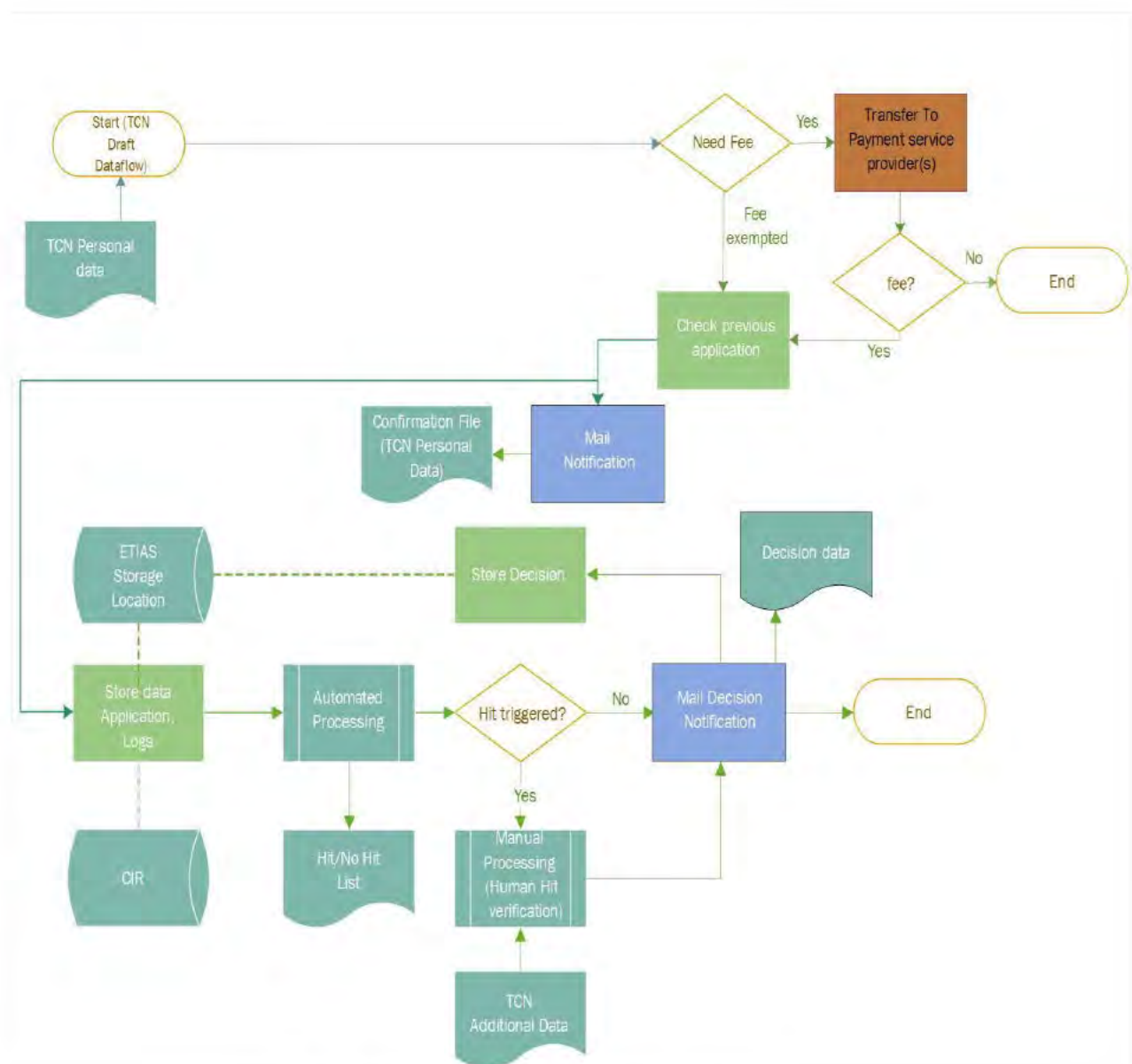


Figure 2 TCN Submission application flow

TCN Submitting application Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 12.1 and indicate for each step you identified which are the supporting assets)
Transfer to Payment service	Description in chapter 5.4.2	Transmit a unique correlation identifier linked to that application form to the payment service provider(s).	SUS1 - ETIAS Central System
Check previous application	Description in chapter 5.4.3	The ETIAS Central System shall determine whether the applicant already has another application file	SUS15 - ETIAS Storage Location
Mail notification	Description in chapter 5.4.4	Central System sends an email with a certified digital signature containing the link to the application draft.	SUS1 - ETIAS Central System SUS6 - Email service
Store data & Application Logs	Description in chapter 5.4.5	Central system will store Application file and logs.	SUS1 - ETIAS Central System SUS15 - ETIAS Storage Location
Automated processing	Description in chapter 5.4.6	Subprocess describe in chapter 5.5	SUS1 - ETIAS Central System
Manual processing	Description in chapter 5.4.7	Subprocess describe in chapter 5.6	SUS1 - ETIAS Central System
Mail decision notification	Description in chapter 5.4.9	Central system will create an email with a certified digital signature and attaches the Travel Authorisation and sends it to the email address of the applicant	SUS1 - ETIAS Central System SUS6 - Email service
Store decision	Description in chapter 5.4.8		SUS15 - ETIAS Database

Table 21 TCN Submitting Application steps

5.4.1. Request Fee

According to the Regulation (EU) 2018/1240 (Article 18) Travel authorisation fee, a travel authorisation fee shall be paid by the applicant for each application. The travel authorisation fee shall be waived for applicants under 18 years or above 70 years of age at the time of the application. The travel authorisation fee shall be charged in euros.

5.4.2. Transfer To payment service provider(s)

According to the Article 4, Fee collection process, of COMMISSION DELEGATED REGULATION (EU) of XXX Draft "on the payment methods and process for the travel authorisation fee, collection process and changes to the fee amount pursuant to Article 18(4) of Regulation (EU) 2018/1240 of the European Parliament and of the Council".

The ETIAS Central System shall generate and attribute a unique correlation identifier linked to that application form. That identifier shall be transmitted to the payment service provider(s).

Upon creation of the application file, the ETIAS Central System shall record and store in the application file a reference to the successful payment of the travel authorisation fee and a unique number of the payment. In addition, the unique correlation identifier shall be deleted from the application file.

Risk R3: The fact that the payment provider will receive a unique correlation identifier directly by the ETIAS CENTRAL SYSTEM give information concerning the future destination of the traveller. This information can be reused for targeted publicity.

Risk R4: As they are not yet contract between EU Commission and the payment provider it is impossible to assess if the applicant could exercise their rights with these payment providers.

5.4.3. Check Previous Application

Regulation (EU) 2018/1240 Article 19(4) the ETIAS Central System shall determine whether the applicant already has another application file in the ETIAS Central System by comparing the data referred to in point (a) of Article 17(2) with the personal data of the application files stored in the ETIAS Central System. In such a case, the ETIAS Central System shall link the new application file to any previous existing application file created for the same applicant.

5.4.4. Mail Notification

Central System creates an application draft, assigns the state of to the application and sends an email with a certified digital signature to the email address provided, containing a link to the application form draft by using the email template

5.4.5. Store data

During the collection phase (5.3) Central system will log Timestamp; IP address; Device information; these logs shall be stored for a period of two years and protected by appropriate measures against unauthorised access. No mention was found if a direct link can be done between the applicant and these logs.

Application file shall be stored in the ETIAS Central System and applicant's data referred to in points (a) to (e) of Article 17(2) of Regulation (EU) 2018/1240 shall be stored/updated in the Common Identity Repository (CIR).

Risk R5 and R6: Regulation (EU) 2018/1725 chapter III define rights for the data subject. Collecting information as time stamp, IP address or device information without a clear consent of the data subject is not compliant with these rights.

5.4.6. Automated Processing

The ETIAS Central System compares the TCN relevant data to the data present in a record, file or alert registered in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol SLTD and TDAWN databases. If records are found in those DBs, this process will return one or several hits. This sub process is described in chapter 5.5

5.4.7. Manual Processing (Human Hit Verification)

Where the automated processing pursuant to Article 20(2) to (5) reports one or several hits the ETIAS Central System shall automatically consult the ETIAS Central Unit. This sub process is described in chapter 5.6

5.4.8. Store Decision

Central System saves the application file, the date of the decision, the validity period of the travel authorisation;

In case of application is being manually processed and accepted, the following activity logs are stored:

NUI user; timestamp; application ID; state of application; reason(s) for final decision; the reference to ETIAS NU of the MS that issued the travel authorisation; flag(s), if applicable; additional information submitted/uploaded to the flag; commencement date of the travel authorisation; expiry date of the travel authorisation.

In case of application is being manually processed and refused, the following activity logs are stored:

NUI User; timestamp; application ID; state of application; reason for rejection; reason(s) for final decision; the reference to ETIAS NU of the MS that refused the travel authorisation

In case of application is being automatically processed with no hit identified, the following activity logs are stored:

Timestamp; application ID; state of application file; commencement date of the travel authorisation; expiry date of the travel authorisation

As defined in the Regulation (EU) 2018/1240 RETENTION AND AMENDMENT OF DATA Article 54 data retention:

1. Each application file shall be stored in the ETIAS Central System for:

(a) the period of validity of the travel authorisation;

(b) five years from the last decision to refuse, annul or revoke the travel authorisation in accordance with Articles 37, 40 and 41. If the data present in a record, file or alert registered in one of the EU information systems, Europol data, the Interpol SLTD or TDAWN databases, the ETIAS watchlist, or the ETIAS screening rules giving rise to such a decision are deleted before the end of that five-year period, the application file shall be deleted within seven days from the date of the deletion of the data in that record, file or alert. For that purpose, the ETIAS Central System shall regularly and automatically verify whether the conditions for the retention of application files referred to in this point are still fulfilled. Where they are no longer fulfilled, it shall delete the application file in an automated manner.

Applicants can give their consent for the storage of their application file data in the ETIAS Central System for an additional period of no more than three years from the end of the validity period of the travel authorisation, for the purpose of facilitating a new application after the expiry of the validity

period of the existing travel authorisation, using the consent tool provided. The applicant may withdraw consent at any time, in which case the application file must automatically be erased from the ETIAS Central System.

Risk R7: The log includes staff member identification and as this information format can change from one member-state to another and then include personal data. The NUI User should be aware of the usage of these data.

5.4.9. Mail decision Notification

If the TCN is admissible for an application, Central system will create an email with a certified digital signature and attaches the Travel Authorisation and sends it to the email address of the applicant.

PA 3

5.5. Automated processing

The automated processing shall automatically and individually process the application files through the ETIAS Central System to identify possible hit(s). ETIAS check application records against other DBs through the ESP, which provides the access to data in other EU systems, as well as Europol and Interpol data.

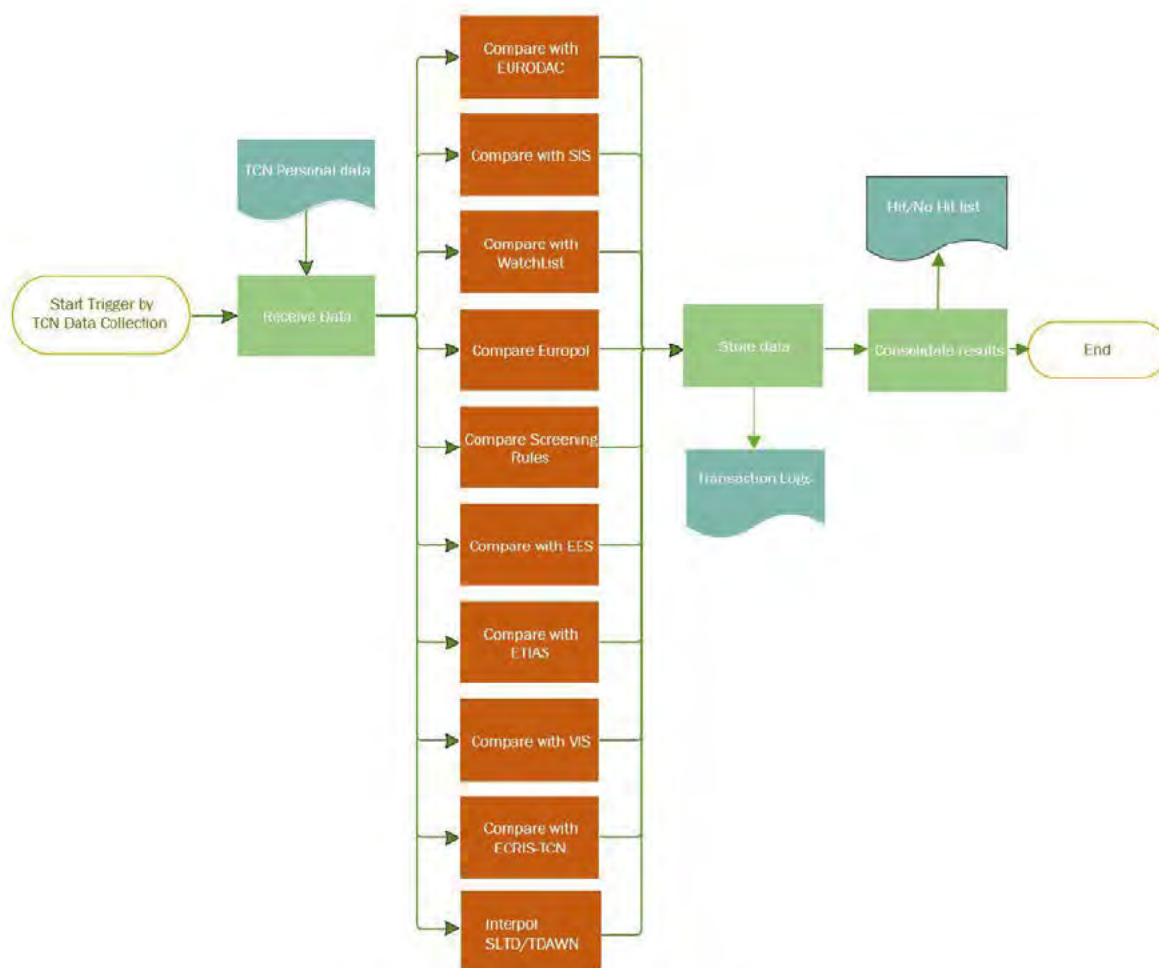


Figure 3 automated processing flow

Automated processing Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	System receives a TCN application file from the sub process TCN Data Collection (5.4)	Regulation (EU) 2018/1240 (Article 20(1)) The application files shall be automatically processed by the ETIAS Central System to identify hit(s).	SUS1 - ETIAS Central System
Merging datasets	During the Consolidate Result sub process, hit/no Hit coming from the different System are merged in the Central System (5.5.2)	Consolidate results coming from the different systems.	SUS1 - ETIAS Central System
Disclosing/transferring the data	Central System receives an application file and transfer information to verify against EU information systems, Europol data and Interpol (o)	Transfer personal data to external system to verify against EU information systems.	SUS1 - ETIAS Central System SuS4 - Secure Communication Infrastructure SUS15 - ETIAS Storage Location SUS16 Watchlist database
Storing the data	Central System will store if there are hit(s). It will also log the hit id returned from by the automated processing process (5-5-3)	Keeping trace about the hit or no hit in other EU information systems.	SUS1 - ETIAS Central System SUS15 - ETIAS Storage Location

Table 22 Automated Processing steps

5.5.1. Compare Data

Central System receives an application file and compares information to verify against EU information systems, Europol data and Interpol databases through the ESP:

- a. whether the travel document used for the application corresponds to a travel document reported lost, stolen, misappropriated or invalidated in SIS;
- b. whether the travel document used for the application corresponds to a travel document reported lost, stolen or invalidated in the SLTD;
- c. whether the applicant is subject to a refusal of entry and stay alert entered in SIS;
- d. whether the applicant is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS;
- e. whether the applicant and the travel document correspond to a refused, revoked or annulled travel authorisation in the ETIAS CS;
- f. whether the data provided in the application concerning the travel document correspond to another application for travel authorisation associated with different identity data referred to in point (a) of Article 17(2) of Regulation (EU) 2018/1240 in the ETIAS CS;
- g. whether the applicant is currently reported as an overstayer or whether he or she has been reported as an overstayer in the past in the EES;
- h. whether the applicant is recorded as having been refused entry in the EES;
- i. whether the applicant has been subject to a decision to refuse, annul or revoke a short stay visa recorded in VIS;
- j. whether the data provided in the application corresponds to data recorded in Europol data;
- k. whether the applicant is registered in Eurodac;
- l. whether the travel document used for the application corresponds to a travel document recorded in a file in TDAWN;
- m. in cases where the applicant is a minor, whether the applicant's parental authority or legal guardian:
 - i. is subject to an alert in respect of persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant or wanted for arrest for extradition purposes in SIS;
 - ii. is subject to a refusal of entry and stay alert entered in SIS;
- n. whether the applicant corresponds to a person whose data is recorded in the ECRIS-TCN for terrorist offences and other serious criminal offences
- o. whether the applicant is the subject of one of the following alerts in SIS:
 - i. an alert on missing persons;
 - ii. an alert on persons sought to assist with a judicial procedure;
 - iii. an alert on persons for discreet checks or specific checks.

The Central System verifies whether the applicant has replied affirmatively to any of the background questions and whether the applicant has not provided a home address but only his city and country of residence;

Following article 20(4) the ETIAS Central System shall compare the relevant data referred to in points (a), (aa), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in the ETIAS watchlist referred to in Article 34.

- (a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;
- (aa) country of birth, first name(s) of the parents of the applicant;
- (b) other names (alias(es), artistic name(s), usual name(s)), if any;
- (c) other nationalities, if any;

[REDACTED]

(d) type, number and country of issue of the travel document;

(f) the applicant's home address or, if not available, his or her city and country of residence;

(g) email address and, if available, phone numbers;

(j) Member State of first intended stay, and optionally, the address of first intended stay;

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

(m) in the case of applications filled in by a person other than the applicant, the surname, first name(s), name of firm, organisation if applicable, email address, mailing address and phone number if available of that person; relationship to the applicant and a signed representation declaration.

(Article 17, (8)) IP address from which the application form was submitted

Following article 7 (2) (c), 9 (a) and 33 (6), the Central System compares the following data to the specific risk indicators "defined, established, assessed *ex ante*, implemented, evaluated *ex post*, revised and deleted by the ETIAS Central Unit after consultation of the ETIAS Screening Board". As per article 20 (5) ETIAS Central System shall compare the relevant data referred to in points (a), (aa), (c), (f), (h) and (i) of Article 17(2) to the specific risk indicators referred to in Article 33 :

(a) surname (family name), first name(s) (given name(s)), surname at birth; date of birth, place of birth, sex, current nationality;

(aa) country of birth, first name(s) of the parents of the applicant;

(c) other nationalities, if any;

(f) the applicant's home address or, if not available, his or her city and country of residence;

(h) education (primary, secondary, higher or none);

(i) current occupation (job group); where the application is subject to the manual processing in accordance with the procedure laid down in Article 26, the Member State responsible may in accordance with Article 27 request that the applicant provide additional information concerning his or her exact job title and employer or, for students, the name of their educational establishment;

Risk R21: *TCN Personal Data will be compared with specific risk indicators defined by the ETIAS Central Unit and ETIAS Screening Board art (7) & art(9), ETIAS Central Unit. Wrong technical implementation, testing or maintenance of the risks indicator (as per art (74)) could lead to discrimination and profiling of the data subjects.*

5.5.2. Consolidated Result

If Automated processing reports no hit then system issues a travel authorisation automatically, otherwise a Manual processing starts (see paragraph 5.6).

5.5.3. Store Data

Central System will log the automated processing activity, it will record following information: Timestamp and searched data. It will also log the usage of the ESP by the ETIAS Central System.

5.5.4. Overall View

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipient)
Application file data	From the ETIAS Central storage location	Verifies against EU information systems, Europol data and Interpol databases through the ESP	ETIAS application storage location	SIS, VIS, EES, ECRIS-TCN, EURODAC, CIR, Interpol, Europol

Table 23 Automated Processing overview

PA 4

5.6. Manual processing

In accordance to the Regulation (EU) 2018/1240 (Article 22), where the automated processing pursuant to Article 20(2) to (5) reports one or several hits the ETIAS Central System shall automatically consult the ETIAS Central Unit.

This data flow defines that ETIAS Central Unit application officers shall process the application file where a hit is reported in the automated processing, and when needed to transfer it to the ETIAS National Unit.

These activities include the verification of the application file personal data and hit(s) triggered by central unit and National Unit officers with the possibility to request additional data's, an in-person interview or via an audio/video tool. Based on these assessments the application is accepted or denied.

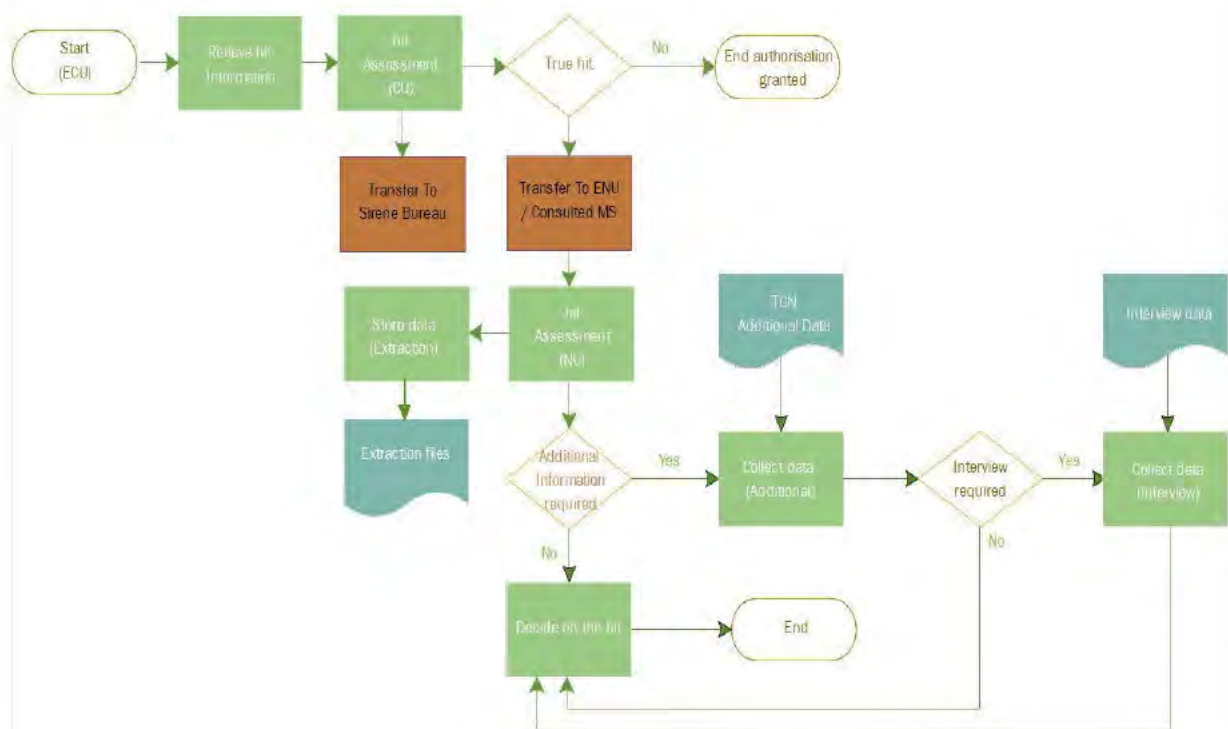


Figure 4 manual processing flow

5.6.1. Retrieve hit information

The ETIAS Central Unit shall have access to the application file and any linked application files, as well as to all the hits triggered during automated processing pursuant to Article 20(2) to (5) and to the information identified by the ETIAS Central System under Article 20(7) and (8).

5.6.2. Hit assessment (CU)

The ETIAS Central Unit verify whether the data recorded in the application file correspond to one or more of the following:

- a) the specific risk indicators referred to in Article 33;
- b) the data present in the ETIAS Central System, including the ETIAS watchlist
- c) the data present in one of the EU information systems that are consulted
- d) Europol data
- e) the data present in the Interpol SLTD or TDAWN databases.

Specific SIS case is explained in next chapter 5.6.3 .Transfer to Sirene Bureau

Where the data do not correspond, and no other hit has been reported during automated processing, and where the examination of an application indicates that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security, illegal immigration or high epidemic risk, the ETIAS Central Unit shall delete the false hit from the application file and the ETIAS Central System shall automatically issue a travel authorisation

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

Where the data made available correspond to those of the applicant or where doubts remain, the unique ID code of the data having triggered a hit shall be kept in the application file and the ETIAS National Unit of the Member State responsible shall be consulted.

5.6.3. Transfer to Sirene Bureau

Where the comparison with SIS reports one or several hits, the ETIAS Central System shall send an automated notification to the ETIAS Central Unit. The ETIAS Central Unit shall verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered that hit and if a correspondence is confirmed, the ETIAS Central System shall send an automated notification to the SIRENE Bureau of the Member State that entered the alert. The SIRENE Bureau concerned shall further verify whether the applicant's personal data correspond to the personal data contained in the alert having triggered the hit and take any appropriate follow-up action.

The notification provided to the SIRENE Bureau of the Member State that entered the alert shall contain the following data:

- (a) surname(s), first name(s) and, if any, alias(es);
- (b) place and date of birth;
- (c) sex;

- (d) nationality and, if any, other nationalities;
- (e) Member State of first intended stay, and if available, the address of first intended stay;
- (f) the applicant's home address or, if not available, his or her city and country of residence;
- (g) travel authorisation status information, indicating whether a travel authorisation has been issued, refused or whether the application is subject to manual processing pursuant to Article 26;
- (h) a reference to any hits obtained in accordance with paragraphs 1 and 2, including the date and time of the hit

5.6.4. Hit assessment (NU)

Where one or several Member States are identified as having entered or supplied the data having triggered a hit, the ETIAS Central Unit shall notify the ETIAS National Unit of the Member State(s) involved, thereby launching a consultation process between them and the ETIAS National Unit of the Member State responsible. The ETIAS National Units of the Member States consulted shall have access to the application file for the purpose of the consultation.

The ETIAS National Unit of the Member States consulted shall provide a reasoned positive opinion on the application; or provide a reasoned negative opinion on the application. The positive or negative opinion shall be recorded in the application file by the ETIAS National Unit of the Member State consulted.

Where the ETIAS National Unit of the Member State responsible deems the information provided by the applicant in the application form to be insufficient to enable it to decide whether to issue or refuse a travel authorisation, it may request additional information, documentation from the applicant, or request an interview as describe in chapter 5.6.6 & 5.6.7.

Risk R8: Inadequate and incomplete Information to the data subject on the processing activity. Data subject has no notification of his/her data transfer to the MS competent authorities. This could affect the effective exercise of his/her right of appeal. Fairness and transparency principles are potentially compromised.

5.6.5. Store Data (File for Extraction)

The Software as describe in Article 4(g) of the IA8³¹ should implement a functionality making automatically available a file for extraction with the following data from the application file:

- 'surname (family name)', 'first name(s) (given names)', 'surname at birth'
- 'date of birth', 'place of birth',
- 'current nationality', 'country of birth',
- 'the type, number and country of issue of the travel document', [and the unique ID code of the data having triggered a hit in the queried EU information systems of Article 20(2) of that Regulation], enabling retrieving the record, file or alert having triggered the hit in the queried EU information systems and where additional information related to the hit in an EU information system referred to in that Article is stored in a national system or a database, to consult that national system or a database supporting the assessment of the security or illegal immigration risk.

Risk R9: The fact that personal data can be extracted from the ETIAS Central System can lead at disclosure of personal data. User should be duly trained and aware about the risk.

³¹ COMMISSION IMPLEMENTING DECISION (EU) .../... of XXX on measures for accessing, amending, erasing and advance erasing of data in the ETIAS Information System, pursuant to Article 73(3)(b) of Regulation (EU) 2018/1240 of the European Parliament and the Council

5.6.6. Collect Data (Additional)

As described in Regulation (EU) 2018/1240 Article 27 the ETIAS National Unit of the Member State responsible shall request additional information or documentation upon the request of a Member State consulted in accordance with Regulation (EU) 2018/1240 (Article 28)

Specific Delegation decision "COMMISSION DELEGATED DECISION (EU) .../... of XXX specifying the content and format of the predetermined list of options to be used for the purpose of requesting additional information or documentation pursuant to Article 27(3) of Regulation (EU) 2018/1240 of the European Parliament and of the Council establishes the format and content of the predetermined list of options to be used for the purpose of requesting additional information or documentation pursuant to Article 27(3) of Regulation (EU) 2018/1240." define the list of option and document who can be asked to the applicant

Some of the options should be considered as sensitive ie: a copy of a court order/judgment or any other relevant document concerning the validity or the cancellation of the SIS refusal of entry and stay, illness, health certificate(s), vaccination certificate(s), hospital invoice(s) or other documents proving a hospital stay, judicial; police certificate(s); judicial invitations(s), court orders or judgments.

Applicant can use the website or mobile application to provide the additional information or documentation. The secure account service System runs a virus scan for the provided answers and uploaded documents to perform a security control.

Where a positive reply is provided for any of the criminal offences and the additional question, the applicant shall be presented with clear instruction and a predetermined list of additional questions for which the applicant shall be required to answer using a free text field for each additional question.

Risk R11: In the framework of the manual processing, usage of free text additional information given by the applicant can induct semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 27 of the Regulation; article 2 (3) (d) and (4), article 3, (3) and (4), article 4 (3), article 6 of the DA 7).

5.6.7. Collect Data (Interview)

Regulation (EU) 2018/1240 Article 27(4) In exceptional circumstances and as a last resort after processing the additional information or documentation, when serious doubts remain regarding the information or documentation provided by the applicant, the applicant may be invited via email for an interview at a consulate in his/her country of residence. The reason for requesting an interview shall be recorded in the application file. For the purpose of the interview, the ETIAS National Unit of the Member State responsible shall indicate the elements to be addressed by the interviewer. Those elements shall relate to the reasons for which the interview was requested. Following the interview, the interviewer shall issue a reasoned opinion for his or her recommendations. The elements addressed and the opinion shall be included in a form to be recorded in the application file on the same day as the date of the interview. Under some conditions defined in the Regulation (EU) 2018/1240 (Article (28(4))), the applicant shall be offered the possibility to conduct the interview by remote means of audio and video communication. The remote means of audio and video communication shall ensure an appropriate level of security and confidentiality

The COMMISSION IMPLEMENTING DECISION (EU) .../... of XXX on the requirements for the means of audio and video communication for the interview pursuant to Article 27(5) Regulation (EU) 2018/1240 define the requirements for the means of audio and video communication including data protection, security and confidentiality.

5.6.8. Decide on the hit

As defined in the Regulation (Article 36)

Where the examination of an application pursuant to the procedures indicates that there are no factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security, illegal immigration or high epidemic risk, a travel authorisation shall be issued by the ETIAS National Unit of the Member State responsible

The ETIAS National Unit of the Member State responsible shall have the possibility to add a flag indicating to border authorities and other authorities with access to the data in the ETIAS Central System that a specific hit triggered during the processing of the application has been assessed and that it has been verified that the hit constituted a false hit or that the manual processing has shown that there were no grounds for the refusal of the travel authorisation.

In cases where ETIAS National Unit has a doubt as to whether sufficient reasons to refuse the travel authorisation exist, the ETIAS National Unit of the Member State responsible shall have the possibility, including after an interview, to issue a travel authorisation with a flag recommending to border authorities to proceed with a second line check

The flag shall be removed automatically once the border authorities have carried out the check and have entered the entry record in the EES

5.6.9. Store Logs

As defined in the Article 1 of the REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the conditions for accessing other EU information systems for ETIAS purposes and amending the Regulation, Regulation (EC) No 767/2008, Regulation (EU) 2017/2226 and Regulation (EU) 2018/1861. The ETIAS Information System shall keep records of all data processing operations carried out for assessments by the ETIAS Central Unit. Those records shall be created and entered automatically in the application file. They shall show the date and time of each operation, the data linked to the hit received, the staff member having performed the manual processing and the outcome of the verification and the corresponding justification

Logs shall be stored for a period of two years and protected by appropriate measures against unauthorised access.

Risk R7: The log includes staff member identification and as this information format can change from one member-state to another and then include personal data. The NUI User should be aware of the usage of these data.

5.6.10. Overall view

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
Application file data	from the ETIAS Central Storage location	Assess the travel authorisation request	ETIAS Central Storage location	ECU, ENU, Europol, Interpol, EU systems
hit id	EU systems	Confirm if the hit is true or false and assess the travel	ETIAS Central Storage location	ECU, ENU

A horizontal bar chart with five segments. The third segment from the left is labeled "authorisation request".

Table 24 Manual processing

5.7. TCN requests access, rectification, completion or erasure of personal data, consent & abuse.

This data flow describes the different actions that a TCN is able to do using the web or mobile application:

- Provide or withdraw their consent for the storage of their application file data in the ETIAS Central System for an additional period,
- Report abuse by the commercial intermediaries that have submitted the application,
- Request of amendment or erasure or access to the personal data to the ETIAS CU or ETIAS NU responsible for his/her application.

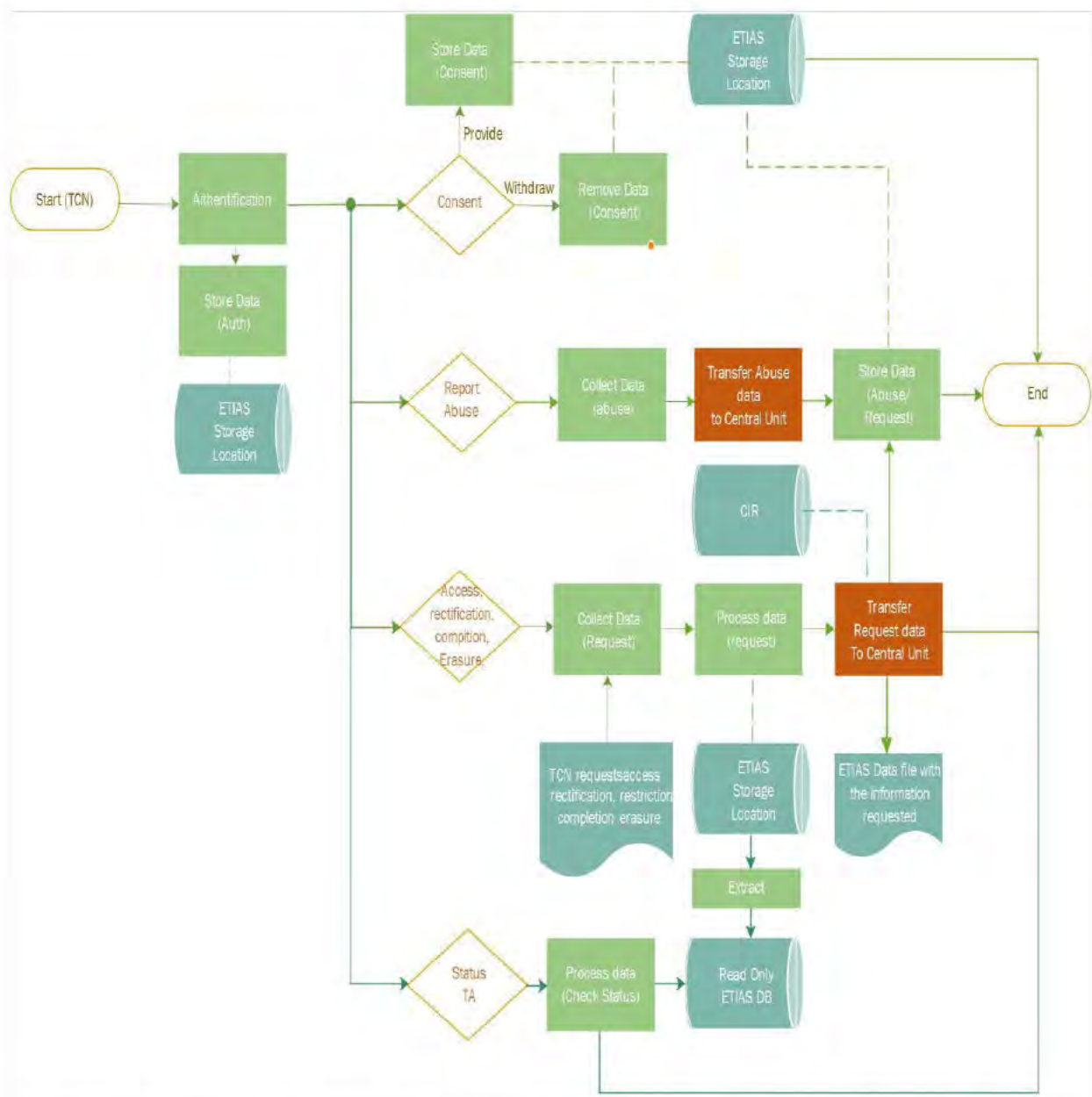


Figure 5 TCN requests access, rectification, completion or erasure of personal data, consent & abuse

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	Access to the public tools as well as to specific sections through the public website/mobile. application should be done following a 2-factor authentication process (5.7.1)	Collection of the personal data needed for the authentication.	SUS1 - ETIAS Central System SUS5 - Public website and an app for mobile devices SUS7 - Secure account service SUS6 Email service SUS13 Web Service
Retrieving/consulting/using the data	The authentication process submitting authentication credentials followed by a unique code generated by the system and sent to the applicant's his personal data email address (5.7.1)	Use the email address as a 2-factor authentication.	SUS1 - ETIAS Central System SuS6 - Secure Mail Service SUS7 - Secure account service SUS13 Web Service
Storing the data	When authentication succeeds, authentication data are logged (5.7.2)	The Regulation Article 69 requires to keep logs of all data processing operations within the ETIAS Information System	SUS15 - ETIAS Storage Location
Collecting of the data	TCN describes the request by entering free text on the selected form of the options type of amendment or erasure.	Collect information concerning the TCN requests or abuse report.	SUS1 - ETIAS Central System SUS5 - Public website and an app for mobile devices
Disclosing/transferring the data	ETIAS CU/NU shall examine and reply to the TCN's request upon reception of the data recorded in the application request form.	Provide abuse information to the central unit for examination.	SUS1 - ETIAS Central system SUS 24 - ETIAS Central Unit
Storing the data	As defined in the Regulation (Article 45(7)) eu-LISA shall keep logs of all data processing operations carried out within the carrier gateway by carriers.	Central system will store logs of all data operation.	SUS1 - ETIAS Central System

Table 25 TCN requests access, rectification, completion or erasure of personal data, consent & abuse steps

5.7.1. Authentication

The Regulation (Article 59(b)) defined that unauthorised persons cannot have an access to the secure web service, the email service, the secure account service, the carrier gateway, the verification tool for applicants and the consent tool for applicants;

In order to request access, rectification, completion or erasure of personal data, applicants shall have access to the public tools as well as to specific sections through the public website/mobile application after a 2-factor authentication process as defined in the implementing decision laying down detailed rules on the operation of the public website and the app for mobile devices.

The two-factor authentication shall consist of the following elements:

1. The applicants shall receive an email containing a unique hyperlink.
2. A unique code generated automatically upon each usage of the unique hyperlink
3. The unique code shall be sent to the email address of the applicant.
4. The unique code shall be usable once and shall expire after a short period of time. Sending a new unique code shall invalidate unique codes previously sent to the same applicant

During the authentication phase, following personal data can be required:

- travel document number;
- country issuer of the travel document;
- date of issue and of expiry date of the travel document;
- first names of both parents.

5.7.2. Store Data (Auth)

When an applicant wants to use the authentication system, the following personal data are stored in the Central System:

- Timestamp; IP address;
- Device information;
- Status of response.

When authentication succeeds, authentication data is logged in the central database. These logs shall be stored for a period of two years and should be protected by appropriate measures against unauthorised access. A particular attention shall be given to the application logs and the secure mail service.

Risk R10: Regulation (EU) 2018/1725 chapter III define rights for the data subject. Collecting information as time stamp, IP address or device information without a clear consent of the data subject is not compliant with these rights.

5.7.3. Consent

This part of the data flow is based on the Regulation Article 54(2). To ease the creation of a new travel authorisation after the expiry of the validity period of an ETIAS travel authorisation, the application file may be stored in the ETIAS Central System for an additional period of no more than three years from the end of the

validity period of the initial travel authorization.

The delegated acts COMMISSION DELEGATED DECISION of XXX defines the tool enabling applicants to give or withdraw their consent for an additional retention period of their application, pursuant to Article 54(2) of the Regulation of the European Parliament and of the Council.

5.7.4. Store data (Consent)

Prior to giving the consent, the applicant shall have access to a read-only version of the application form and the personal data submitted, a read-only version of additional documentation or information submitted, a read-only version of data added to the application file following the decision to issue the travel authorisation.

When consent is given, the application form containing the personal data will be stored in the ETIAS Central System.

The consent tool shall also keep activity logs, containing the value of tick box giving or withdrawing consent.

Activity logs of the tool shall be copied to the Central System. They shall be stored for no longer than one year after the end of the extended retention period of the application file, before being automatically deleted.

5.7.5. Remove data (Consent)

The applicant may withdraw his or her consent at any time, in accordance with Article 7(3) of Regulation (EU) 2016/679. If the applicant withdraws consent, the application file shall automatically be erased from the ETIAS Central System.

5.7.6. Report abuse

As defined in the Regulation Article 15(5), applicant must be able to report abuse by the commercial intermediaries who submitted the application on his or her behalf. The form to report the abuse shall be made accessible via the dedicated public website or via the app for mobile devices.

5.7.7. Collect Data (abuse)

Following the IA 1 concerning the reporting of abuses committed by commercial intermediaries, the free text report submitted by the traveller " shall not collect any personal data "³². Moreover, the article 1 (a) of the IA 1 annex foresees an introductory notice at the beginning of the form :

"1 Introduction

(a) *The following introductory notice is to appear at the beginning of this form:*

*"... Please do not insert any personal data in this form, whether they are yours or those of any other person."*³³

In addition, the same legal basis provides that the traveller is required to double check that no personal data have been entered in the free text space :

³² Commission implementing regulation (EU) on the reporting of a abuse by commercial intermediaries providing application services for travel authorisation under Regulation (EU) 2018/1240 of the European Parliament and of the Council, Recital (5) : " In order to ensure that applicants are adequately informed of the nature and purpose of the reporting facility, the form should clarify that the reporting system is for monitoring purposes, it shall not collect any personal data and does not constitute a channel for appealing decisions on applications, or as a substitute for the pursuit of remedies under administrative, civil or criminal law."

³³ Annex to the Commission Implementing Regulation on the reporting of abuses pursuant to Article 15(5) of Regulation (EU) 2018/1240 of the European Parliament and the Council, article 1 (a).

[REDACTED]

"Prior to submission, the applicant must be offered the possibility to confirm:

(iii) the applicant is informed that no personal data should be included in the report and where personal data are nonetheless provided consents that the data will be redacted"³⁴.

Thus, although the above-mentioned legal provisions considerably reduce the likelihood of risks related to the collection of personal data in free text spaces, it is not possible to exclude that the TCN includes personal data in its free text report, especially in the field indicated in point 4 of the annex of IA 1, named "Description and consequences of abuse".

In addition to this information, the applicant must be offered the possibility to upload documents (if available) these one can also contained personal data³⁵.

Although the legal basis prevents it,

Therefore, since the legal basis does not provide any information on the method used to identify and "redact"³⁶ possible personal data from the free text, the following risk should be raised :

Risk R13: The free text space and supporting documents of the reporting of abuse may contain personal data. This could affect the traveller's fundamental right to the protection of personal data, exposing the data subject to processing of data beyond the scope and without fairness.

5.7.8. **Transfer abuse to Central Unit**

The ETIAS Central Unit will monitor, process and analyse all reports of abuses.

Once a year, the ETIAS Central Unit shall submit a report to the Commission, including an anonymised description of the abuses reported, similarities between the cases, recurrences, trends and characteristics and an overview of the actions taken to adapt the information to the general public and applicants.

5.7.9. **Store Data (abuses from commercial intermediaries)**

Abuse Personal data reports will be stored in the central system but the retention period of this information is not clearly defined in the regulation.

Risk R14: Article 54 and 69 define the retention period for the travel authorisation and the logs. No retention period is defined in the legal base or in the architecture or business document concerning the personal data contained in the abuse from commercial field. Store for long period personal data create risks and are not in the sense of the Regulation 2018/1725.

5.7.10. **Access, Rectification, Completion, Erasure**

As defined in the Regulation Article 64, Right of access to, of rectification, of completion, of erasure of personal data and of restriction of processing, and in order to exercise their rights, any applicant shall have the right to address him or herself to the ETIAS Central Unit or to the ETIAS National Unit responsible for his or her application (Article 64 (2)). The unit that receives the request shall examine and reply as soon as possible, and at the latest within 30 days.

³⁴ Annex to the Commission Implementing Regulation on the reporting of abuses pursuant to Article 15(5) of Regulation (EU) 2018/1240 of the European Parliament and the Council, article 7 (iii).

³⁵ Annex to the Commission Implementing Regulation on the reporting of abuses pursuant to Article 15(5) of Regulation (EU) 2018/1240 of the European Parliament and the Council, article 6.

³⁶ Ibidem.



5.7.11. Collect Data (request)

TCN explains the request entering free text in the selected form in the section options for amendment or erasure.

Risk R12: In the framework of the access, amend, erase request by the applicant, the usage of free text can induct semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 64 of the Regulation; article 4 (3) (b) of IA 13).

5.7.12. Process Data (request)

Central system performs a completeness and consistency check.

In case of amendment or erasure of applicant’s data referred to in points (a) to (e) of Article 17(2) of the Regulation, the Common Identity Repository (CIR) shall be updated accordingly

The Central System sends an email notification to the applicant with the form attached informing of the request.

5.7.13. Transfer data (Transfer Request to Central Unit)

Applicant’s request is transferred to ETIAS Central Unit or to the ETIAS National Unit to processes it.

No specific description in the regulation or in the Business use case model documentation were found concerning the storage location or retention period of these requests.

Risk R15: no clear storage location or retention period are defined for applicant request, this can lead to keep personal information to long or in an unsecure location.

5.7.14. Check Application Status

A verification tool shall be implemented on a public website or on a mobile application allowing applicants to check the status of their application (submitted) or travel authorisation (valid, refused, annulled, revoked or expired) and its period of validity.

5.7.15. Overall View

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
Requested access, rectification, completion or erasure, Consent, Abuse report.	TCN, Parental Authority/Legal Guardian.	Execute the requested action on the TCN personal data.	ETIAS Central Storage location CIR	ECU

Table 26 TCN requests access, rectification, completion or erasure of personal data, consent & abuse overview

5.8. Watchlist management

As defined in the Regulation (Article 34(1)) "The ETIAS watchlist shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence. The ETIAS watchlist shall form part of the ETIAS Central System."

This data flow defines how ETIAS NUs and Europol shall introduce, amend or erase records in the ETIAS watchlist on the basis of information related to terrorist offences or other serious criminal offences.

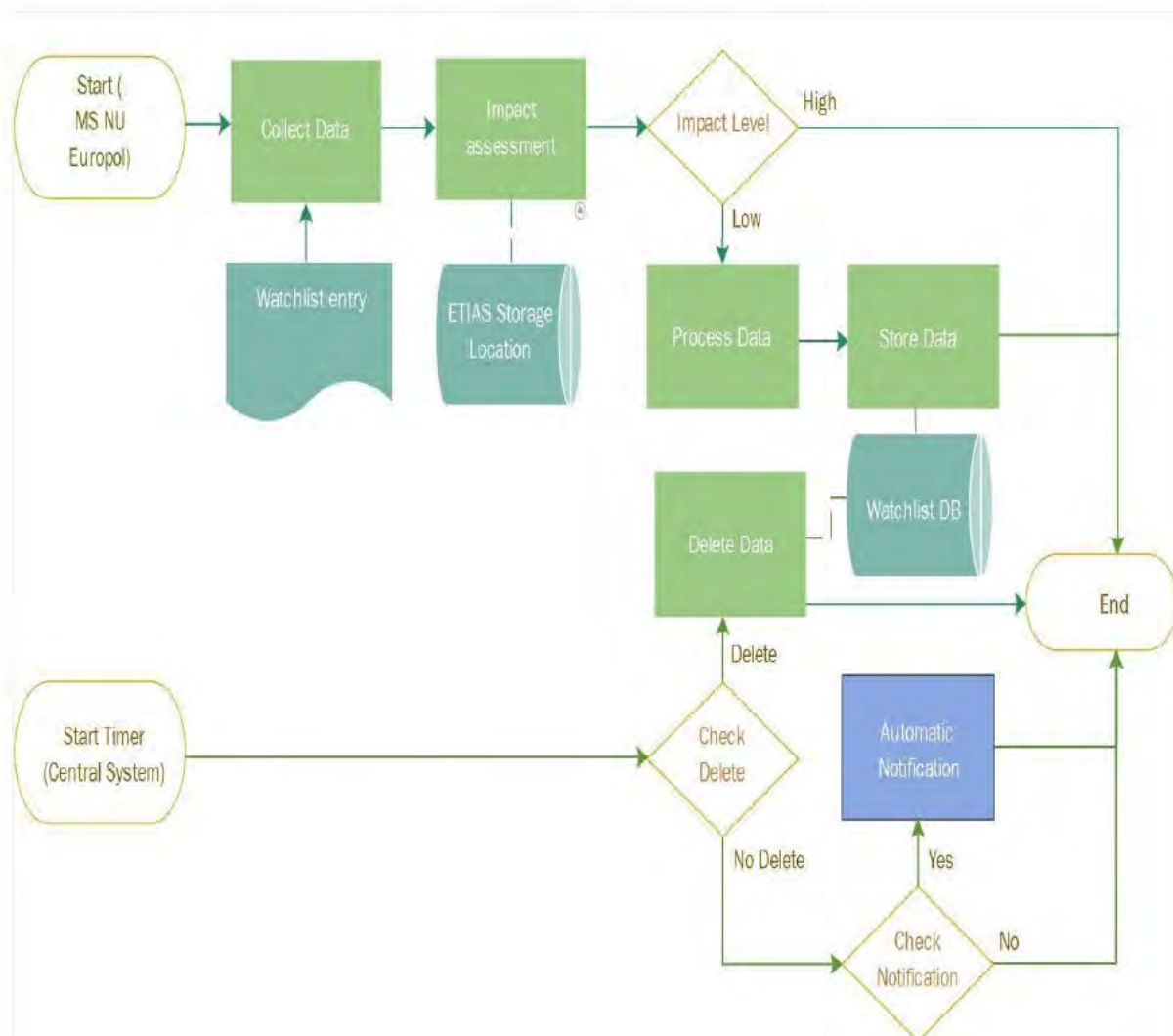


Figure 6 Watchlist management

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 12.1 and indicate for each step you identified which are the supporting assets)
Collect Data	Description can be found in chapter 5.8.2	Europol and Member State National Unit can, as defined in the Regulation (Article 34), create an ETIAS watchlist entry composed of data describe in chapter 5.8.2	SUS 16 - Watchlist Database SUS3 - The communication infrastructure between the ETIAS Central System and the NUIs which shall be secure and encrypted SUS4 - A secure communication infrastructure between the ETIAS Central System and other EU information systems and Europol
Impact assessment	Description can be found in chapter 5.8.3	Europol or a Member State National Unit shall assess the potential impact of the data on the proportion of applications manually processed.	SUS10 - Watchlist assessment tool
Process Data	Description can be found in chapter 5.8.4	Activation of the new entry in the watchlist and the removal of the draft.	SUS 16 - Watchlist Database
Store Data	Description can be found in chapter 5.8.5	Completed with: a national identifier allowing Member States or Europol to correlate the watchlist entry and their records	SUS 16 - Watchlist Database
Start Timer	Description can be found in chapter 5.8.6	Recurrent task to allow the Central System to validate if some watch list entries, drafts or logs should be deleted or will be deleted.	SUS1 - ETIAS Central System
Check & Delete Data	Description can be found in chapter 5.8.7	Central system will validate and if needed delete draft or watchlist entry.	SUS1 - ETIAS Central System SUS 16 - Watchlist Database
Automatic Notification	Description can be found in chapter 5.8.8	ETIAS Central System shall send an automatic notification to the competent authorities if draft should be deleted.	SUS1 - ETIAS Central System

Table 27 Watchlist Management

5.8.1. Prerequisite

Per article 35(1) (letter a) and c)) of the Regulation:

“Before Europol or a Member State enters data into the ETIAS watchlist, it shall:

- a.determine whether the information is adequate, accurate and important enough to be included in the ETIAS watchlist;
- b.assess the potential impact of the data on the proportion of applications manually processed; (will be developed in chapter 5.8.3).
- c.verify whether the data correspond to an alert entered in SIS”;

5.8.2. Collect Data

Europol and Member State National Unit can, as defined in the Regulation (Article 34), create a ETIAS watchlist entry composed of data consisting of one or more of the following items:

- (a) surname;
- (b) surname at birth;
- (c) date of birth;
- (d) other names (alias(es), artistic name(s), usual name(s));
- (e) travel document(s) (type, number and country of issuance of the travel document(s));
- (f) home address;
- (g) email address;
- (h) phone number;
- (i) the name, email address, mailing address, phone number of a firm or organization;
- (j) IP address.

If available, the following items of data shall be added to the related items constituted of at least one of the items of data listed above: first name(s), place of birth, country of birth, sex and nationality.

Until the conditions of Article 35(1)(a) to (c) of the Regulation have been met (determine whether the information is adequate, accurate and important enough to be included in the ETIAS watchlist, verify whether the data correspond to an alert entered in SIS), data entries shall be saved as drafts. Drafts saved for more than 14 calendar days shall be automatically deleted. 72 hours before the deletion, the ETIAS Central System shall send an automatic notification to the competent authorities within the ETIAS National Units or Europol having prepared the draft informing them that the draft shall be automatically deleted.

The secure technical solution shall be designed and implemented to ensure the confidentiality of the data as defined in the Watchlist Implementing Act Article 7. “encryption in transit” and “encryption at rest” must be use to add an additional layer of protection preventing unauthorized access.

Risk R17: Interception of watchlist entry due this sensitive information can have a huge impact on the fundamental right of the data subject. To mitigate the risk strong encryption in transit and at rest should be used. A clear decision on this protocol should be done and analysed to avoid confidentiality risks.

5.8.3. Impact Assessment

Each data entry shall be saved as a draft until it has been established that is deemed adequate, accurate and important enough to be included in the ETIAS watchlist, and the data do not correspond to an alert entered in SIS.

As defined in the Regulation (Article 35(1b))³⁷ Europol or a Member State National Unit shall assess the potential impact of the data on the proportion of applications manually processed. Europol or a Member State National Unit are able to create an active entry in the ETIAS watchlist only when the result of the impact assessment tool reports a low impact.

As described in Watchlist Implementing Act Article 5(5)

To assess the level of impact an entry would have on the number of applications to be manually processed, the impact assessment tool shall perform automatic queries in exact mode on the following data fields of Article 17(2) of that Regulation:

- a. 'place of birth', 'sex', 'current nationality' of the data field (a);
- b. 'country of birth' of the data field (aa);
- c. 'type', 'number' and 'country of issue of the travel document' of the data field (d);
- d. 'phone number' of the data field (g);
- e. 'phone number' of the data field (m).

For the data field of Article 17(8) of the Regulation, the automatic queries shall be performed by default in exact mode while for following data fields of Article 17(2) of that Regulation, the automatic queries shall be performed by default in inexact mode:

- a. 'surname', 'surname at birth', 'date of birth', 'first name(s)' of the data field (a),
- b. 'home address' of the data field (f);
- c. 'email address' of the data field (g);
- d. 'name of firm or organisation', 'email address', 'mailing address' of the data field (m).

The default search mode applicable to the fields of the previous paragraph can be changed from an inexact mode of the search to an exact mode or vice-versa at the time of entering the data. The selected mode will be applicable for the impact assessment as well as for the queries referred to in Watchlist Implementing Act Article 7.

For the purpose of monitoring and for assessing the effectiveness of the impact threshold, the number of impact assessments made as well as an indication of the result of those impact assessments shall be recorded. This indication shall enable to distinguish between the low and high levels of impact as well as the figures expressing this impact. The content itself of the entries shall never be recorded for the purposes of this paragraph.

***Risk R16:** Not appropriate use of the impact assessment tool by National competent authorities could lead to discrimination (generic research made in not-exact mode). By example it checks if there are some difference in the impact for applicant using not exact mode (city or another one, sex...).*

³⁷ Regulation EU 2018/1240 Article 35 (1b) : "Before Europol or a Member State enters data into the ETIAS watchlist, it shall: (..)

b) assess the potential impact of the data on the proportion of applications manually processed; (..)"

5.8.4. Process Data

When the potential impact of the data on the proportion of applications manually process is low, the draft information should be replaced by a new activated entry in the watchlist.

5.8.5. Store Data

All data entered shall be completed with: a national identifier allowing Member States or Europol to correlate the watchlist entry and their records; and the start and end date of the validity of the watchlist entry.

The watchlist entry is stored in the watchlist database, the storage limitation (retention period) is the responsibility of the member states and Europol.

The system records activity logs: User, Timestamp and State of data entry.

The watchlist, the impact assessment tool and the secure technical solution shall keep activity logs containing, at least:

- date and time of access;
- the national authority or Europol;
- the result of the impact assessment referred to in Article 6;
- amendments and erasure of data operations;
- automatic deletions of drafts of Article 3;

Data contained in the watchlist shall not be logged.

Activity and document logs of the watchlist, the impact assessment tool and the secure technical solution shall be stored in the ETIAS Central System.

5.8.6. Start Timer (Central System)

Central System must validate if some watch list entries, drafts or logs should be deleted or will be deleted.

5.8.7. Check Data & Delete Data

An entry in the watchlist shall be automatically deleted once reaching the validity date.

Drafts saved for more than 14 calendar days shall be automatically deleted.

The logs shall be automatically deleted three years after the deletion of the corresponding watchlist entry.

5.8.8. Check Notification & Automatic Notification

72 Hours before the deletion, the ETIAS Central System shall send an automatic notification to the competent authorities within the ETIAS National Units or Europol having prepared the draft informing them that the draft shall be automatically deleted.

5.8.9. Overall View

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
'place of birth', 'sex', 'current nationality', 'country of birth', 'type', 'number' and 'country of issue of the travel document', 'phone number', 'IP address', 'surname', 'surname at birth', 'date of birth', 'first name(s)', 'home address', 'email address', 'name of firm or organisation', 'email address', 'mailing address'	These data are provided by the National Authority in charge of the management of the watchlist - Europol -	The data are compared to the content of the ETIAS Central Storage location to evaluate the number of potential matches. If the number of matches is below the defined threshold, these criteria will be used during the automated process	In the ETIAS watchlist DB location at eu-LISA operational sites	The ETIAS Automated process

Table 28 Watchlist Management overview

5.9. Watchlist review

Europol and Member States shall review and verify the continued accuracy of the data it entered into the ETIAS watchlist regularly.

In accordance to the Commission Implementing Decision defining the technical specification of the ETIAS watchlist and of the assessment tool, the ETIAS Central system shall send automated notifications to the competent authorities within the ETIAS National Units and to Europol to inform them about new or updated alerts entered into SIS that correspond to data entered in the watchlist. Upon receipt of such notification, the competent authorities within the ETIAS National Units or Europol shall manually verify the data. Where the verification reveals that the data entered into the ETIAS watchlist corresponds to a new or updated alert entered in SIS, the watchlist entry shall be deleted

This data flow defines how ETIAS NUs and Europol shall review and verify the continued accuracy of the data it has entered into the ETIAS watchlist regularly, and at least once a year, possible actions are to amend or erase.

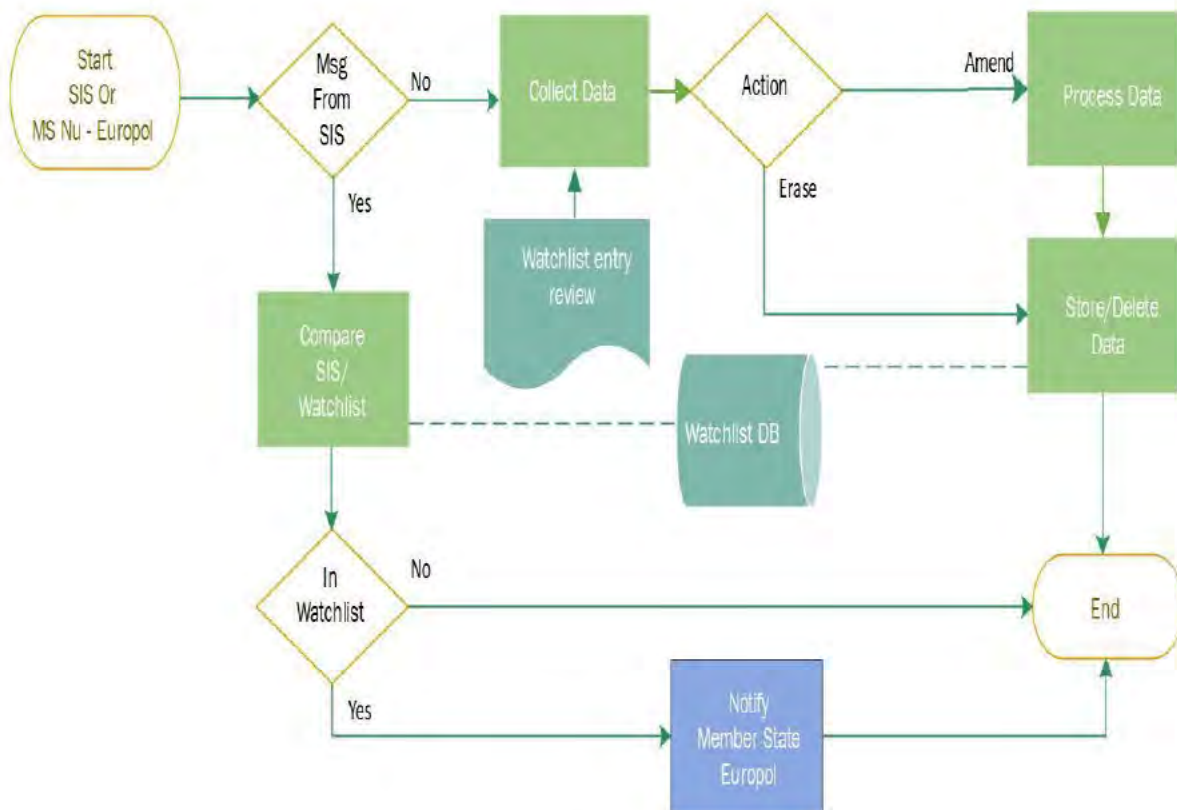


Figure 7 Watchlist review flow

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	The ETIAS NU and Europol are able to review a watchlist entry. (5.9.3)	Review data accuracy.	SUS1 - ETIAS Central System SUS2 - National Uniform Interface (NUI) SUS3 - The communication infrastructure between the ETIAS Central System and the NUs which shall be secure and encrypted SUS4 - A secure communication infrastructure between the ETIAS Central System and other EU information systems and Europol
Retrieving/consulting/using the data	The ETIAS NU and Europol are able to review a watchlist entry. (5.9.3)	Review data accuracy.	SUS16 - ETIAS watchlist Database SUS1 - ETIAS Central System SUS3 - The communication infrastructure between the ETIAS Central System and the NUs which shall be secure and encrypted
Editing/altering the data	The ETIAS NU and Europol are able to update a watchlist entry. (5.9.5)	Review data accuracy.	SUS16 - ETIAS watchlist Database SUS1 - ETIAS Central System SUS3 - The communication infrastructure between the ETIAS Central System and the NUs which shall be secure and encrypted

Table 29 Watchlist review

5.9.1. Message From SIS

This technical step is the validation of the source of the message by the ETIAS Central System. It will validate if the message is coming from the Schengen Information System (SIS) or coming from Europol or the member state National Unit and determine the next step in the dataflow.

5.9.2. Compare SIS/Watchlist

Central System will compare the information included in the SIS messages and the watchlist, to validate if the SIS alert corresponds to an entry already existing in the watchlist. If this entry already exists the responsible Europol or a Member State National Unit should be notified.

5.9.3. Collect Data

The ETIAS NU and Europol will send a new version of the watchlist entry in case of amendment or the id of this entry if it should be deleted. According to the ETIAS Business Process Model the updated watchlist entry will be saved as a draft and continue the data flow.

5.9.4. Process Data

As defined in the Regulation (Article 35(1b)) Europol or a Member State National Unit shall assess the potential impact of the data on the proportion of applications manually processed. Europol or a Member State National Unit are able to enter record in the ETIAS watchlist only when the result of the impact assessment tool reports a low impact. Detail of impact assessment can be found in Chapter 5.8.3.

When the potential impact of the data on the proportion of applications manually process is low, the draft information should be replaced by a new activated entry in the watchlist.

The system records following activity logs: the national authority or Europol:

- Timestamp;
- Draft ID;
- Impact assessment results (High, Low);
- Amendments and erasure of data operations.

5.9.5. Store/Delete Data

The amended watchlist entry is stored in the watchlist database, the storage limitation (retention period) is the responsibility of the MS, depending on specific policies, and on Europol.

Drafts saved for more than 14 calendar days shall be automatically deleted.

In case of erasure of entry, the data entry is deleted immediately.

ETIAS NU or Europol has 48h to complete the one-year review in the watchlist DB after the notification. In case of no action, the watchlist entry will be deleted automatically.

Risk R16: As a draft can be stored for 14 calendar days, mixing draft and active record can be a risk, since over no clear location is defined for draft storage.

5.9.6. Overall View

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
'place of birth', 'sex', 'current nationality', 'country of birth', 'type', 'number' and 'country of issue of the travel document', 'phone number', 'IP address', 'surname', 'surname at birth', 'date of birth', 'first name(s)', 'home address', 'email address', 'name of firm or organisation', 'email address', 'mailing address'	These data are provided by the National Authority in charge of the management of the watchlist and by Europol	The data are compared with the content of the ETIAS Central Storage location to evaluate the number of potential matches. If the number of matches is below the defined threshold, these criteria will be used during the automated process	In the ETIAS watchlist DB location at eu-LISA operational sites	ETIAS Central system. The ETIAS Automated process

Table 30 Watchlist Review overview

5.10. Access to the ETIAS Central System for Border control and law enforcement purposes

This data flow defines how EU Authorities shall be able to consult the relevant personal data after submitting a consultation request.

CHAPTER X PROCEDURE AND CONDITIONS FOR ACCESS TO THE ETIAS CENTRAL SYSTEM FOR LAW ENFORCEMENT PURPOSES.

To exclude systematic searches, the processing of data stored in the ETIAS Central System should take place only in specific cases and only when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to ETIAS when they have reasonable grounds to believe that such access will provide information that will assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence.

- Article 51 Procedure for access to the ETIAS Central System for law enforcement purposes
- Article 52 Conditions for access to data recorded in the ETIAS Central System by designated authorities of Member States
- Article 53 Procedure and conditions for access to data recorded in the ETIAS Central System by Europol

The Regulation (Article 47) defines Access by border authorities to the ETIAS Central System in accordance with Article 47. This access shall be limited to searching the ETIAS Central System to obtain the travel authorisation status of a traveller present at an external border crossing point and to the data referred to in points (a), (c) and (d) of Article 47(2). In addition, border authorities shall be informed automatically of the flags referred to in Article 36(2) and (3) and of the reasons for the flags

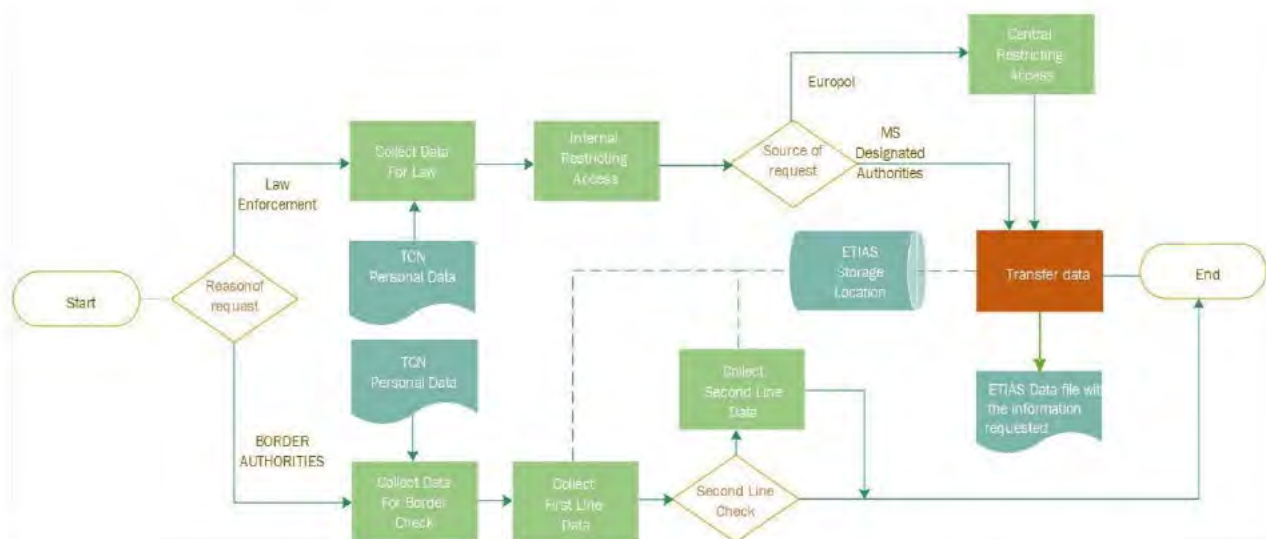


Figure 8 Access for Border control and law enforcement purposes flow

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	Received data consultation request	Consult data	SUS1 - ETIAS Central System SUS2 - National Uniform Interface (NUI) SUS3 - Communication Infrastructure SUS4 - A secure communication infrastructure between the ETIAS Central System and other EU information systems and Europol SUS14 - Software for applications processing and consulting
Retrieving/consulting/using the data	Checking or verifying if the conditions for entry or stay on the territory of the Member States are fulfilled and for the purpose of taking appropriate measures relating thereto. Give to Europol or Member State's designated authorities the mean for prevention, detection or investigation of terrorist offences or other serious criminal offences;	Provide TCN personal data for border check or Law enforcement.	SUS15 - ETIAS Storage Location
Restricting the access to the data	For Europol Access request, the Central Unit will preapprove or not the request coming from Europol	The Regulation Article 53(1) Restrict access to the ETIAS Data for Europol	SUS17 - ETIAS Central Unit

Table 31 Access to the ETIAS Central System for Border control and law enforcement purposes

5.10.1. Prerequisite

Concerning the access to the ETIAS Personal Data's by the Member's state, the Regulation (Article 50):

Member States shall designate the authorities which are entitled to request consultation of data recorded in the ETIAS Central System in order to prevent, detect and investigate terrorist offences or other serious criminal offences

Each Member State shall also designate a central access point which shall have access to the ETIAS Central System. The central access point shall verify that the conditions to request access to the ETIAS Central System laid down in the Regulation (Article 52) are fulfilled.

At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System through the central access points. Only duly empowered staff of the central access points shall be authorised to access the ETIAS Central System.

The Regulation (Article 53(2-3)):

2. The reasoned request shall contain evidence that all the following conditions are met:

(a) the consultation is necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate;

(b) the consultation is necessary and proportionate in a specific case;

(c) the consultation shall be limited to searching with data referred to in Article 52(2) in combination with the data listed under Article 52(3) where necessary;

(d) evidence or reasonable grounds exist to consider that the consultation will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category of traveller covered by this Regulation.

3. Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by a specialised unit of duly empowered Europol officials, which shall examine in an efficient and timely manner whether the request fulfils all the conditions in paragraph 2.

5.10.2. Collect data for Law enforcement

The Europol or Member State's designated authorities can request an access to a TCN personal data;

Concerning Member State's designated authorities following personal data's can be used to search in the ETIAS Central System.

- surname (family name) and, if available, first name(s) (given names);
- other names (alias(es), artistic name(s), usual name(s));
- number of the travel document;
- home address;
- email address;
- phone numbers;
- IP address.

Consultation of the ETIAS Central System with the previous data may be combined with the following data in

[REDACTED]

the application file to narrow down the search:

- nationality or nationalities;
- sex;
- date of birth or age range

As defined in Article 52(2.4) of the Regulation "Consultation of the ETIAS Central System shall, in the event of a hit with data recorded in an application file, give access to the data referred to in points (a) to (g) and (j) to (m) of Article 17(2) which are recorded in that application file as well as to data entered in that application file in respect of the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) recorded in the application file shall only be given if consultation of that data was explicitly requested by an operating unit in a reasoned electronic or written request submitted under Article 51(1) and that request has been independently verified and approved by the central access point. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2)."

Concerning Europol following personal data's can be used to search in the ETIAS Central System.

- name;
- travel document number;
- application number;
- nationality;
- date of birth;
- sex;

The Article 53(1) of the Regulation does not define any restriction concerning the personal data that can be used for the request. Where consultation of data referred to current occupation (job group) and concerning additional question that the applicant must answer Article 17(4) (convicted of any criminal offence, stayed in a specific war or conflict zone, decision requiring him or her to leave the territory of a Member State or of any third countries) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data.

5.10.3. Internal Restricting Access

Concerning the request done by Member State's designated authorities:

A National Unit shall submit a reasoned electronic or written request for consultation of a specific set of data stored in the ETIAS Central System to a central access point.

Upon receipt of the request for access, the central access point shall verify whether the conditions for access referred to in Article 52 are fulfilled, including by checking whether any request for consultation of data referring to current occupation (job group) and concerning additional question that the applicant must answer Article 17(4) (convicted of any criminal offence, stayed in a specific war or conflict zone, decision requiring him or her to leave the territory of a Member State or of any third countries) is justified.

If the conditions for access are fulfilled, the central access point shall process the request.

Concerning the request done by Europol:

[REDACTED]

Article 53(3) of the Regulation:

Europol requests for consultation of data stored in the ETIAS Central System shall be subject to prior verification by a specialised unit of duly empowered Europol officials, which shall examine in an efficient and timely manner whether the request fulfils all the conditions in Regulation (EU) 2018/1240 Article 53(2)

4. Consultation of the ETIAS Central System shall, in the event of a hit with data stored in an application file, give access to the data referred to in points (a) to (g) and (j) to (m) of Article 17(2) as well as to the data added to the application file relating to the issue, refusal, annulment or revocation of a travel authorisation in accordance with Articles 39 and 43. Access to the data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) added to the application file shall only be given if consultation of those data was explicitly requested by Europol. Consultation of the ETIAS Central System shall not give access to the data concerning education referred to in point (h) of Article 17(2).

5. Once the specialised unit of duly empowered Europol officials has approved the request, the ETIAS Central Unit shall process the request for consultation of data stored in the ETIAS Central System. It shall transmit the requested data to Europol in such a way as not to compromise the security of the data.

5.10.4. Central Restriction Access

For Europol access request, the ETIAS Central Unit must consults the request and launches the queries if they fulfil the condition laydown in article 53 of the Regulation.

5.10.5. Transfer Data

Concerning the request done by Member State's designated authorities:

The data stored in the ETIAS Central System accessed by the central access point shall be transmitted to the operating National Unit that made the request in such a way that the security of the data is not compromised.

For Europol:

When the request is processed by the ETIAS Central Unit, Europol will be able to select the access request and can see the results on screen or export them in a structured format.

At these moment activity logs are stored containing User, timestamp of consultation, application consulted ID

5.10.6. Collect Data at Border

The border authorities competent for carrying out border checks at external border crossing points in accordance with Regulation (EU) 2016/399 shall consult the ETIAS Central System using the data contained in the machine-readable zone of the travel document.

5.10.7. First Line Collection Data

For the purpose of checking or verifying if the conditions for entry or stay on the territory of the Member States are fulfilled and for the purpose of taking appropriate measures relating thereto, the immigration authorities of the Member States shall have access to search the ETIAS Central System this access shall be allowed only where the following conditions are met:

- [REDACTED]
- (a) a prior search has been conducted in the EES under Article 26 of Regulation (EU) 2017/2226; and
- (b) the search result indicates that the EES does not contain an entry record corresponding to the presence of the third country national on the territory of Member States.

The ETIAS Central System shall respond by indicating:

- whether or not the person has a valid travel authorisation, and in the case of a travel authorisation with limited territorial validity issued under Article 44, the Member State(s) for which it is valid;
- any flag attached to the travel authorisation under Article 36(2) and (3);
- whether the travel authorisation will expire within the next 90 days and the remaining validity period;
- the data referred to in points (k) and (l) of Article 17(2).

Risk R20: access to ETIAS central system is allowed only if condition defined under Article 49 are met, however it is not possible for ETIAS to validate that these pre-conditions were done or not.

5.10.8. Second Line Data Collection

Where the ETIAS Central System responds by indicating a flag attached to a travel authorisation under Article 36(2)

"In cases where there is doubt as to whether sufficient reasons to refuse the travel authorisation exist, the ETIAS National Unit of the Member State responsible shall have the possibility, including after an interview, to issue a travel authorisation with a flag recommending to border authorities to proceed with a second line check."

The border authorities shall proceed to a second line check. For the purposes of the second line check they shall be authorised to consult the additional information added to the application file in accordance with point (e) of Article 39(1)

"any flags attached to the travel authorisation as laid down in Article 36(2) and (3), together with an indication of the reasons for such flag(s), and additional information relevant to second line checks in the case of Article 36(2), and additional information relevant to border authorities in the case of Article 36(3)"

or point (f) of Article 44(6).

"Where a travel authorisation with limited territorial validity is issued, the following data shall be added to the application file by the ETIAS National Unit which issued that authorisation:

- status information indicating that a travel authorisation with limited territorial validity has been issued;
- the Member State(s) to which the travel authorisation holder is entitled to travel and the validity period of that travel authorisation;
- the ETIAS National Unit of the Member State that issued the travel authorisation with limited territorial validity and its address;
- date of the decision to issue the travel authorisation with limited territorial validity;
- a reference to the humanitarian grounds, reasons of national interest or international obligations

invoked;

- any flags attached to the travel authorisation, as laid down in Article 36(2) and (3), together with an indication of the reasons for such flag(s) and additional information relevant to second line checks in the case of Article 36(2), and additional information relevant to border authorities in the case of Article 36(3).

Where an ETIAS National Unit issues a travel authorisation with limited territorial validity with no information or documentation having been submitted by the applicant, that ETIAS National Unit shall record and store appropriate information or documentation in the application file justifying that decision.”

Where the ETIAS Central System responds by indicating a flag referred to in Article 36(3) and where additional verifications are needed, border authorities may access the ETIAS Central System to obtain the additional information provided for in point (e) of Article 39(1) or point (f) of Article 44(6).

5.10.9. Overall view:

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
TCN personal data	from the ETIAS Central System	Consult data	Member State Central Access Point	Designated Authorities, Europol

Table 32 Access to the ETIAS Central System for Border control and law enforcement purposes overview

5.11. Carriers verification

As defined in the the Regulation (Article 45(1)) "Air carriers, sea carriers and international carriers transporting groups overland by coach shall send a query to the ETIAS Information System in order to verify whether or not third-country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation." This data flow defines how Carriers, through the carrier gateway, get an 'OK/NOT OK/Not applicable' answer indicating whether the person has a valid travel authorisation.

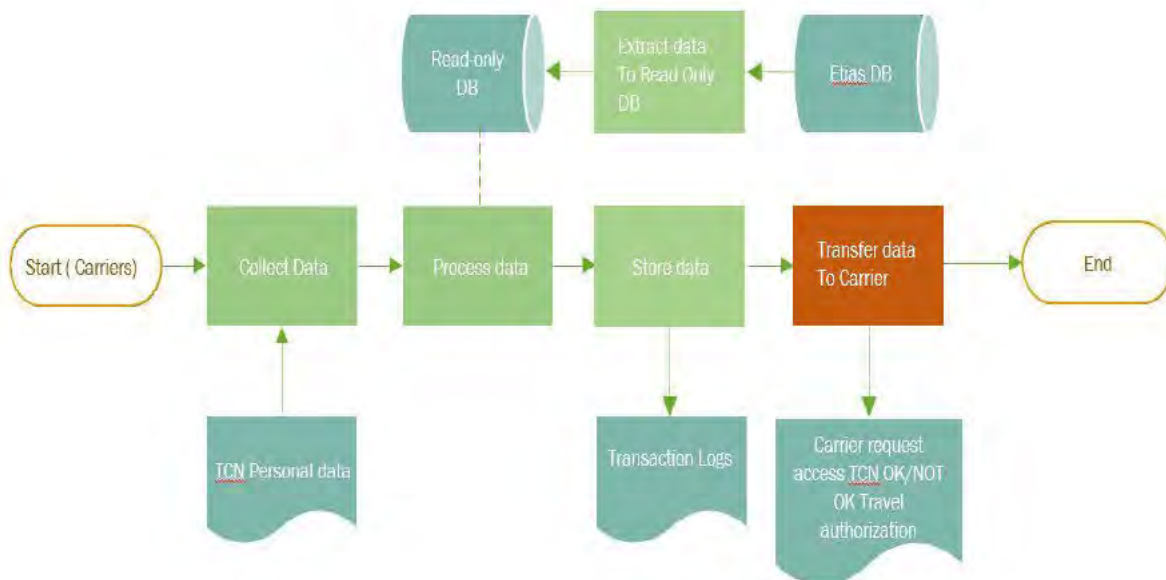


Figure 9 Carrier verification flow

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	See "Collect data" (5.11.2)	The Regulation (Article 13(3)): "Access by carriers to the ETIAS Information System in accordance with Article 45 shall be limited to sending queries to the ETIAS Information System to obtain the travel authorisation status of a traveller."	SUS11 - Carriers Gateway
Retrieving/consulting/using the data	See "Process data" (5.11.3)	Create a read only database as defined in Regulation the Regulation (Article 45(4)). Compare collected Personal data with the data in the read only database.	SUS12- Carrier Gateway Database
Disclosing/transferring the data	See extract Data to Read Only Database (5.11.4) See Transfer Data to carriers (5.11.6)	Generate the Read Only Database. Indicating whether or not the TCN has a valid travel authorization.	SUS15 - ETIAS Storage Location SUS12- Carrier Gateway Database SUS1 - ETIAS Central System SUS11 - Carriers Gateway
Restricting the access to the data	See Prerequisite (5.11.1)	Allow duly authorised members of its staff to access the carrier gateway	SUS11- Carriers Gateway
Storing the data	See Store Data (5.11.5)	Keep logs of all data processing operations	SUS1 - ETIAS Central System SUS12 - Carrier Gateway Database

Table 33 Carriers verification

5.11.1. Prerequisite:

Following Article (3) of the IA 6³⁸:

Carriers shall connect to the carrier interface either through:

- (a) Carriers dedicated network connection or*
- (b) Internet connection*

Recital (9) A carrier may allow duly authorised members of its staff to access the carrier gateway.

As defined in Article (6) of previous COMMISSION IMPLEMENTING REGULATION eu-LISA shall be responsible for the security of the carrier interface, for the security of the personal data it contains

Risk R18: Technical deficiencies in the control of accesses through the carrier interface could allow unauthorized access to personal information.

5.11.2. Collect Data

Carrier Commission Implementing Regulation Article (4) In order to perform the query, the carrier shall provide the following TCN personal data contained in the machine-readable zone of the travel document;

- a) surname (family name); first name or names (given names);*
- b) date of birth; sex; nationality;*
- c) the type and number of the travel document and the three letter code of the issuing country of the travel document;*
- d) the date of expiry of the validity of the travel document.*

Further to this data, the carrier shall also provide:

- a) the scheduled Member State of entry;*
- b) the scheduled day of arrival at the border of the Member State of entry;*
- c) the details (date and local time of scheduled departure, identification number if available, other means of identifying the transport if not) of the means of transportation used to access the territory of a Schengen Member State (flight, ship or coach).*

5.11.3. Process Data

Personal data provided during the "collect data" (5.11.2) are processed to query in a read only database as defined in the Regulation (Article 45(4)) 4.

Central system will compare collected personal data to

the data in the read only database and provides "OK", "Not OK" or "Not applicable" as a reply to the carrier query to the next step of the dataflow. The business rules concerning the data validation is defined in Article 5(2-3-4) of the *Carrier Commission Implementing Regulation*. In case of "Not OK", the reply shall specify that the response is coming from the ETIAS Information System.

5.11.4. Extract Data to Read Only Database

The Read Only database is created based on Article (6) of the *Carrier Commission Implementing Regulation Data*

³⁸ Commission implementing regulation laying down the rules and conditions for the verifications by carriers pursuant to Articles 45(2) and (3) and 46(4) of Regulation (EU) 2018/1240, including specific provisions for the protection of the data where provided by or to carriers, and security rules applicable to this access (see tab 7, chapter 3.2.2.)

[REDACTED]

extraction requirements

"1. In accordance with Article 45(4) of Regulation (EU) 2018/1240, the carrier interface shall use a separate read-only database updated on a daily basis via a one-way mechanism retrieving the minimum necessary subset of ETIAS data. In addition to the daily update of data, to ensure that the data accessed by carriers in the read-only database, referred to in paragraph 1, is consistent with the data stored in the ETIAS Central System, data on issued, annulled and revoked travel authorisations shall be automatically pushed, within 5 minutes, to the read-only database. "

"3. Under no circumstances shall it be possible to initiate a connection from the read-only database toward the ETIAS Central System. The only transfer permitted is from the ETIAS Central System towards the read-only database after the process for extracting, consolidating and loading of the minimum dataset from the ETIAS Central System. All operations performed by this process shall be logged. "

Risk R19: Data integrity is critical and at the moment of this DPIA there are no information concerning the measures included in ETIAS central system to guarantee the integrity of these data during the export to the read-only database.

5.11.5. Store Data

As defined in the Regulation (Article 45(7)) eu-LISA shall keep logs of all data processing operations carried out within the carrier gateway by carriers.

Those logs shall show the date and time of each operation, the data used for interrogation, the data transmitted by the carrier gateway and the name of the carrier in question. Logs shall be stored for a period of two years and protected by appropriate measures against unauthorised access.

5.11.6. Transfer Data to carriers

Carrier Gateway will return to the carrier the result of the sub process "Process Data", "Ok", "NOT OK" or "Not applicable" answer indicating whether or not the person has a valid travel authorization.



5.11.7. Overall View

What do we collect (personal data)	From where/whom (origin of data)	What do we do with it (use)	Where do we keep it (storage)	Who do we give it to (recipients)
The data contained in the machine-readable zone of the travel document and indicate the Member State of entry	In the machine-readable zone of the travel.	Query the ETIAS Information System in order to verify whether third-country nationals subject to the travel authorisation requirement are in possession of a valid travel authorisation.	Carrier system	OK/NOK is provided to the carrier
Logs that show the date and time of each operation, the data used for interrogation, the data transmitted by the carrier gateway and the name of the carrier in question	from the carrier (gateway)	To resolve any potential dispute arising from application of the regulation	ETIAS system	ETIAS

Table 34 Carriers verification overview

5.12. European Border and Coast Guard Agency support to carrier or TCN

This data flow defines how a TCN or Carrier is able to ask for support to European Border and Coast Guard Agency.

The description is based on two main legal bases;

1. Article 46 of the Regulation.

Fall-back procedures in the case of a technical impossibility to access data by carriers
Where it is technically impossible to proceed with the query referred to in Article 45(1) because of a failure of any part of the ETIAS Information System, the carriers shall be exempted of the obligation to verify the possession of a valid travel authorisation. Where such a failure is detected by eu-LISA, the ETIAS Central Unit shall notify the carriers. It shall also notify the carriers once the failure is remedied. Where such a failure is detected by the carriers, they may notify the ETIAS Central Unit

2. The provision of article 13 of the Commission implementing regulation for carriers³⁹
Assistance to carriers

A web form as part of the ticketing tool shall be made available to carriers on a public website in order to allow carriers to request assistance pursuant to Article 46 of the Regulation

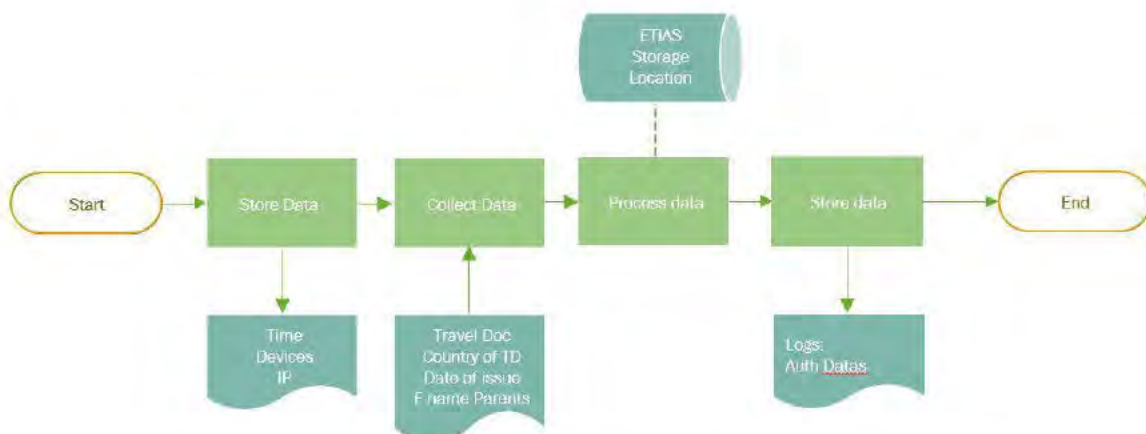


Figure 10 European Border and Coast Guard Agency support to carrier or TCN

³⁹ COMMISSION IMPLEMENTING REGULATION (EU) .../... laying down the rules and conditions for the verifications by carriers³⁹ pursuant to Articles 45(2) and (3) and 46(4) of Regulation (EU) 2018/1240, including specific provisions for the protection of the data where provided by or to carriers, and security rules applicable to this access"

Steps	Description of the process	Description of the purpose (please distinguish between purposes when necessary)	Data supporting assets (Please refer to the typology of supporting assets provided in annex 13.1 and indicate for each step you identified which are the supporting assets)
Collecting of the data	Collect the request from TCN and carrier	The Centre shall act as a single point of contact to register carriers and to provide support to the registered carriers for operational and technical requests.	SUS5- Public website and an app for mobile devices SUS1 - ETIAS Central System SUS11- Carrier Gateway
Editing/altering the data	Helping TCN	Providing support in writing to travellers who have encountered problems when filling in the application form and have requested assistance through a standard contact form; maintaining a list of frequent questions and answers available online;	SUS5- Public website and an app for mobile devices SUS1 - ETIAS Central System SUS11- Carrier Gateway
Storing the data	In addition to the data logged by ETIAS as described in Article 45(7) of the Regulation, the carrier may also log: (a) the time stamps of the request and the response; (b) the content of the received response; (c) the identification of the Carrier's staff members or system executing the request.	Store logs and data provided during the collection phase in case of issued.	SUS1 - ETIAS Central System

Table 35 Carriers verification overview

5.12.1. **Collect data**

European Border and Coast Guard Agency collect data issued from the request of support made by carriers.

The request shall at least contain the following information:

- (a) the identification and contact details of the carrier;
- (b) a summary of the request; and
- (c) whether the request is of a technical nature and, in such case, the date and time of the start of the technical issue.

5.12.2. **Data processing**

Carriers shall receive an acknowledgement of receipt of the request by the ETIAS Central Unit. This receipt shall contain a ticket number. Where the request for assistance is of a technical nature, the ETIAS Central Unit shall send the request to eu-LISA that shall be responsible for providing technical assistance to carriers. If the request for assistance is not of a technical nature, the ETIAS Central Unit shall assist carriers by directing them to relevant information.

5.12.3. **Store data**

Carriers personal data provided during the collection phase should be stored with the same retention period as other ETIAS personal data defined in the Regulation Article 54 and 69 for logs.

5.13. Interaction with other processes

Interaction with other processes	Y/N (Yes/No)
Does these processes rely on personal data being fed in from other systems?	Y (processes in EES; SIS; VIS; EURODAC, ECRIS-TCN, Europol DB, SLTD; TDAWN)
Are personal data from this process re-used in other processes?	N*

Table 36 Interaction with other processes

According to article 20 of The Regulation, “the ETIAS Central System shall compare the relevant data referred to in points (a), (b), (c), (d), (f), (g), (j), (k) and (m) of Article 17(2) and in Article 17(8) to the data present in a record, file or alert registered in the ETIAS Central System, SIS, the EES, VIS, Eurodac, Europol data and Interpol SLTD and TDAWN databases”.

*Following the Commission Working Document, published the 8th of September 2020: “A future API instrument could re-use the data sent under the ETIAS/EES(VIS) Regulations for purposes specific to the API instrument and thus prevent passengers, carriers and service providers of needing to provide the (nearly) identical data twice”.⁴⁰

⁴⁰ COMMISSION STAFF WORKING DOCUMENT EVALUATION of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), Brussels, 8.9.2020 SWD(2020) 174 final, p. 41

6. Necessity and Proportionality Assessment

This section aims to assess the Necessity and the proportionality of ETIAS processing activities (PA) listed in chapter 4.1 Name and description of the data processing activity.

6.1 Necessity (Need for the processing in order to achieve the aims assigned to the organization)	PA
As per articles 6 of the regulation, eu-LISA has been mandated to develop ETIAS Information System and ensure its technical management. Following article 57, eu-LISA is also data controller for the security of the ETIAS Information System Listed below the reasons "why" each ETIAS processing operation is an effective mean to fulfil the mandate assigned to eu-LISA.	General
How and why is the proposed processing operation an effective means for the Agency to fulfil the mandate assigned to it?	General
	General
	PA 1;2;3;5;7
	PA 1;5;6;7;8



risks requires effective responses using modern means. Since these means often involve the processing of significant amounts of personal data, appropriate safeguards should be introduced to keep the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary in a democratic society”.

Listed below the reasons “how” each ETIAS processing operation is an effective mean to fulfil the mandate assigned to eu-LISA

- Tackling new forms of security threats, new patterns of illegal immigration and high epidemic risks

Recital 41: “Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in Directive (EU) 2017/541 of the European Parliament and of the Council (1) or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA”.

PA
2;3;5;6;8

Recital 42: “Access to ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for the private life of individuals and to the protection of personal data of those persons whose personal data are processed in ETIAS”. This interference was mitigated by EU legislator by limiting strictly data retention and data access from competent authorities from Member States and Europol.

Limiting data retention

Recital 41: Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and to Europol only subject to the strict conditions set out in this Regulation. This will ensure that the processing of data stored in ETIAS is limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and other serious criminal offences in accordance with requirements laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case.

PA 4;6

Limiting access to data stored by ex-ante verification:

Recital 42: “(..) access to data stored in ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences should only be granted following a reasoned request by the operating unit of a designated authority explaining its necessity.

PA 5;7

	Limiting access to data stored by an ex post verification:	
	Recital 42: In cases of urgency, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or another serious criminal offence, the verification of whether the conditions were fulfilled should take place after access to such data has been granted to the designated competent authorities. This ex post verification should take place without undue delay and in any event no later than seven working days after the processing of the request.	PA 4;
	Limiting access to the ETIAS Central System for law enforcement purposes	
	Article 53 (1): An operating unit referred to in Article 50(3) shall submit a reasoned electronic or written request for consultation of a specific set of data stored in the ETIAS Central System to a central access point referred to in Article 50(2). Where consultation of data referred to in point (i) of Article 17(2) and points (a) to (c) of Article 17(4) is sought, the reasoned electronic or written request shall include a justification of the necessity to consult those specific data.	PA 5;8
	Limiting access to the ETIAS Central System by designated authorities of Member States Article 52 (1) (b): "access for consultation is necessary and proportionate in a specific case"	PA 4
How have you considered alternatives for fulfilling this task? Why the approach chosen is the least intrusive one?	Limiting access to the ETIAS Central System by Europol Article 53 (2)(b): "the consultation is necessary and proportionate in a specific case"	
	The EU Commission Feasibility Study on ETIAS ⁴¹ underlined that the European Travel Information and Authorisation System is less intrusive than similar systems already adopted by third countries.	General
	The categories of data collected by ETIAS (according to article 17 The Regulation) includes maximum 26 data fields, while the ESTA system in US collect minimum 37 data fields. Data collected in ETIAS are also much more limited than the information currently requested in the Schengen visa process (minimum 44 data fields). ETIAS would also not collect biometric data as opposed to the Schengen visa process since the reliability of biometric data remotely collected cannot be ensured ⁴² .	

⁴¹ European Commission, Feasibility Study for a European Travel Information and Authorisation System (ETIAS) Final Report, 16 November 2016.

⁴² Ibidem, p. 107.

As reminded by the EDPS in his report of 2017⁴³, "the main reference when assessing the necessity of measures that limit the exercise of the rights guaranteed under Article 8 of the Charter is Article 52(1) of the Charter and the case law of the CJEU. In addition, the criteria in Article 8(2) ECHR and specifically the condition for a limitation to be necessary in a democratic society, as interpreted in the case-law of the ECtHR, should also be taken into account in the analysis".

On this base, limitations of the right of personal data protection (article 8 EUCHFR) related to ETIAS processing operations are provided by law but some doubts related to the compliance with the necessity principle still remain legitimate.

Indeed, the EDPS, in the Opinion 3/2017⁴⁴, highlighted the risk of profiling related to the screening rules algorithm and "calls for convincing evidence supporting the necessity of using profiling tools for the purposes of ETIAS"⁴⁵.

This critical point falls under the responsibility of the member of the screening board (European Board and Coast Guard and of Member States), thus it's out of the direct scope of this assessment. However, in chapter 7 (table 41) a risk of wrong technical implementation, testing or maintenance of the risks indicator by eu-LISA (as per art (74)) was raised since it could lead to discrimination and profiling of the data subjects⁴⁶.

Nevertheless, an alternative may be considered concerning the retention of data in the watchlist to protect the right of data subjects to be informed and the right to an effective remedy:

According to article 35 (6) of The Regulation:

"Following a review, Member States and Europol shall withdraw data from the ETIAS watchlist if it is proven that the reasons for which they were entered no longer hold, or that the data are obsolete or not up to date"

The EUCJ case law reminded that data processing (and transfer) for the purpose of preventing terroristic and security threats: "must consist of the least harmful measures to the rights recognised by Articles 7 and 8 of the Charter, while making an effective contribution to the public security objective pursued by the agreement envisaged"⁴⁷.

The ECtHR case law reminded that: "as soon as information can be given without jeopardising the purpose of the measure after termination of the surveillance measure, information should, however, be provided to the persons concerned"⁴⁸.

⁴³ EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 April 2017.

⁴⁴ EDPS, Opinion 3/2017 EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS), 6 March 2017.

⁴⁵ Ibidem, p. 9.

⁴⁶ Infra, Chapter 7, table 41, Risk 19.

⁴⁷ EUCJ, AG Opinion 1/15 of 26 July 2017, on the Draft Agreement between Canada and the EU on the transfer and processing of PNR, paragraph 205 and 220.

⁴⁸ ECtHR, R. Zakharov v. Russia, paragraph 287. See also ECtHR, Szabo and Vissy v. Hungary, paragraph 86.

Following articles 30(2)(c), 42(c) and 43(2) ETIAS Regulation, TCN must be informed of the refusal, annulment or revocation of a travel authorisation. This notification must also contain the grounds of this decision prescribed in Articles 37(1) and (2) in order to lodge an appeal. However, no information is given to the TCN where the reason for refusal is the existence of an entry on the watchlist. This restriction of the right to information is justified by the nature of the watchlist itself and it could be considered "necessary in a democratic society in the interests of national security" (Art. 8, (2) ECHR). Moreover, the reasons for its secrecy are grounded in order to ensure its effectiveness.

Nevertheless, when information concerning the TCN is deleted, following the case law cited above, it is legitimate to think that appropriate information is necessary for the TCN.

Therefore, an alternative to ensure that the processing operation on personal data stored in the watchlist, foreseen by article 6 The Regulation, is the less intrusive possible could be proposed:

"without jeopardizing the purpose of the processing activities, in the case of TCN authorization was refused, revoked, annulled due to a hit in the watchlist, Member States and Europol should inform the data subject after the withdrawal of his/her personal data from the watchlist".

Interaction between ETIAS and ECRIS-TCN

Recital 58 of ETIAS regulation states that ECRIS-TCN would be automatically consulted when examining ETIAS applications. Therefore, the European Commission in its proposal stated that it was not necessary to further justify the necessity and proportionality of the extension of the scope of ECRIS-TCN⁴⁹. EU Agency for Fundamental rights (FRA) expressed serious concerns about using "ECRIS-TCN data for immigration law enforcement purposes outside of criminal proceedings"⁵⁰. EDPS correctly pointed out that the reference to ECRIS-TCN in Recital 58 of the ETIAS Regulation cannot be considered as sufficient to justify an expansion of the ECRIS-TCN scope. Furthermore, article 20 of the ETIAS Regulation specifically – and exhaustively – lists the systems that ETIAS will query and for what reason. This list does not include the ECRIS-TCN.

This DPIA aims to highlight once more the position expressed by EDPS: "broadening of the use of an existing system would be difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law"⁵¹. However, it falls outside of the scope of this DPIA to make a judgement on the compatibility of the legal basis with the data protection principles.

⁴⁹ See The European Commission package of ETIAS consequential amendments Substitute impact assessment, December 2018 pp 18-22.

⁵⁰ FRA, 'Opinion of the European Union Agency for Fundamental Rights concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information System' (2015) 3

⁵¹ EDPS, Formal comment of the EDPS on two proposals to establish the conditions for accessing other EU information system for ETIAS purpose, 19 march 2019, p.3.



	Since legal base cover this aspect, no alternative measures were proposed on it	
Please rate the overall necessity from 1 (low) to 4 (imperative)		3/4

Table 37 Necessity Assessment



6.2 Proportionality (Ensure that advantages resulting from processing are not outweighed by the disadvantages that processing causes)		Stakeholders
What are the benefits of the processing?	- ETIAS proposed processing will reduce procedures and border crossing times. - It will ensure a better accessibility to the information for the third country national, and a higher transparency on the data processing by the ETIAS public website and the app for mobile devices as defined in The Regulation, article 16 and article 71 The Regulation (article 14) states that ETIAS processing activity will protect TCN from discrimination and ensures the respect of fundamental rights: <i>"Processing of personal data within the ETIAS Information System by any user shall not result in discrimination against third-country nationals on the grounds of 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. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability. The best interests of the child shall be a primary consideration".</i> As The Regulation (article 7 point m) define, ETIAS Central Unit <i>"providing support in writing to travellers who have encountered problems when filling in the application form and have requested assistance through a standard contact form; maintaining a list of frequent questions and answers available online;"</i> - ETIAS is increasing the effectiveness of services to citizens and the assistance and protection for the third country nationals.	TCN Data Subjects
	As ETIAS central database strengthens border management, reinforces the EU's visa liberalisation policy, helps preventing irregular migration, limits high epidemic risk and fortifies the fight against terrorism and organised crime.	Member States EUIs Interpol
How eu-LISA limited itself in the ETIAS processing activities?	Following position expressed by European Parliament in its substitute impact assessment ⁵² , keeping logs of all processing activities will be a relevant effort for eu-LISA to ensure the compliance of safeguards required by EU-DPR	General

⁵² European Parliament, The European Commission package of ETIAS consequential amendments Substitute impact assessment, December 2019, p.34 key finding 10.



Benefits for the data subjects	☒ Direct and objective benefits for the individuals impacted by the risks Detailed benefits: ☐ Global benefits for society ☒ Better service for all citizens and/or data subjects at risk <i>ETIAS processing activity will reduce procedures and border crossing times.</i> ☒ Higher accessibility to information <i>It will ensure a better accessibility to the information for the third country national, and a higher transparency on the data processing</i> ☐ Higher environmental sustainability ☐ Higher transparency on data processing ☐ Substantial health improvement for citizens and/or data subjects at risk ☐ Assistance and protection of disadvantage people or people at risk ☒ Safeguarding public interest as regards of Member State security, public security or defence matters <i>ETIAS Central System will strengthen border management, reinforces the EU's visa liberalisation policy, helps preventing irregular migration, limits high epidemic risk and fortifies the fight against terrorism and organised crime</i> ☐ Increasing the effectiveness of services to citizens and/or data subjects at risk ☐ More accessible and inclusive public services ☐ Help and protection of disadvantage people or at risk ☐ Reducing discrimination (by gender, age, nationality, disability, etc.) ☐ Empowerment of the citizen	
Benefits for Agency or Public Administrations in general	[This section lists the benefits that the implementation of the data processing has for the Agency itself]: ☒ Legal compliance ☒ Improving efficiency ☐ Cost reduction ☐ Increased control of the Agency activities ☐ Improved transparency of the data controller (or data processor, if applicable) ☐ Improving security of the Agency ☐ Corporate image enhancement ☐ Others: please list them	
What are the main risks to fundamental rights ⁵³ ?		
Risk	Likelihood (rate from 1 to 4, see knowledge base in annex)	Impact (rate from 1 to 4, see knowledge base in annex)

⁵³ https://www.europarl.europa.eu/charter/pdf/text_en.pdf



Respect for private and family life	2	3
Protection of personal data	3	3
Non-discrimination ⁵⁴	3	4
Right to an effective remedy and to a fair trial ⁵⁵	3	4
Please rate the overall proportionality from 1 (low) to 4 (imperative)		3/4

Table 38 Proportionality Assessment

⁵⁴ Specially for TCNs whose travel authorisation has been refused pursuant article 37 (1)(c)" poses an illegal immigration risk".

⁵⁵ Limited to TCNs whose travel authorisation has been refused pursuant article 37 (1)(b)" poses a security risk" and (c)" poses an illegal immigration risk".

7. Identify and Assess Risks

Based on the definition of risk above, the risk is quantified in terms of impact and likelihood:

- 3) **Impact** represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts toward the data subjects and eu-LISA;
- 4) **Likelihood** expresses the possibility of a risk occurring. It primarily relates to the level of *affectation* of the data protection principle (fairness, transparency, etc.).

In accordance with [13.2. Knowledge base](#) for likelihood and impact ratings in the Annex, risks were classified as Negligible, Limited, Significant and Maximum. To establish the classification, different factors have been considered when rating the different risks relating to ETIAS personal data processing context (risk result).

LOW RISKS		HIGH RISKS	
1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
Rating Likelihood			
It does not seem possible that the data protection principle (fairness, transparency, etc.) could be affected.	It seems difficult that the data protection principle (fairness, transparency, etc.) could be affected.	It seems possible for the data protection principle (fairness, transparency, etc.) to be affected.	It seems extremely likely that the data protection principle (fairness, transparency, etc.) would be affected.
Rating Impact			
Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties.	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome.

Table 39 Risk classification

Final rating is the product of the following operation: Likelihood x impact

1 to 2 Negligible; 3 to 5 Limited; 6 to 10 Significant; 11 to 16 Maximum

Impact	Likelihood				
		1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
	4 : Maximum	4	8	12	16
	3 : Significant	3	6	9	12
	2 : Limited	2	4	6	8
	1 : Negligible	1	2	3	4

Table 40 Risk rating



Nr	Item in the data flow diagram	Description of risk	Associated data protection principle (s)	Likelihood (gross)	Severity (gross)	Overall risk
R1	PA1 –Step 4 Collect Data (5.3.4)	To be able to save a draft, applicants shall provide their email address. Where the applicant e-mail address is not validated at the early stage of Data collecting, the hyperlink could be sent to a different person. Two-factors authentication as proposed by IA 2 using only mail address is not appropriate.	Fairness Transparency Accuracy Security	3	3	9 -Significant
R2	PA 1–Step 9 Store Data Draft (5.3.9)	The Store location of TCN application draft is not clearly defined by regulation or current architecture document.	Fairness, Transparency, Purpose limitation, Storage limitation, Security	3	3	9 -Significant
R3	PA 2 –Step 2 Transfer to payment service provider(s) (5.4.2)	The unique identifier (ID) transferred from ETIAS CS to the payment service provider could allow the latter to create a link with an applicant, due to the request for payment of an ETIAS application. By making a link between the payment owner and an existing application in the ETIAS system, the payment service provider could transfer/sell personal data of the payment owner to third commercial parties (travel agencies, hotel booking websites, etc.).	Fairness, Transparency, Purpose limitation	2	2	4 - Limited
R4	PA 2 –Step 2 Transfer to payment service provider(s) (5.4.2)	Since the contract between the Commission and the Payment provider is not finalized yet, it is impossible to assess if TCNs could exercise their rights before the transfer.	Fairness, Transparency, Purpose limitation	2	3	6 - Significant

R5	PA 2 – Step 5 Collect Data (5.4.5)	TCN personal data (log Timestamp; IP address; Device information ⁵⁶) could be collected without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.	Fairness, Data minimization Storage limitation	3	2	6 - Significant
R6	PA 2 – Step 5 Store Data (5.4.5)	TCN personal data (log Timestamp; IP address; Device information) could be stored without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.	Fairness, Transparency	3	2	6 - Significant
R7	PA 2 – Step 8 Store Decision PA 4 – Step 9 Store logs (5.4.8) (5.6.9)	Lack of procedures and tools for managing authorized person rights due to the fact that NUI user is not aware about the usage of his personal data. (in case of application is being manually processed and accepted, NUI user ID and Time stamps logs are stored)	Fairness transparency Security	2	2	4 - Limited
R8	PA 4 – Step 4 Transfer data to competent National authorities (5.6.4)	Inadequate and incomplete information to the data subject on the processing activity, due to the fact that data subject is not aware about the transfer of his personal data to Ms competent authorities.	Fairness Transparency	3	2	6 - Significant
R9	PA 4 – Step 5 File for extraction (5.6.5)	In the framework of the manual processing, during the hit verification process (article 4(g) of IA 8 Access, Amend, Erase), National Units could export TCN's personal data. Possible lack of expert knowledge about data protection of the extracted personal data at the NUs level could have a negative impact on TCN fundamental rights (unlawful disclosure; processing beyond the purpose/without consent)	Fairness Transparency Accuracy Security Purpose limitation	3	3	9 - Significant

⁵⁶ These logs shall be stored in ETIAS storage location for a period of two years

R10	PA5-Step 2* Store Data (Authentication) (5.7.2) *This risk is valid for all logs	Technical information related to the processing activity (Timestamp; IP address; Device information; Status of response) could be registered, modified or cancelled without the consent of the application requestor	Transparency Store limitation Data minimization	2	2	4 -Limited
R11	PA 4 –Step 6 (5.6.6) Collection free text for additional information	In the framework of the manual processing, usage of free text additional information given by the applicant can induct semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 27 of the Regulation; article 2 (3) (d) and (4), article 3, (3) and (4); article 4, (3); article 6 of the DA 7).	Accuracy	3	3	9 -Significant
R12	PA 5- Step 11 (5.7.11) Free text for amend, erase request	In the framework of the access, amend, erase request by the applicant, the usage of free text can induct semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 64 of the Regulation; article 4 (3) (b) of IA 13).	Accuracy	3	3	9 -Significant
R13	PA 5- Step 7 (5.7.7) Collect free text for abuse report	The free text space and supporting documents of the reporting of abuse may contain personal data. This could affect the traveller's fundamental right to the protection of personal data, exposing the data subjects to processing their data beyond the purpose and without fairness.	Accuracy Fairness Purpose limitation	2	2	4 -Limited
R14	PA5- Step 9 Store Data (abuses from commercial intermediaries) (5.7.9)	Lack of clear and sufficient legal basis for data storage limitation. During the TCN request concerning the abuse from commercial intermediaries, personal data (free text request and supporting documents) are stored in the CS, but the retention period is not clearly defined.	Transparency Store limitation Data minimization	2	2	4 -Limited
R15	PA5- Step 13 (Transfer data) (5.7.13)	In the framework of the request coming from TCN to amend/erase her/his personal data, there is a lack	Fairness Transparency Store limitation	3	2	6 - Significant

		of clear and sufficient legal basis (or architecture information) concerning the storage location and retention period of these requests.	Purpose limitation			
R16	PA6 – Step 3 (Impact Assessment Tool) (5.8.3)	Not appropriate use of the impact assessment tool by National competent authorities could lead to discrimination (generic research made in not-exact mode).	Fairness Transparency Accuracy	2	3	6 - Significant
R17	PA6-Step2 (Collect Data) (5.8.2):	At the time of drafting this DPIA the encryption protocol for "securing data in transit and at rest" is not defined yet. Resulting a possible unauthorized access to personal data.	Accuracy Security Data integrity	3	3	9 - Significant
R18	PA9 –Step 1 Prerequisite (5.11.1)	Technical deficiencies in the control of accesses through the carrier interface could allow unauthorized access to personal information.	Fairness Security	2	3	6 - Significant
R19	PA9-Step4 (5.11.4)	At the time of drafting this DPIA there is a lack of information concerning the technical or organizational process that could undermine the information integrity during the extraction data from the ETIAS DB to the Read-Only DB	Accuracy	2	3	6 - Significant
R20	PA 8- Step 7 Collect data (5.10.7)	Following article 49, (2), immigration authorities querying EES could access additional categories of data by querying ETIAS central system. This information's go beyond the categories of data to be collected under the purpose of EES (details on family members and minors), Article 49, (3).	Purpose limitation	3	3	9 - Significant
R21	PA3 – Step 1 Compare Data Risk indicators from screening rules (5.5.1)	TCN Personal Data will be compared with specific risk indicators defined by the ETIAS Central Unit and ETIAS Screening Board art (7) (2) (c) and art(9) Wrong technical implementation, testing or maintenance of the risk indicators (as per art (74)) could lead	Accuracy	3	3	9 - Significant

		to discrimination and profiling of the data subjects.				
--	--	---	--	--	--	--

Table 41 Identified Risks

7.1 Guiding questions on data protection principles

The risk analysis is performed taking into account the list of data protection principles and evaluating the possible impact on personal data assessing the severity and the likelihood of an event. These two values are used according to the matrix reported in the annex of the document which includes a description of the criteria to assign the value.

The following sections provide the analysis for each data protection principle. According to the responses as estimated value of the likelihood and severity of impact is fixed, a table will report the answers as provided by the eu-LISA DPIA template (Section 12.4)

7.1.1. Fairness analysis

Fairness is a data protection principle related to several aspects of the data processing. The data subject should expect the data processing, the data subject should also be informed before the data processing to know how to exercise her/his rights and should know how her/his data will be used.

Fairness										
Questions	Step of the operation									
	Only answer (Yes/No) to the steps included in your processing operation									
	TCN Draft Application	Submitting application	Automated processing: Identifying hits in the application files	Manual Processing	TCN requests access, rectification, completion or erasure of personal data	Access to the ETIAS Central System for law enforcement purposes	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Is the processing of this data something that people can expect, even without reading the information that you give them?	Y	Y	Y	Y	Y	Y	N	N	Y	Y
2. Consent										
a. If you rely on consent, is it really freely given?	Y	Y	Y	Y	Y	Y	N	N	Y	Y

Fairness

b. If you rely on consent, can people revoke it? Please indicate how.	Y	N	N	Y During the Interview (see 5.1.4)	Y	N	N	N/A	N	N
c. If your processing operation relies on consent, please indicate how you document that people gave it. If it relies on a legal obligation, internal rules or other, please indicate which.	TCN is informed of the storage of the draft application and of the possibility to amend erase it within 48 hours	TCNs give consent by submitting a travel authorisation application	N/A	Art. 27 of the Regulation	TCNs submit a specific request	N/A	N/A	N/A	N/A	TCNs and Carriers submit a specific request for support
3. Could this operation decrease the likelihood that people exercise their fundamental rights (e.g. freedom of expression, belief...) ? E.g. When investigating e-mails, if one checked the content instead of only checking the traffic data, this would decrease	N	N	Y	Y	N	Y	Y	Y	Y	N



Fairness										
the likelihood that people exercise their freedom of expression.										
4. Could this processing operation lead to discrimination?	N	N	N	Y	N	Y	Y	Y	N	N
5. Is it easy for people to exercise their rights to access, rectification, erasure, etc.?	Y	N	N	Y	Y	N	N	N	N/A	N/A
Based on your answers, assess the likelihood that a Data Subject would be affected by an unfair processing of his/her data (rate from 1 to 4)									2/4	
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)									3/4	

Table 42 Fairness analysis

TCNs give consent by submitting an 'electronically signed' travel authorisation application. According to article 3(1) point 18, 'electronically signed' means the confirmation of agreement through the ticking of an appropriate box in the application form or the request for consent.

Regulation 2018/1725, at the article 3 (1) point 15, states that consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

In order to ensure consent of data retention eu-LISA has to develop a consent tool for the purposes of giving or withdrawing consent to prolong the storing of the application file (article 54 of the regulation; articles 1,2,3,4,5 of Commission Delegated Decision xxx/xxx...).

The Article 71 of the ETIAS The Regulation establishes that the ETIAS Central Unit shall provide the general public with all relevant information in relation to applying for a travel authorisation. Moreover, the Article 72 of the ETIAS The Regulation establishes that the Commission shall, in cooperation with the European External Action Service, the ETIAS Central Unit, and the Member States, including their consulates in the third countries concerned, accompany the start of operations by ETIAS with an information campaign to inform third-country nationals.



This should reduce the possibility that the TCNs cannot expect the requirements of their personal data even if they did not read the information provided them.

Nevertheless, the Regulation does not ensure that data subject receives an adequate level of information to “expect” the automatic processing of his/her data.

The article 64 of ETIAS regulation defines the right of access to, of rectification, of completion, of erasure of personal data and of restriction of processing, enforcing the fairness and transparency of the data processing. The latter, ensuring data subjects rights to intervene, strongly reduce the likelihood of an event that could compromise the fairness of the data processing. In this case, the severity of impact for the data subject could be evaluated high due to the limitation of the data subject’s rights.

7.1.2. Transparency analysis

Transparency means that the people whose data are processed should be aware of their data processing and should be able to understand the objectives and the purpose. Regarding the controls at the border, all travellers have the right to be informed on the nature of the control and to a professional, friendly and courteous treatment, in accordance with applicable international, Union and national law⁵⁷.

⁵⁷ Section 1.2 of the Practical Handbook for Border Guards (Schengen Handbook)



Transparency										
Questions	Step of the operation									
	Only answer (Yes/No) to the steps included in your processing operation									
	TCN Draft Application	Submitting application	Automated processing: Identifying hits in the	Manual Processing	TCN requests access, rectification, completion or erasure of personal data	Access to the ETIAS Central System for law enforcement purposes	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Is the information you provide complete and easy to understand?	Y	Y	N	Y	Y	N	N	N	Y	Y
2. Do you make sure the information you provide actually reaches the individuals concerned? Answer Y/N and indicate how.	Y	Y TCNs could find information about their eligibility to travel on the public Website, on the application for mobile devices	N	N	Y Article 64 (1) of the Regulation	N	N	N	Y	Y



		to be used for applying to ETIAS. This information should also be disseminated through a common leaflet and by any other appropriate means (Recital 50; 63)								
3. Is it targeted to the audience? E.g. job applicants may require tailored information. Answer Y/N and indicate how.	Y	Y	N	Y	Y	Y	N/A	N/A	Y	Y
4. In case you defer informing people, please indicate how you justify this.	N	N	N	The results of the assessment of the security, illegal immigration or high epidemic risk and the justification behind the decision to issue or refuse a travel authorisation shall be recorded in the application file	N	N/A	N/A	N/A	N	N



				by the staff member having performed the risk assessment. (Article 26 (7) of the Regulation)						
--	--	--	--	--	--	--	--	--	--	--

Based on your answers, assess the likelihood that a Data Subject would be affected by a non-transparent processing of his/her data (rate from 1 to 4)

3/4

Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)

4/4

Table 43 Transparency analysis

To ensure transparency is especially important if the controller do not collect the data directly from data subjects, but from other sources. As highlighted by EDPS: “in case you have a legal reason not to inform people (or to not inform them just yet - e.g. the early stages of an OLAF investigation), you have to think about when and how you will be able to inform them. If people do not know about your processing of their personal data, they cannot exercise their other rights under the Regulation. If your processing relies on consent, not informing people appropriately means additionally that their consent is invalid”.

The complexity of the automated process could easily increase likelihood for the transparency to be affected with a significant moral and material impact.

Furthermore, the access to the ETIAS Central System for law enforcement purposes and the watch list management could produce a maximum impact, leading to:

- Unlawfulness in the data processing;
- Lack of transparency for automated individual decisions;
- Discrimination

The lack of transparency in the automated process depending on the screening rules, could affect the effectiveness of the manual processing of applications carried out by the ETIAS Central Unit or ETIAS National Units.

7.1.3. Purpose limitation analysis

Purpose limitation is the principle that personal data collected for one purpose should not be re-used for other, incompatible purposes.

Purpose limitation										
Questions	Step of the operation									
	Only answer (Yes/No) to the steps included in your processing operation									
	TCN Draft Application	Submitting application	Automated processing: Identifying hits in the	Manual Processing	TCN requests access, rectification,	Access to the ETIAS Central System for law	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Have you identified all purposes of your process?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2. Are all purposes compatible with the initial purpose?	Y	Y	Y	Y	Y	Y	N	N	Y	Y



Purpose limitation										
3. Is there a risk that the data could be reused for other purposes? Please indicate how you ensure that data are only used for their defined purposes.	N	N	N	N	N	Y	Y	N/A	N	N
4. In case you want to re-use data for scientific research, statistical or historical purposes, do you apply appropriate safeguards? Please indicate which safeguards you apply.	N	Y Article 84 includes safeguards related to non-discrimination	N/A	N/A	N/A	N/A	N/A	N/A	N	N
Based on your answers, assess the likelihood that a Data Subject would be affected by a default of purpose limitation (rate from 1 to 4)								1/4		
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)								4/4		

Table 44 Purpose limitation analysis

According to article 1 of the Regulation, the purpose of this processing is to enable consideration of whether the presence in the territory of the Member States of third-country nationals exempt from the requirement to be in possession of a visa would pose a security, illegal immigration or high epidemic risk. For this purpose, a travel authorisation and the conditions and procedures to issue or refuse it have been introduced.

Article 4 provides more details on the ETIAS purpose:

By supporting the competent authorities of the Member States, ETIAS shall:

(a) contribute to a high level of security by providing for a thorough security risk assessment of applicants, prior to their arrival at external border crossing points, in order to determine



whether there are factual indications or reasonable grounds based on factual indications to conclude that the presence of the person on the territory of the Member States poses a security risk;

(b) contribute to the prevention of illegal immigration by providing for an illegal immigration risk assessment of applicants prior to their arrival at external border crossing points;

(c) contribute to the protection of public health by providing for an assessment of whether the applicant poses a high epidemic risk within the meaning of point 8 of Article 3(1) prior to their or their arrival at external border crossing points;

(d) enhance the effectiveness of border checks;

(e) support the objectives of SIS related to alerts on third-country nationals subject to a refusal of entry and stay, alerts on persons wanted for arrest for surrender purposes or extradition purposes, alerts on missing persons, alerts on persons sought to assist with a judicial procedure and alerts on persons for discreet checks or specific checks;

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

Article 84 defines safeguards to ensure the purpose limitation in reporting and statistic processing activities: “ [t]he duly authorised staff of the competent authorities of Member States, the Commission, eu-LISA and the ETIAS Central Unit shall have access to consult the following data, solely for the purposes of reporting and statistics, without allowing for individual identification and in accordance with the safeguards related to non-discrimination referred to in Article 14”.

In order to limit the diverted use of data entered in the watchlist by competent authorities of the Member states and Europol staff, eu-LISA is responsible for the design and development of an assessment tool, to be used to assess the potential impact of entering data into the ETIAS watchlist on the proportion of applications that are manually processed. Since the system and this specific assessment tool itself are in the design phase, it is impossible, now, to provide an *ex post* assessment of the impacts on purpose limitation. Nevertheless, the importance of this assessment tool is underlined in order to avoid any diverted use of sensitive data (as defined by art. 11 of regulation 2018/1725) entered in the watchlist.

If policies and procedures to perform the data processing in the watchlist are not clear and complete there might be a significant risk that the protection of data is compromised.

Except for the watchlist, the purpose limitation is guaranteed by the configuration of the system. Following the regulation, the system will implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for the purpose of each processing activities are processed.

7.1.4. Data Minimisation

Data minimisation principle means that the data processing operation is done using only the needed personal data to fulfil the purpose of the processing and only keeps them for as long as necessary for this purpose.



Data minimisation										
Questions		Step of the operation								
		Only answer (Yes/No) to the steps included in your processing operation								
	TCN Store Draft	Submitting application	Automated processing: Identifying hits in the Central System	Manual Processing	TCN requests access, rectification, deletion	Access to the ETIAS Central System for law enforcement purposes	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Do data you collect measure exactly what you need to achieve your goal?	Y	Y	Y	Y	N/A	Y	N/A	N/A	Y	Y
2. Are there data items you could remove/mask without compromising the purpose of the process?	N	N	N	Y	N/A	Y	Y	N/A	N/A	Y
3. When you collect data, for instance in forms, do you clearly distinguish between mandatory and optional information?	Y	Y	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A



4. If you want to keep information for statistical purposes, do you appropriately manage the risk of re-identification? Answer Y/N and indicate how.	N	Y (Article 84 (1) of the Regulation)	N/A	N/A	N/A	Y Article 84 (1) of the Regulation	N/A	N/A	N/A	N/A
---	---	---	-----	-----	-----	---------------------------------------	-----	-----	-----	-----

Based on your answers, assess the likelihood that a Data Subject would be affected by a default of data minimization (rate from 1 to 4)	1/4
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)	3/4

Table 45 Data minimisation analysis

Article 17 of the Regulation lists all personal data submitted by the applicant through the application. Article 13 specifies the data accessed by stakeholders depending on their profile. Where the ETIAS National Unit of the Member State responsible deems the information provided by the applicant in the application form to be insufficient to enable it to decide whether to issue or refuse a travel authorisation, it may request additional information or documentation from the applicant (article 27). The Commission Delegated Decision of XXX defines all the additional documents and data that could be requested by National authorities. At the moment, given the unapproved nature of this Delegated Decisions, it is excluded that sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation may be requested as additional information during the manual processing.

No data could be removed (masked or hidden) because this operation could result in a failure of the purpose of the data processing. All these data are needed and mandatory to perform the data processing. In case of statistical purposes, the data are managed as required by article 84 to prevent the identification of individuals.

If the staff is not correctly trained to use the personal data and the TCNs are not properly informed on the data processing purpose and limitation, there could be a risk of collection exceeding purpose.

An illegitimate data processing is potentially low but if it happens the impact on data subjects' rights is significant.

7.1.5. Accuracy analysis

Accuracy principle means that during the data processing operation the competent authority is obliged to make sure that the information processes about people is accurate, in terms of completeness, quality.

Accuracy										
Questions		Step of the operation								
		Only answer (Yes/No) to the steps included in your processing operation								
	TCN Save Draft	Submitting application	Automated processing: Identifying hits in the application files	Manual Processing	TCN requests access, rectification, completion	Access to the ETIAS Central System for law enforcement purposes	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Are the data of sufficient quality for the purpose?	N	Y	Y	Y	N/A	Y	Y	Y	N/A	Y
2. Do your tools allow upgrading/correcting data where necessary?	Y	Y	Y	Y	N/A	N/A	Y	Y	Y	Y



Accuracy										
3. Do your tools allow consistency checks? E.g. automatically checking if birth dates entered are in the right format.	Y	Y	N/A	N/A	N/A	N/A	Y	N/A	Y	Y
4. Do you take sufficient measures to ensure the accuracy of data you collect yourself, and review it? Answer Y/N and indicate how.	N e-mail address need to be validate at the early stage of TCN data collection	N/A	Y	Y	N/A	N/A	Y	N/A	Y	Y
5. Do you take sufficient measures to ensure that the data that you obtain from third parties is accurate, and do you review it? Answer Y/N and indicate how.	N e-mail address need to be validate at the early stage of Applicant data collection	N/A	Y	Y	N/A	N/A	Y	N/A	Y	N/A



Based on your answers, assess the likelihood that a Data Subject would be affected by the processing of inaccurate data (rate from 1 to 4)	3/4
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)	3/4

Table 46 Data minimisation analysis

Article 17 states that the application submitted includes a declaration of the authenticity, completeness, correctness and reliability of the data submitted and a declaration of the veracity and reliability of the statements made. Each applicant shall also state that he or she has understood the conditions for entry referred to in Article 6 of Regulation (EU) 2016/399 and that he or she may be requested to provide the relevant supporting documents at each entry.

For the watchlist:

Art 35

4. Member States and Europol shall be responsible for the accuracy of the data referred to in Article 34(2) that they enter into the ETIAS watchlist and for keeping them up to date. 19.9.2018 Official Journal of the European Union L 236/35 EN 5. Europol shall review and verify the continued accuracy of the data it has entered into the ETIAS watchlist regularly, and at least once a year. Member States shall likewise review and verify the continued accuracy of the data they have entered into the ETIAS watchlist regularly and at least once a year. Europol and Member States shall develop and implement a joint procedure to ensure fulfilment of their responsibilities under this paragraph.

Europol shall review and verify the continued accuracy of the data it has entered into the ETIAS watchlist regularly, and at least once a year. Member States shall likewise review and verify the continued accuracy of the data they have entered into the ETIAS watchlist regularly and at least once a year. Europol and Member States shall develop and implement a joint procedure to ensure fulfilment of their responsibilities under this paragraph

7.1.6. Storage limitation analysis

Storage limitation principle refers to keeping personal data as long as necessary and as short as possible.

Storage limitation (Retention period)

Questions	Step of the operation									
	Only answer (Yes/No) to the steps included in your processing operation									
	TCN Save Draft	Submitting application	Automated processing: Identifying hits in the application files	Manual Processing	TCN requests access, rectification,	Access to the ETIAS Central System for law	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers
1. Is the retention period defined by EU legislation?	Y	Y	Y	Y	N/A	Y	N	N	N	N/A
2. Can you distinguish retention periods for different parts of the data? Please indicate the retention period.	N	Y Article 54 1.(a) the period of validity of the travel authorisation; +	Y	Y	N/A	Y	N	N	N	N/A

Storage limitation (Retention period)

		2. An additional period of no more than three years								
3. Is it really necessary to keep data for this period with regard to the purpose? Please indicate the purpose for retaining the data for this period.	Y Amend, erase personal data	Y Article 54 1. For the purpose of supporting the decision to deliver, refuse, annul or revoke the travel authorisation + 2. For the purpose of facilitating a new application after the expiry of the validity period of an ETIAS travel authorisation	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A



Storage limitation (Retention period)										
4. If you cannot delete the data immediately after the retention period, can you restrict or block access to it?	Draft is automated erased within 48 hours	Y	Y	Y	Y	N/A	N	Y	N	N/A
5. Will your tools allow automated erasure at the end of the storage period?	Y	Y	Y	N/A	N/A	N/A	N	N	N	N/A

Based on your answers, assess the likelihood that a Data Subject would be affected by a default of storage limitation (rate from 1 to 4)	2/4
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)	4/4

Table 47 Storage limitation -retention period analysis

Article 54: Each application file shall be stored in the ETIAS Central System for:

- (a) the period of validity of the travel authorisation;
- (b) five years from the last decision to refuse, annul or revoke the travel authorisation, the application file shall be deleted within seven days from the date of the deletion of the data in that record, file or alert.

Article 54 : Upon expiry of its retention period the application file shall automatically be erased from the ETIAS Central System.

In case of inability to erase data timely, data access should be blocked after the legal retention period



Article 35 : 6. Following a review, Member States and Europol shall withdraw data from the ETIAS watchlist if it is proven that the reasons for which they were entered no longer hold, or that the data are obsolete or not up to date.

Article 45 : 2 : Carriers may store the information sent and the answer received in accordance with the applicable law. The OK/NOT OK answer shall not be regarded as a decision to authorise or refuse entry in accordance with Regulation (EU) 2016/399.

The implementing decision (EU) .../... of XXX laying down the rules and conditions for the verifications by carriers, as well as provisions for data protection, security for the carriers' authentication scheme and fall-back procedures, at the moment, does not include any provision on data stored by carriers.

7.1.7. Security analysis

The security principle in data protection means that during the data processing the information should be managed ensuring its confidentiality, integrity and availability. This approach is based on EDPS guidance on "Security measure for personal data processing"⁵⁸

Article 4 (f) of Regulation 2018/1725 states that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"

Since the security risk assessment for ETIAS is not performed yet, the answers to questions (1)-(5) and (6) of the following tab is negative (N) because these informations are related to the Information Security Management (ISRM) process. This section aims to underline the security principle in data processing activities, referring to confidentiality and integrity.

'Confidentiality' refers to the property of information only being available to authorised persons with a need to know. 'Integrity' refers to the property of information not being able to be changed without proper authorisation. 'Availability' refers to article 33(1)(c) that stresses "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

As highlighted by EDPS, "breaches of confidentiality of personal data can cause various kinds of harm, such as psychological distress (e.g. a leak of medical data) and financial harm (e.g. when leaked personal data are used for identity theft) to individuals. To avoid this, you should design your systems in a way that access to personal data is limited on a strict need-to-know basis and that personal data are protected against being read by unauthorised person at all stages – whether at rest or in transit, using encryption where appropriate"⁵⁹. Moreover, "[b]reaches of integrity of personal data can affect people if decisions about them are taken on the basis of corrupted information"⁶⁰, and "[b]reaches

⁵⁸ EDPS, Security Measures for Personal Data Processing Article 22 of Regulation 45/2001, 21 March 2016.

⁵⁹ EDPS, Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, 3 July 2019 p. 15

⁶⁰ Ibidem.



of availability prevent the very use of the data”⁶¹.

The typical high-level risks identified that could affect personal data principles are the following:

- Malware, ransomware and cryptojacking which can destroy or disrupt the ETIAS central system with the consequences of compromising integrity and availability of the personal data;
- Denial of service which can disrupt the ETIAS central system with the consequences of compromising availability of the personal data;
- Data breaches which can disclose data of the ETIAS central system with the consequences of compromising confidentiality of the personal data;
- Physical manipulation, damages, theft, loss that can allow data collection, espionage, disclosure with the consequences of compromising confidentiality, integrity and availability of the personal data.

Security										
Questions		Step of the operation								
		Only answer (Yes/No) to the steps included in your processing operation								
	TCN Draft Application	Submitting application	Automated processing: Identifying hits in the application files	Manual Processing	TCN requests access, rectification, completion	Access to the ETIAS Central System for law enforcement purposes	Watchlist management	Watchlist review	Carriers access for verification purposes	EBCGA support to carriers

⁶¹ Ibidem.



Security									
1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks that could affect personal data and the IT systems supporting their processing?	N/A	Y	Y	Y	Y	Y	Y	Y	N/A
2. Do you target the impact on people's fundamental rights, freedoms and interests, and not only the risks to the organisation?	Y	Y	Y	Y	N/A	Y	N	N	N/A



Security										
3. Do you take into account the nature, scope, context and purpose of processing when assessing the risks?	Y	Y	Y	Y	N/A	Y	Y	Y	Y	N/A
4. Do you manage your system vulnerabilities and threats for your data and systems?	N	Y	Y	Y	N/A	Y	Y	Y	Y	N/A
5. Do you have resources and staff with assigned roles to perform the risk assessment?	N/A	Y	Y	Y	Y	Y	Y	Y	Y	Y



Security									
6. Do you systematically review and update the security measures in relation to the context of the processing and the risks?	N/A	Y	Y	Y	Y	Y	Y	Y	Y
Based on your answers, assess the likelihood that a Data Subject would be affected by a breach of security in the processing of his/her data (rate from 1 to 4)									2/4
Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)									4/4

Table 48 Security analysis

“Logging accesses to personal data is a way to ensure that you spot any possible breaches and to show proof of who accessed the data. Breaches of integrity of personal data can affect people if decisions about them are taken on the basis of corrupted information. To avoid this, you have to for example design your systems in a way that personal data can only be changed by authorised users and that such changes are auditable. Breaches of availability prevent the very use of the data”⁶²

Following article 69 (4) “Such logs may be used only for monitoring the admissibility of data processing and to ensure data security and integrity. The logs shall be protected by appropriate measures against unauthorised access. They shall be deleted one year after the retention period referred to in Article 54 has expired, if they are not required for monitoring procedures which have already begun”.

⁶² EDPS, Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, 3 July 2019 p. 15.

Without predicting the result of a detailed security risk analysis, some security risks with significant impact on personal data are listed in the table below:

Risk ID	Item in data flow	Explanation and reference	Countermeasure	L	I	Risk value	Risk value after counter measure
SR1	Unsecure web interface Public interface 5.3 TCN Draft Application 5.3.4 Collect data 5.3.9 Store Data (draft) 5.3.9 Step Store data (draft) 5.7 TCN requests access, rectification, completion or erasure of personal data, consent & abuse. – Step 5.7.1 to 5.7.14	Poorly developed web interface could reveal vulnerabilities exploited by hacker to steal personal data in databases. https://owasp.org/www-project-top-ten/	Implement countermeasures explained on OWASP website for each of the top ten vulnerabilities: 1. Injection. 2. Broken Authentication. 3. Sensitive Data Exposure 4. XML External Entities (XXE). 5. Broken Access Control 6. Security Misconfiguration. 7. Cross-Site Scripting XSS. 8. Insecure Deserialization. 9. Using Components with Known Vulnerabilities. 10. Insufficient Logging & Monitoring.	2	4	8	2
SR2	Unsecure web interface Public interface 5.3 TCN Draft Application 5.3.4 Collect data 5.3.6 Store or Submit Draft 5.7 TCN requests access, rectification, completion or erasure of personal data, consent & abuse. – Step 5.7.1 to 5.6.14	Poorly developed web interface could reveal vulnerabilities exploited by hacker to steal personal data of travel authorization applicants. https://owasp.org/www-project-top-ten/	Implement countermeasures explained on OWASP website for each of the top ten vulnerabilities: 1. Injection. 2. Broken Authentication. 3. Sensitive Data Exposure 4. XML External Entities (XXE). 5. Broken Access Control 6. Security Misconfiguration. 7. Cross-Site Scripting XSS. 8. Insecure Deserialization. 9. Using Components with Known Vulnerabilities. 10. Insufficient Logging & Monitoring.	2	2	4	2



SR3	Unsecure web interface Carrier interface 5.11 Carriers verification 5.11 Carriers verification – step 5.11.3 Process Data – step 5.11.4 Extract Data to Read Only Database 5.11.5 Store Data 5.11.6 Transfer Data to carriers	Poorly developed web interface could reveal vulnerabilities exploited by hacker to steal personal data in databases. Uncontrolled carrier security environment is an additional vulnerability https://owasp.org/www-project-top-ten/	Implement countermeasures explained on OWASP website for each of the top ten vulnerabilities: 1. Injection. 2. Broken Authentication. 3. Sensitive Data Exposure 4. XML External Entities (XXE). 5. Broken Access Control 6. Security Misconfiguration. 7. Cross-Site Scripting XSS. 8. Insecure Deserialization. 9. Using Components with Known Vulnerabilities. 10. Insufficient Logging & Monitoring. 11. Ensure security controls in place at carrier side are satisfactory.	2	4	8	2
SR4	Unsecure mobile application 5.3 TCN Draft Application Step Collect data - Step Store or Submit Draft 5.7 TCN requests access, rectification, completion or erasure of personal data, consent & abuse.– Step 5.7.1 to 5.7.14	Poorly developed mobile application could reveal vulnerabilities exploited by hacker to steal applicants' personal data.	Implement recommended OWASP countermeasures for each of the top ten vulnerabilities. https://owasp.org/www-project-mobile-top-10/	2	2	4	2
SR5	Unsecure log management Secure mail service 5.3 TCN Draft Application 5.3.8 Transmission of the hyperlink 5.3.13 Use mail address for authentication 5.4.9 Mail decision Notification	Logs of mail service contains personal data, and uncontrolled access to these logs could lead unlawful data processing.	Encrypt or anonymize personal data. Implement and monitor an access control policy	2	4	8	2

Table 49 Security risks first set

8. Measures to Mitigate Identified Risks

In this chapter, mitigation measures are proposed to each risk and the effect on the risk is defined by the following ratings (Likelihood x Severity):

- **Eliminated:** Mitigation measure eliminate the original identified risk
- **Reduced:** Residual risk is lower than the original identified risk
- **Transferred:** Risk is to be addressed also in a different DPIA
- **Accepted:** Risk and/or mitigation measure falls partially outside of the scope of this DPIA

Out of the 21 risks identified in the previous section remain 16 "Significant" risks.

Considering proposed measures, the residual ratings of the risks are the following:

- Eliminated: Risk 10
- Reduced: Risks 1-2-3-4-5-6-8-11-12-13-14-15-17-19-20-21
- Reduced & Transferred: Risks 7-9-16-18

It must be noted that this list presumes the acceptance of all the proposed mitigation measures. In case of refusal of mitigations measures and where further clarifications will be provided by actor involved in design phase, the risks need to be reassessed accordingly.

Considering that the present DPIA is carried out before ETIAS design and development phase, the mitigation measures listed below should be considered as an integral part of the data protection by design process.

The following mitigation measures are technical and organisational recommendations as per articles 4 and 33 of the EU GDPR on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, which aim to reduce either the likelihood or the impact of the identified risks in chapter 7.

N°	Risk	Option to reduce or eliminate risk	Effect on risk	Likelihood (residual)	Severity (residual)	Residual risk	Measure approved (Yes/No)
1	R1	Eu-LISA shall ensure that a technical solution is designed and developed to validate the e-mail address of the applicant at the early stage of the Data collection.	Reduced	1	3	3	Y
2	R2	Eu-LISA shall ensure the design and the development of a secure storage for data application Draft to enable the confidentiality, integrity and availability of the information contained to be respected.	Reduced	1	3	3	Y

		The security Risk assessment should include information on this asset.					
3	R3; R4;	Eu-LISA shall ensure that all the legal requirements are implemented in order to enable that in the framework of the contract to be finalised between the commission and the payment service provider, only the unique identifier (ID) shall be transferred to the third parties (e.g. payment providers) in order to be processed in compliance with Data Protection regulation and principles.	Reduced	1	2	2	Y
4	R5, R6	Eu-LISA, after establishing whether the technical solutions make it possible to establish a link between the logs and the applicant, shall provide sufficient information about the processing of personal data on several levels, which is easily accessible to the data subjects.	Reduced	1	2	2	Y
5	R7	Based on the Train-the-Trainer approach, Eu-LISA shall provide all relevant information/training to raise the awareness of the Member States about the data relating to NUIs users stored in the CS.	Reduced/ Transferred ⁶³	1	2	2	Y
6	R8	Eu-LISA shall ensure that the design of the "software for the purpose of manual processing of applications and for accessing and amending data for the purposes of appeals", is implemented by including a disclaimer informing travelers that their data could be manually processed by competent authorities of one or more Member States. This will help to ensure the exercise of the right of appeal. (Article 4(1) of the IA 8 is an open list of specific functionalities)	Reduced	1	2	2	Y
7	R9	Eu-LISA shall share the outcomes of this assessment with Member States in order to raise awareness for them to elaborate mitigation measure at their level (e.g. authorized staff training)	Reduced/ Transferred ⁶⁴	2	2	4	Y
8	R10	Eu-LISA shall ensure the design of a technical solution to fairly obtain the consent of data subject to the storage of logs of his/her authentication (Timestamp; IP address; Device information; Status of response) in the Central System. Eu-LISA shall also ensure the integrity of those log files.	Eliminated	0	2	0	Y

⁶³ Mitigation measure related to this risks falls also under the responsibility of Member States. That is why this risk is reduced regarding eu-LISA responsibility and considered as 'transferred' for the remaining aspect not in scope of ETIAS DPIA.

⁶⁴ Mitigation measure related to this risks falls also under the responsibility of Member States. That is why this risk is reduced regarding eu-LISA responsibility and considered as 'transferred' for the remaining aspect not in scope of ETIAS DPIA.

9	R11; R12;	Eu-LISA shall ensure the development of all technical solutions to enable quality compliance of data entered by applicant or third party, in the free text space and limit as much as possible the use of free text as foreseen by legal basis (IA 1 Annex).	Reduced	2	2	4	Y
10	R13	Eu-LISA shall implement of all legal requirements, notably from AI 1 and his ANNEX, by ensuring that the applicant is informed prior to submission that no personal data should be included in the report and where personal data are nonetheless provided consents that the data will be redacted.	Reduced	1	2	2	Y
11	R14	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the data retention period in Central System of personal data related to the abuse reports, notably free text and supporting documents has the same duration as that foreseen for the personal data related to the application.	Reduced	1	2	2	Y
12	R15	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the storage location and the data retention period of applicant request concerning the access, rectification, completion, erasure of personal data, consent and abuse, are the same as those foreseen for the data related to the application.	Reduced	2	2	4	Y
13	R16	Eu-LISA shall deliver the training to MS competent authorities following the Train-The-Trainer approach on how the impact assessment tool will support Watchlist management.	Reduced and transferred ⁶⁵	1	3	3	Y
14	R17	Eu-LISA shall ensure the design and the implementation of a secure encryption mechanism following best practices and requirement from legal basis to enable the integrity and the confidentiality of the data.	Reduced	1	3	3	Y
15	R18	Eu-LISA shall include the carrier interface in the scope of the Security Risk assessment and identify the appropriate measures which will ensure the confidentiality, integrity and availability of carrier interface and personal data that will be managed.	Reduced/ Transferred ⁶⁶	1	3	3	Y
16	R19	Eu-LISA shall adopt all technical measures to ensure the integrity and the confidentiality of personal data in the extraction to the RODB	Reduced	1	3	3	Y
17	R20	Before giving an access to the information relating to the traveller's parental authority or legal guardian information ETIAS should	Reduced	1	3	3	Y

⁶⁵ Mitigation measure related to this risks falls also under the responsibility of Member States. That is why this risk is reduced regarding eu-LISA responsibility and considered as 'transferred' for the remaining aspect not in scope of ETIAS DPIA.

⁶⁶ This risks related to the access by carrier through Web services is also tackled in the specific EES WS' DPIA but have an impact on ETIAS. That is why the risks, although mention here, are reduced (partially) and considered as 'transferred' for the remaining aspect not in scope of ETIAS DPIA.



		validate that a prior search has been conducted in the EES under Article 26 of Regulation (EU) 2017/2226 and the search result indicates that the EES does not contain an entry record corresponding to the presence of the third country national on the territory of Member States.					
18	R21	Eu-LISA shall adopt secure development standard during the development, testing and maintenance phases to guarantee that the risk indicators will be correctly developed and tested, as defined in article 7(c) article 33 and article 74 (1).	Reduced	1	3	3	Y

Table 50 Option to reduce or eliminate risk



9. DS (Data Subjects) Comments (If Applicable)

Not applicable as Data Subjects (Applicants, Parents of the Applicant or Family members, Commercial Intermediaries, suspected persons,) cannot be consulted.

10. Conclusions and Recommendations

After carrying out the data protection impact assessment and after seeking the advice of the Data Protection Officer, the data controller/person responsible of the design is of the opinion that:

- ☒ Taking into account the safeguards, security measures and controls to mitigate the risks, the processing of personal data **does not represent a high risk** to the rights and freedoms of natural persons and the processing of personal data will be carried out.
- ☐ Taking into account the safeguards, security measures and controls to mitigate the risks, the processing of personal data **still represents a high risk** to the rights and freedoms of natural persons and the European Data Protection Supervisor will be consulted.
- ☐ Taking into account the safeguards, security measures and controls to mitigate the risks, the processing of personal data **still represents a high risk** to the rights and freedoms of natural persons and the processing of personal data will not be carried out.

Table 51 Conclusions and Recommendations

As outlined in chapter 8, out of the 21 risks identified in the present report 18 are rated as "Significant" risks.

Considering proposed measures, the residual rating of the risks are the following:

- Eliminated: Risk 10
- Reduced: Risks 1-2-3-4-5-6-8-11-12-13-14-15-16-17-19-20-21
- Reduced & Transferred: Risks 7-9-18

It must be noted that this list presumes the acceptance of all the proposed mitigation measures. In case of refusal of mitigations measures and where further clarifications will be provided by actor involved in design phase, the risks need to be reassessed accordingly.

Considering that the present DPIA is carried out before ETIAS design and development phase, the mitigation measures listed below should be considered as an integral part of the data protection by design process.

In addition to the mitigation measures proposed in Chapter 8, the analysis carried out so far, from the eu-LISA perspective, allows us to make the following recommendations:

1. A **Security Risk Assessment** should be performed to identify, analyse and solve potential security vulnerabilities of the ETIAS infrastructure eu-LISA has to design, develop and maintain in operation
2. **Risks of potential violations of fundamental rights related to the data processing activities of ETIAS**, which do not fall within the scope of the present DPIA, have already been raised by the EDPS in the Opinion 3/2017⁶⁷ and still need to be addressed in specific impact assessments to be performed by FRONTEX and Member States.

⁶⁷ EDPS, Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS), 17 March 2017.

In particular, with regard to the **risks of profiling** related to the **risk indicators for screening rules**⁶⁸, especially to the assessment of the illegal migration risks. Indeed, there is no definition of illegal immigration in the regulation and this lack of certainty could generate an abuse of discretionary powers, raising concerns on the necessity and proportionality of the Screening rules mechanism.

11. Action Plan

On the basis of the elements highlighted in this DPIA, the following action plan indicates the actions to be taken to bring the design and development phase into line with the principle of data protection by design and by default.

Since at the moment no Product Owner is appointed for ETIAS, the person accountable for the implementation of the mitigation measures proposed in this report is the Program manager/Product owner (when appointed) that will coordinate the actions with different sectors involved in the design.

Risk	Description of the control/measure	Accountable for the implementation	Expected date	Status
Risk 1: To be able to save a draft, applicants shall provide their email address. Where the applicant e-mail address is not validated at the early stage of Data collecting, the hyperlink could be sent to a different person. Two-factors authentication as proposed by IA 2 using only mail address is not appropriate	Eu-LISA shall ensure that a technical solution is designed and developed to validate the e-mail address of the applicant at the early stage of the Data collection.	<i>ETIAS Program manager/Product owner seconded by Architecture</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 2: The Store location of TCN application draft is not clearly defined by regulation or current architecture document.	Eu-LISA shall ensure the design and the development of a secure storage for data application Draft to enable the confidentiality, integrity and availability of the information contained to be respected. The security Risk assessment should include information on this asset	<i>ETIAS Program manager/Product owner seconded by Architecture & Security</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 3: The unique identifier (ID) transferred from ETIAS CS to the payment service provider could allow the latter to create a link with an applicant, due to the request for payment of an ETIAS application. By making a link between the payment owner and an existing application in the ETIAS system, the payment service provider could transfer/sell personal data of the payment owner to third commercial	Eu-LISA shall ensure that all the legal requirements are implemented in order to enable that in the framework of the contract to be finalised between the commission and the payment service provider, only the unique identifier (ID) shall be transferred to the third parties (e.g. payment providers) in order to be processed	<i>ETIAS Program manager/Product owner seconded by Business Relations Management</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved

⁶⁸ See Supra, chapter 3.3 p. 25

parties (travel agencies, hotel booking websites, etc.).	in compliance with Data Protection regulation and principles.			
Risk 4 : Since the contract between the Commission and the Payment provider is not finalized yet, it is impossible to assess if TCNs could exercise their rights before the transfer.				
Risk 5 :TCN personal data (log Timestamp; IP address; Device information ⁶⁹) could be collected without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.	Eu-LISA, after establishing whether the technical solutions make it possible to establish a link between the logs and the applicant, shall provide sufficient information about the processing of personal data on several levels, which is easily comprehensible by the data subjects.	ETIAS Program manager/Product owner seconded by Architecture, Security and DPO	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 6: TCN personal data (log Timestamp; IP address; Device information) could be stored without providing proper information or in unauthorized manner. Legal base does not clarify if a direct link can be done between the applicant and these logs.				
Risk 7: Lack of procedures and tools for managing authorized person rights due to the fact that NUI user is not aware about the usage of his personal data. (in case of application is being manually processed and accepted, NUI user ID and Time stamps logs are stored)	Based on the Train-the-Trainer approach, Eu-LISA shall provide all relevant information/training to raise the awareness of the Member States about the data relating to NUIs users stored in the CS.	ETIAS Program manager/Product owner seconded by Capability Building Sector/ relevant sectors * *(Depending to the level of technical information needed by MS authorities)	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 8 : Inadequate and incomplete information to the data subject on the processing activity, due to the fact that data subject is not aware about the transfer of his personal data to Ms competent authorities.	Eu-LISA shall ensure that the design of the "software for the purpose of manual processing of applications and for accessing and amending data for the purposes of appeals", is implemented by including a disclaimer informing	ETIAS Program manager/Product owner seconded by Architecture	By the end of the "Analysis & Design" work	to be initiated once DPIA is approved

⁶⁹ These logs shall be stored in ETIAS storage location for a period of two years

	travellers that their data could be manually processed by competent authorities of one or more Member States. This will help to ensure the exercise of the right of appeal. (Article 4(1) of the IA 8 is an open list of specific functionalities)		package	
Risk 9: In the framework of the manual processing, during the hit verification process (article 4(g) of IA 8 Access, Amend, Erase), National Units could export TCN's personal data. Possible lack of expert knowledge about data protection of the extracted personal data at the NUs level could have a negative impact on TCN fundamental rights (unlawful disclosure; processing beyond the purpose/without consent)	Eu-LISA shall share the outcomes of this assessment with Member States in order to raise awareness for them to elaborate mitigation measure at their level (e.g. authorized staff training)	Member States	By the entry into operations of the system	to be initiated once DPIA is approved
Risk 10: Technical information related to the processing activity (Timestamp; IP address; Device information; Status of response) could be registered, modified or cancelled without the consent of the application requestor	Eu-LISA shall ensure the design of a technical solution to fairly obtain the consent of data subject to the storage of logs of his/her authentication (Timestamp; IP address; Device information; Status of response) in the Central System. Eu-LISA shall also ensure the integrity of those log files.	ETIAS Program manager/Product owner seconded by Architecture And Security	By the entry into operations of the system	to be initiated once DPIA is approved
Risk 11: In the framework of the manual processing, usage of free text additional information given by the applicant can induce semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights (article 27 of the Regulation; article 2 (3) (d) and (4), article 3, (3) and (4); article 4, (3); article 6 of the DA 7).	Eu-LISA shall ensure the development of all technical solutions to enable quality compliance of data entered by applicant or third party, in the free text space and limit as much as possible the use of free text as foreseen by legal basis (IA 1 Annex).	ETIAS Program manager/Product owner seconded by Architecture	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 12: In the framework of the access, amend, erase request by the applicant, the usage of free text can induce semantic errors. Quality criteria can be not sufficient and produce negative impacts on TCNs fundamental rights				

(article 64 of the Regulation; article 4 (3) (b) of IA 13).				
Risk 13: The free text space and supporting documents of the reporting of abuse may contain personal data. This could affect the traveller's fundamental right to the protection of personal data, exposing the data subjects to processing their data beyond the purpose and without fairness	Eu-LISA shall implement of all legal requirements, notably from AI 1 and his ANNEX, by ensuring that the applicant is informed prior to submission that no personal data should be included in the report and where personal data are nonetheless provided consents that the data will be redacted.	<i>ETIAS Program manager/Product owner seconded by Architecture & Business Relations Management</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 14: Lack of clear and sufficient legal basis for data storage limitation. During the TCN request concerning the abuse from commercial intermediaries, personal data (free text request and supporting documents) are stored in the CS, but the retention period is not clearly defined.	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the data retention period in Central System of personal data related to the abuse reports, notably free text and supporting documents has the same duration as that foreseen for the personal data related to the application.	<i>ETIAS Program manager/Product owner seconded by Architecture</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 15: In the framework of the request coming from TCN to amend/erase her/his personal data, there is a lack of clear and sufficient legal basis (or architecture information) concerning the storage location and retention period of these requests.	Eu-LISA, in accordance with the ETIAS retention policy, shall define whether the storage location and the data retention period of applicant request concerning the access, rectification, completion, erasure of personal data, consent and abuse, are the same as those foreseen for the data related to the application.	<i>ETIAS Program manager/Product owner seconded by Security & Architecture</i>	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 16 : Not appropriate use of the impact assessment tool by National competent authorities could lead to discrimination (generic research made in not-exact mode).	Eu-LISA shall deliver the training to MS competent authorities following the Train-The-Trainer approach on how the impact assessment tool will support Watchlist management.	<i>ETIAS Program manager/Product owner seconded Capability Building Sector/other relevant sectors* Member States</i> <i>*(Depending to the level of needed technical information)</i>	Before entry into operations of the system	to be initiated once DPIA is approved
Risk 17: At the time of drafting this DPIA the encryption protocol for "securing data in	Eu-LISA shall ensure the design and the implementation of a secure encryption mechanism following best practices and	<i>ETIAS Program manager/Product owner seconded</i>	By the end of the "Analysis	to be initiated once DPIA

transit and at rest" is not defined yet. Resulting a possible unauthorized access to personal data.	requirement from legal basis to enable the integrity and the confidentiality of the data.	by Security & Architecture	& Design" work package	is approved
Risk 18 : Technical deficiencies in the control of accesses through the carrier interfaces could allow unauthorized access to personal information	Eu-LISA shall include the carrier interface in the scope of the Security Risk assessment and identify the appropriate measures which will ensure the confidentiality, integrity and availability of carrier interface and personal data that will be managed.	ETIAS Program manager/Product owner seconded by Architecture & Security	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 19: At the time of drafting this DPIA there is a lack of information concerning the technical or organizational process that could undermine the information integrity during the extraction data from the ETIAS DB to the Read-Only DB	Eu-LISA shall adopt all technical measures to ensure the integrity and the confidentiality of personal data in the extraction to the RO DB	ETIAS Program manager/Product owner seconded by Security & Architecture	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 20 : Following article 49, (2), immigration authorities querying EES could access additional categories of data by querying ETIAS central system. This information's go beyond the categories of data to be collected under the purpose of EES (details on family members and minors), Article 49, (3).	Before giving an access to the information relating to the traveller's parental authority or legal guardian information ETIAS should validate that a prior search has been conducted in the EES under Article 26 of Regulation (EU) 2017/2226 and the search result indicates that the EES does not contain an entry record corresponding to the presence of the third country national on the territory of Member States.	ETIAS Program manager/Product owner seconded by Architecture	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved
Risk 21 : TCN Personal Data will be compared with specific risk indicators defined by the ETIAS Central Unit and ETIAS Screening Board art (7) & art(9), ETIAS Central Unit. Wrong technical implementation, testing or maintenance of the risks indicator (as per art (74)) could lead to discrimination and profiling of the data subjects.	Eu-LISA shall adopt secure development standard during the development, testing and maintenance phases to guarantee that the risk indicators will be correctly developed and tested, as defined in article 7(c) article 33 and article 74 (1).	ETIAS Program manager/Product owner seconded by Architecture; Test and transition Unit & Security	By the end of the "Analysis & Design" work package	to be initiated once DPIA is approved

Table 52 Action plan

[The DPIA should be treated as a 'live document' and revisited:

- As the project progresses
- If the organisational or societal context for the project changes significantly
- If the aims of the project change during the project lifecycle.

If the changes to the project create new data protection implications:

- The threshold assessment may need to be revisited to ensure that the PIA is still appropriate.
- A new DPIA may need to be undertaken if the changes are substantial and result in significant data protection risks that were not considered in the original DPIA.]

12. ANNEXES

12.1. eu-LISA DPO Comments

[12/February/2021]

The content of this DPIA includes a systematic description of the system and the purpose of the processing, assessment of the necessity and proportionality in relation to the purpose, assessment of risks to the rights and freedoms of data subjects, and measures to address the risks. These are the specific elements that a DPIA shall at least contain according to article 39 of Regulation (EU) 2018/1725.

The Data Protection Officer (DPO) of eu-LISA has been engaged at different stages of the development of this DPIA. The DPO's views and advice has been provided along meetings and within specific comments over the initial drafts. The DPO provided to the team in charge of carrying out this DPIA references to relevant documentation and guidelines such as those from EDPS⁷⁰ or WP29 Guidelines on Data Protection Impact Assessment (DPIA)⁷¹.

This section provides her general opinion and recommendations for the consideration of the Agency and its stakeholders. At best, clarifications and references on how these views and recommendations have been taken into account shall be included in the relevant part of this DPIA, and when they were not considered, the reasons for that.

- **Reasons for this DPIA:** Having regards to Regulation (EU) 2018/1240, the role of eu-LISA in relation to the processing of personal data in ETIAS Information System is, on one hand, data controller in relation to information security management of the ETIAS Central System and, on the other hand, data processor in relation to the processing of personal data in the ETIAS Information System. Under the

⁷⁰ [Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies \(EUIs\).](#)

⁷¹ [Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.](#)

[REDACTED]

latter role, its responsibilities include the technical development of the ETIAS Information System, for establishing interoperability between the ETIAS Central System and other EU information systems, and for enabling querying of Interpol databases. Moreover, eu-LISA shall define the design of the physical architecture of the system and ensure its technical management. eu-LISA shall follow the principles of privacy by design and by default during the entire lifecycle of the development of ETIAS.

Having this into consideration, and that ETIAS processes personal data of highly sensitive nature at large-scale and counts as an exclusion database, eu-LISA considered and decided to carry out this DPIA. This is without prejudice of other ETIAS data controllers' obligation to carry out its own DPIA that can be informed by the DPIA prepared by eu-LISA, if appropriate.

This DPIA also serves as a tool to embed privacy by design and other appropriate information security measures into the specifications, design and build of the system and procedures. This important fact, which accounts for the responsibilities given to eu-LISA in regards to ETIAS, may want to be highlighted in the list of reasons to conduct this DPIA which, at the moment of providing this opinion, is not.

On the other hand, eu-LISA has completed a threshold assessment. However, since eu-LISA has already identified that the data processing in ETIAS poses a high risk for individuals due to the large-scale processing of personal data of highly sensitive nature and to the criterion of exclusion database, in the light of article 3(5) and Annex 2 of the Decision of the EDPS of 16 July 2019⁷², this threshold assessment does not seem to deem necessary.

- **Roles and responsibilities:** Although roles in regards to data protection have been identified for each party, it is highly recommended that this part is reviewed in depth. At the moment of providing this opinion, ETIAS National Units are considered not only joint controllers of ETIAS but also data processors. Europol has been identified as a data processor, internal to eu-LISA while, on the other side, it has been included in the list of joint controllers of ETIAS. The DPO does not share this analysis. The DPO has provided extensive explanations and clarifications on the roles during the regular meetings organised to discuss the ETIAS DPIA which do not seem to be fully addressed. Therefore, the DPO attaches her own analysis to this opinion and asks for this section to be revisited in the light of these inputs.

Moreover, eu-LISA is involving contractors to support its tasks in regards to ETIAS. It is also recommended that their role and the relationship with key stakeholders of the system is explained.

- **Systematic description of the system (processes in which personal data might be used):** The first step to compliance is to provide a clear description of the processing by understanding and mapping out all data flows in ETIAS.

It is important to describe the processing in a way that is accessible to those who are consulted. In that sense, describing the processing activity of a complex system such as ETIAS can be difficult. Therefore, it might be appropriate to opt for a simpler DPIA report that reflects the main findings and that would include a more high-level description of the processing while referring to detailed information included as annex.

Efforts have been made to facilitate the assessment by separating the entire data processing in different data flows mainly based on purposes and by including a brief description of the different steps. However, a systematic description of each of them has not been conducted and therefore key elements, such as which personal data is processed, from whom, for how long, by whom is accessed and under which conditions, have been overlooked. Subsequently, the DPO advises to revisit the systematic description and attaches a sample of the expected assessment to clarify and support the team in charge of conducting this DPIA (2021-02 ETIAS DPIA_DRAFT_v3 – Sample.xls).

⁷² [Decision of the EDPS of 16 July 2019 on the DPIA lists issued under articles 39\(4\) and \(5\) of Regulation \(EU\) 2018/1725](#)

[REDACTED]

Having a clear understanding of ETIAS design and envisaged implementation will be very valuable to identify known and new risks for the data subjects' rights and freedoms. Understanding which operations are carried out over the personal data is key to identify the potential risks.

- **Necessity:** To elaborate on the necessity of ETIAS, a brief explanation should be provided on why eu-LISA needs to carry out this processing operation, and the question '*How and why is the proposed processing operation an effective means for the Agency to fulfil the mandate assigned to it?*' needs to be answered in an effective way. Considering that eu-LISA is responsible for developing ETIAS and ensuring its technical management and also data controller for the security of the ETIAS Information System, it is advisable to focus on including the reasons and means why the proposed design of ETIAS is adequate for eu-LISA to achieve its mandate.
- **Proportionality:** When assessing the proportionality, the interests of the eu-LISA and its stakeholders need to be weighted up against the rights and freedoms of individuals. Although the derogation in Article 39(10) of the Regulation does not apply, since there was no general impact assessment preceding the adoption of the ETIAS Regulation, it is not for eu-LISA – neither as data controller of the security of ETIAS Information System nor as data processor responsible for the design, implementation and operational management of the system - to weight the proportionality of adopting ETIAS but to assess how eu-LISA limits itself to what is necessary within the Information System for the aim of the processing. Remaining within these limits will result into benefits for the data subjects. Several of these benefits have been presented in this section of the DPIA. However, it is also recommended to include a brief description on how eu-LISA limits itself to what is necessary for the aim of the processing.
- **Risk identification:** undertaking a general revision of the identified risks is highly advised. If the team in charge of performing this DPIA follows the above-mentioned recommendation related to the systematic description of the data processing, additional data subjects and new categories of personal data of highly sensitive nature will be identified. This might imply new risks for the rights and freedoms of the data subjects that were not considered yet and that, subsequently, will trigger the need to revisit the risk analysis.
- **Initial scoring of risks and description of the system:** eu-LISA has applicable security policies which include the security measures that, by default, need to be applied to the large-scale systems it operates. These measures constitute an information security baseline.

On the other hand, the applicable legal framework of ETIAS includes requirements that also constitute a security and data protection – by design - baseline for this service. Additionally, there could be, for instance, contracts in place with the contractors and well-defined procedures such as those for handling data breaches.

Therefore, considering all the existing elements, it is recommended that the baseline both for security and data protection are identified and presented in the systematic description of the system as it has a direct impact on the initial scoring of the risks.

- **Assessment of risks:** general comments have been provided along this opinion, and specific ones have been provided in the meetings and revisions of the document.
- **Measures envisaged to address the risks:** undertaking a general revision of the identified measures is highly advised. In particular, in the light of a more comprehensive description of the data processing operations and identification of additional data subjects and categories of personal data of high sensitive nature. This exercise will result in new risks for the rights and freedoms of the data subjects that most likely have not yet been considered and new measures might be deemed necessary.

- **Consultations to other parties:** Details on which other parties were consulted directly or indirectly by eu-LISA on the design of ETIAS at this stage should be documented including details on the consultation, how their inputs were taken into account and the modalities of the consultations (surveys, experts groups, advisory groups, industry representatives, ...)
- **Conclusions and sign-off:** After identifying measures to address the risks and documenting the residual level of the risk posed by the processing, an action plan should be developed. At the time of providing this opinion, this action plan is missing. Therefore, the team in charge of carrying out this DPIA is encouraged to elaborate this action plan including relevant owners of these actions.

At the same time, the team is encouraged to make efforts in identifying the relevant actors for the sign-off process. The ETIAS business owner of eu-LISA should take part not only in the development of this DPIA but also in its validation process. Security of personal data is an important element of this data processing operation and a direct responsibility of eu-LISA as data controller for the security of the ETIAS Information System. Therefore, the Security Officer of eu-LISA shall be engaged in the sign-off process, likewise, the Head of the Operations Department of eu-LISA - as ETIAS will be implemented by this Department -. The Executive Director of eu-LISA should be part of the final validation of this DPIA.

12.2. Addressing DPO Comments

1. **Reasons for this DPIA:** DPO comments have been fully implemented by rephrasing text in chapter 2. In an addition, a specific mention that “DPIA also serves as a tool to embed privacy by design and other appropriate information security measures into the specifications, design and build of the system and procedures”, was added (chapter 2, page 17, line 7) even though the same concept is expressed in the paragraph 2.2..
2. **Roles and responsibilities:** In the final version of this report eu-LISA DPO position was taken in account and EUROPOL was included as data recipient and a third party providing data to ETIAS processing activities.
3. **Systematic description of the system:** The DPIA team started working on the new excel template immediately after receiving it from DPO. Information related to data subjects, personal data, roles, retention periods, legal bases, supporting assets were gathered, and one Dataflow (“TCN save draft”) was completed as test. This enabled the positive and negative points of the proposal to be appreciated. Indeed, the excel file allows a more in-depth analysis of each step of processing activities, more than 24 sub-dataflows (coming from the breaking down of existing dataflow already described in the present report) are identified. However, most of the information detailed in the excel file was already present in the word file. In addition, this new exercise needs a relevant amount of time to be performed. Nevertheless, it would be done in the next version of ETIAS DPIA (v. 2.0).
4. **Necessity:** eu-LISA DPO comments were implemented in chapter 6.1. The answer to the question *‘How and why is the proposed processing operation an effective means for the Agency to fulfil the mandate assigned to it?’* was redrafted in an effective way, as requested by DPO, considering the fact that eu-LISA is responsible for developing ETIAS and ensuring its technical management and also data controller for the security of the ETIAS Information System.
5. **Proportionality:** The assessment was also implemented with a further element requested by DPO, the answer to the question: how eu-LISA limited itself in the ETIAS processing activity? The answer to this question is in line with the position expressed by the European Parliament substitute impact assessment⁷³,

⁷³ European Parliament, The European Commission package of ETIAS consequential amendments Substitute impact assessment, December 2019, p.34 key finding 10.

[REDACTED]

according to which keeping all logs will participate to ensure the compliance of safeguards required by EU-DPR (chapter 6.2).

6. **Risk identification/ Assessment of risks / Measures envisaged to address the risks:** All risks were redrafted, to achieve a more precise description following DPO and project management advice. The initial work on the excel template highlighted that, this supporting tool could lead to the identification of new risks that, at the moment, are negligible, limited and medium. Nevertheless, the further granularity of the Excel file does not show, at the moment - with only 5% of the workflows reassessed -, that new High Risks could be raised.
7. **Initial scoring of risks and description of the system:** In the view of the fact that the Security Risk assessment for ETIAS is an ongoing parallel exercise that was not finalized by the time of closing this DPIA, security policies and security measures were analysed in the present report at high level. This part will be further elaborated in a next version of the DPIA.
8. **Consultations with other parties:** a specific paragraph (4.5.2) was added to this report to complete the external context information with the description of the inputs coming from the consultations between eu-LISA and other stakeholders.
9. **Conclusions and sign-off:** An action plan was added to the present report, to facilitate the implementation of proposed mitigation measures aimed at ensuring data protection in subsequent design phases.

12.3. Knowledge base for the description of supporting assets

Typology of supporting assets		
Information systems	Hardware and electronic data media	Example: Computers, communication relays, USB drives, hard drives
	Software	Example: Operating systems, messaging, databases, business application
	Computer channels	Example: Computer channels: Cables, WiFi, fiber optic
Organisations	People	Example: Users, IT administrators, policymakers
Hardware	Paper documents	Example: Print, photocopies, handwritten documents
Hardware	Paper transmission channels	Example: Mail, workflow

Table 53 Knowledge base for the description of supporting assets

12.4. Knowledge base for likelihood and impact ratings

1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
Rating likelihood			
It does not seem possible that the data protection principle (fairness, transparency, etc.) could be affected.	It seems difficult that the data protection principle (fairness, transparency, etc.) could be affected.	It seems possible for the data protection principle (fairness, transparency, etc.) to be affected.	It seems extremely likely that the data protection principle (fairness, transparency, etc.) would be affected.
Rating impact			
Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties.	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome.

1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
Examples			
Physical impacts: classical negligible physical impacts include lack of adequate care for a dependent person (minor, person under guardianships), transient headaches...	Physical impacts: minor illness, lack of care leading to a Minor but real harm, Defamation resulting in physical or psychological retaliation	Physical impacts: Serious physical ailments causing long-term harm, Alteration of physical integrity (following an assault, an accident at home, work, etc.)	Physical impacts: Long-term or permanent physical ailments (e.g. due to disregard of contraindications), Death, Permanent impairment of physical integrity
Material impacts: - Loss of time in repeating formalities or waiting for them to be fulfilled - Receipt of unsolicited mail (e.g. spams) - Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) - Targeted advertising for common consumer products	Material impacts: - Unanticipated payments (e.g. fines imposed erroneously), - Denial of access to services, blocked account - Lost opportunities of comfort (i.e. cancellation of leisure, termination of an online account) - Missed career promotion - Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects - Cost rise (e.g. increased insurance prices) - Non-updated data (e.g. position held previously) - Processing of incorrect data creating malfunctions - Targeted online advertising on a private aspect that the individual wanted to keep confidential - Inaccurate or inappropriate profiling	Material impacts: - Non-temporary financial difficulties (e.g. obligation to take a loan) - Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) - Prohibition on the holding of bank accounts - Damage to property - Loss of housing, Loss of employment - Separation or divorce - Financial loss as a result of a fraud (e.g. after an attempted phishing), Misappropriation of money not compensated - Blocked abroad	Material impacts: - Financial risk - Substantial debts - Inability to work - Inability to relocate - Loss of evidence in the context of litigation - Loss of access to vital infrastructure (water, electricity)".



1 : Negligible	2 : Limited	3 : Significant	4 : Maximum
Moral impacts: - annoyance caused by information received/requested - Fear of losing control over one's data - Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) - Lack of respect for the freedom of online movement due to the denial of access to a commercial site	Moral impacts: - Refusal to continue using information systems - Minor but objective psychological ailments (defamation, reputation) - Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation) - Feeling of invasion of privacy without irreversible damage - Intimidation on social networks	Moral impacts: - Serious psychological ailments (depression, phobia) - Feeling of invasion of privacy with irreversible damage - Feeling of vulnerability after a summons to court - Feeling of violation of fundamental rights - Victim of blackmailing - Cyberbullying	Moral impacts: - Long-term or permanent psychological ailments - Criminal penalty - Abduction - Loss of family ties - Inability to sue - Change of administrative status and/or loss of legal autonomy (guardianship)

Table 54 Knowledge base for likelihood and impact ratings



12.5. Identification of the risks

[Go through your data flow diagram and for each step, ask yourself how this could affect the persons concerned against the background of the data protection principles. Map dataflow diagram items and protection targets.]

	Fairness	Transparency	Purpose limitation	Data minimisation	Accuracy	Storage limitation	Security
Collection	X	X	X	X	X		X
Merging datasets	X	X	X	X	X		X
Organisation/structuring			X	X	X		
Retrieval/consultation/use	X	X	X		X	X	X
Editing/alteration		X		X	X		X
Disclosure/Transfer	X	X	X	X	X		X
Restriction			X	X	X	X	X
Storage	X	X	X			X	X
Erasure/destruction			X			X	X

Table 55 Identification of the risks

12.7. Knowledge base for possible risks and mitigation measures

[The section includes examples of risks and possible measures to address them. However, this is not intended to be an exhaustive list. Therefore, it should be understood that there are risks that affect the processing of personal data, which are not listed in this catalogue as well as measures other than those proposed below.]

12.7.1. General	
Risk	Measures
Economic losses and reputational damages arising from breach of the legislation on protection of personal data	Training on data protection. Clear communication on staff responsibilities in relation to compliance with privacy policies of the organization as well as the sanctions associated with non-compliance.
Economic losses and reputational damages arising from the breach of sector laws with impact on data protection to which the controller may be subject	Training on data protection on the specifics of particular department. Clear communication on staff responsibilities in relation to compliance with the organization's privacy policies related to the sector laws that affect the organization, as well as the sanctions associated with the breach.
Economic losses, loss of customers and reputational damage deriving from the lack of adequate security measures or from its inefficiency, in particular, in case of loss of personal information	Appropriate staff training on security and proper use of ICT. Clear communication on staff responsibilities in relation to compliance with policies and measures of security as well as the sanctions associated with non-compliance.
Loss of stakeholders' trust in eu-LISA services derived from the reputational damage caused by a deficient management of people's privacy	Appropriate staff training on data protection, security and proper use of ICT.
Lack of expert knowledge about data protection	Appoint a person or department responsible for the dialogue with the data subjects in everything related to the privacy and protection of personal data, and clearly communicate how to contact him/her.

12.7.1. General

and channels of communication with the data subjects	Appoint a Data Protection Officer (DPO) to deal with all issues related to privacy within the organization and advice.
Late incorporation of experts in data protection (in particular, DPO) to the project or insufficient definition of their functions and competences	Include DPO in the project from the initial phases. Establish functions of the DPO and his/her involvement in the projects.

12.7.2. Legitimacy of the processing and transfer of personal data

Risk	Measures
Processing personal data when it is not necessary for the purpose	Use dissociated data whenever possible and do not use data unreasonably.
	Allow anonymous use of services and products when it is not necessary to identify people.
	Use pseudonyms or attribute codes to replace the identity data. Even if pseudonymised data is not absolutely unlinked, it can contribute to ensure that the information about the identity of affected data subjects is only accessible to a reduced number of people.
	Avoid using biometric data except when it is necessary or absolutely justified.
The lack of clear and sufficient legal basis for the processing or purpose of personal data	Proper staff training on data protection, security and use of ICT.
	Review the data protection legislation to identify the basis and purpose of processing of personal data and ensure that it is in compliance with legislation.
	If necessary, seek DPO advice.
	If personal data is transferred, conclude written agreements, establishing the conditions, under which the transfer occurs and, where appropriate, as well as the possibilities of supervision and control of compliance with the agreement.



12.7.2. Legitimacy of the processing and transfer of personal data	
Obtaining doubtful or invalid consent for processing or transfer of personal data	Ensure that there is no other more suitable legal basis for the processing.
	When the data processing is legitimized by a contractual relationship, always offer the possibility of separate consent to process data for purposes that are not necessary for its compliance or improvement thereof, avoiding including them indissolubly in the clauses of the contract.
	Avoid making the use of a product or service conditional on consent for different purposes.
	In the workplace, avoid basing data processing on the consent of staff.
	Avoid forcing consent from a position of prevalence of the person in charge.
Establishing difficult withdrawal of consent or objection concerning processing or transfer.	Establish clear procedures for the withdrawal of consent or objection concerning particular processing.
	Establish the necessary mechanisms to ensure that the data subject's rights to withdraw consent or object processing or transfer is easily exercised.
Difficulties to guarantee the legitimacy of data processing and transfer from third parties	Require guarantees that personal data from the third parties was obtained in compliance with law.
	In case of advertising campaigns by the third parties, demand the proof from the third party that the people whose data will be used have given their consent for it.
Request and process special categories of data without necessity or without adopting the necessary safeguards	Verify that the processing of special categories of data is necessary for the purpose or goal pursued.
	Check if the processing is allowed or required by law.
	Otherwise, establish procedures which guarantee the obtaining of expressed consent (in writing when necessary) and which allow you to prove that you have it.



12.7.2. Legitimacy of the processing and transfer of personal data

Complementing personal data in an unforeseen manner which is unforeseen in the initial purposes and without adequate information to the data subjects when interconnecting with other databases of the organization or from third parties, in particular, the re-identification of dissociated information

Verify the legitimacy of the foreseen data interconnection.

Clearly define the personal data resulting from the processing and verify that after operation they still are the only personal data that were generated.

Use tracking cookies or others tracking mechanisms without getting a valid consent after providing adequate information

Avoid the use of cookies or other tracking and monitoring mechanisms. In case if they are used, prefer the less invasive (own cookies over cookies of third parties, session cookies versus permanent cookies, short expiration periods of cookies, etc.)

Inform with transparency about the use and purposes of cookies. In particular, this information may be offered through a layer system.

Respect the preferences established by the data subjects in their browsers on the tracking your navigation.

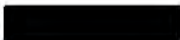
12.7.3. International Transfers

Risk	Measures
Secret access to personal data by the authorities of third countries	Include safeguard clauses concerning information about access to personal data transferred to third countries' authorities as soon as possible
Lack of compliance controls of the transfer safeguards	If there are international transfers to countries outside the European Economic Area, implement control procedures necessary (including contractual ones) to ensure conditions are met under which the transfer took place. In this regard, we must pay special attention when contracting cloud computing services or hosting in third countries.
Obstacles by the data importer for the exercise of supervision and agreed control procedures	Ensure the enforceability of control mechanisms such as lists of processors, countries where they operate, possibility to review documentation and perform audits, etc.
Inability to help citizens to exercise their rights before the transfer	Ensure the functioning of communication channel between importer and exporter to accommodate the data subjects' requests. Implement procedures to ensure the accommodation of the data subjects' requests.
Failure to obtain authorizations according to legal requirements	Request authorisation by the EDPS, in necessary cases.



12.7.4. Records and Register of the Processing Activities

Risk	Measures
Lack of the necessary mechanisms and procedures to detect when the processing activity must be registered, modified or cancelled	Include in the processes and methodologies of development of new projects a phase or task concerning the review of the need for normative compliance.
The lack of necessary mechanisms and procedures detecting when DPIA and consultation the supervisory authority is required	Include in the processes and methodologies of development of new projects a phase or task to check the need to comply with data protection legal requirements.



12.7.5. Transparency of the Processing Activities

Risk	Measures
Collecting personal data without providing proper information or in unauthorized manner (cookies, geographic location, behaviour, browsing habits, etc.)	Establish procedures for review systematic and mandatory personal data collection forms to guarantee compliance with the data protection policies, the homogeneity of the information and the sufficient information to the data subject.
Information on the protection published in the web environment (privacy policies, information clauses) are difficult to locate or disseminated in various sections, which makes access complicated	Structure and provide the information about the processing of personal data on several levels, which is easily accessible to the data subjects. Consider using of icons or other graphics to facilitate understanding of information.
	Verify that the information provided in all places is consistent and systematic.
	Verify that the information is provided in all forms.
Information for the data subject is written unclearly, which prevents the data subject from understanding how the his/her data is processed	Implement clear privacy policies, concise and easily accessible to the data subjects, in standardized forms, and with uniformity in all environments of the organization.

12.7.6. Quality of data

Risk	Measures
Collecting the data or data categories, which are unnecessary for the purposes of processing (new system, product or service)	Thoroughly review information flows to detect whether the personal data requested is necessary for the processing.
Existence of technical or organizational errors that lead to the lack of information integrity, allowing the existence of duplicate records with different information or contradictory, which may derive in making wrong decisions	Establish technical and organizational measures, which ensure that updates of the data subject's data is communicated to all the information systems and departments of the organization, which are authorized to use it.
Insufficient guarantees concerning the use of personal data for historical, statistical or scientific purposes	Use anonymous or disassociated personal data, when possible. Use pseudonyms or attribute codes for identifying data. Therefore, even if it is not leading to the absolute dissociation of data, the identity of the data subject would be accessible to a reduced number of people. Ensure that the adequate security measures corresponding to security level to of data are used
<i>Personal data usage for purposes not specified or incompatible with the following: movements or location</i>	Provide clear and transparent information about the purpose for which it is processed; in particular, Privacy Policy should be visible and easily accessible. Provide information on the criteria used in decision-making and allow the data subject to challenge the decision. Provide information on the measures that have been implemented to achieve the necessary balance between legitimate interest of the controller and the fundamental rights of the data subjects.



12.7.6. Quality of data

to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; decisions relevant to the people (particularly those belonging to vulnerable groups), especially if they can be discriminatory, including differences in prices and costs of services and products or obstacles to border crossing

Automated decision making with possible relevant consequences for persons
Use of metadata for undeclared or incompatible

Establish mechanisms and procedures, which enable to solve the errors in a quick and efficient way

Establish possibilities for challenge agile to offer adequate remedies to the data subject.

Establish alternative channels to try with false negatives and false positives in people identification and authentication through biometric data.

12.7.6. Quality of data

purposes with the declared ones.

Make inferences or erroneous deductions lines (and, where appropriate, harmful) on specific people through the use of artificial intelligence techniques (in particular, data mining), facial recognition or biometric analysis of any kind

Lack of clear procedures and of suitable tools for guaranteeing ex officio cancellation of personal data once have ceased to be necessary for the purpose or purposes for which they were picked up

Clearly define the cancellation deadlines for all personal data of the information systems

Set automatic controls within the information systems to notify of the proximity of the cancellation deadlines of the information.

Implement mechanisms to carry out and manage said cancellation at the time adequate including, if applicable, the temporary blocking of personal data.



12.7.7. Special categories of data	
Risk	Measures
Systematic or occasional failures or errors to obtain expressed consent, when this is the legal base for your processing	Avoid using special categories of data unless it is absolutely necessary
	Establish procedures that guarantee obtaining expressed consent (and in writing when necessary) to allow you to prove that you obtained it
Wrong assumption of the existence of a legal authorization for the processing or transfer of special category data	Appoint a DPO for a qualified advice
Poor or reversible dissociation that allows the re-identification of special category data in research processes that only plan to use anonymous data	Use dissociation techniques that guarantee the real anonymity of the information or, at less, that the residual risk of re-identification is minimal



12.7.8. Confidentiality obligation	
Risk	Measures
Unauthorized access to personal data	Establish mechanisms and procedures for awareness about the obligation to keep secret about personal data that are known in the exercise of professional functions.
	Establish disciplinary sanctions for those who breach the duty of secrecy and confidentiality policies of the organization
	Establish procedures guaranteeing that employees, who access personal data are formally informed about the obligation not to disclose personal data they process when exercising their functions and the consequences of the data breach
	Inform that the competent authorities will be notified of any confidentiality breach that could imply liability.
	Establish procedures to ensure the destruction of disposed media containing personal data
Violations of the confidentiality of personal data by organization employees	Proper employee training on obligations and responsibilities regarding the confidentiality of the information
	Establishment of dissuasive sanctions for employees who violate the confidentiality of personal data as well as clear and complete communication thereof.

12.7.9. Data Processor

Risk	Measures
Non-existence of contract or preparation of an incorrect contract that does not reflect all the necessary data protection clauses and adequate guarantees	Establish procedures, which guarantee that whenever a manager is processing the data, the corresponding clauses are included into the contract in accordance with the data protection legislation
Lack of diligence (or difficulty in demonstrate it) in the choice of processing manager	Select data processors who provide sufficient guarantees of compliance with the contracts and the adoption of security measures stipulated through, by example, of his adhesion to possible codes of conduct or to certified and certified solvency certification schemes Contractually establish mechanisms of supervision, verification and audit of treatments ordered from third parties.
Poor management of outsourcing and insufficient control over managers and subcontractors and, in particular difficulties in verifying or supervising that the person in charge and subcontractors meet the instructions and especially the security measures	Establish mechanisms and procedures, which guarantee control over the activities of the subcontractors Perform periodic audits of the person in charge of processing to ensure that it meets the requirements set in contract Define service level agreements and adopt instructions on the appropriate security measures

12.7.9. Data Processor

No definition or deficiencies in procedures to communicate to responsible person for exercising the rights of the data subjects	Include in the custom contract the obligation to communicate the data subjects on exercising their rights
	Define the procedures on effective communication
Difficulties to achieve the portability of personal data to other environments	Include the portability obligation in the contract and service level agreements
	Establish technical and organizational measures that guarantee portability.

12.7.10. Rights of the data subjects

Risk	Measures
Difficult or impossible to exercise of the rights of the data subjects	Implement systems that allow the data subjects to access their data easily, directly and securely, as well as easily exercise their rights
	Avoid systems of exercise of rights of the data subjects that involve requesting a remuneration
	Avoid establishing procedures, which are complex and laborious
	Train the entire staff to know what to do if you receive data subjects' request or must inform the data subject on how to exercise their rights



12.7.10.Rights of the data subjects	
	Define which people or departments will be responsible for managing the rights of the data subjects and train them properly
Lack of procedures and tools for managing stakeholder rights	Define management procedures and implementation tools, which ensure that all employees know how to act when receiving data subject's request and what information should be supplied in this case.
	Training of the employees in charge of dealing with the data subjects' in supporting them to exercise their rights
	Lack of procedures and tools for informing on rectifications, cancellations or oppositions to assignees of personal information

12.7.11.Security	
Risk	Measures
Lack of security measures or poor application. Definition of security and competence setting	Appointment of a person responsible for security and establishment by the direction of their functions, competencies and attributions in the development and management of projects
	Include within the procedures of design and development of new products and services the incorporation of the person in charge of security in the initial phases of same
Organizational deficiencies in access control management	Strict access to information policies for the need to know for granting access to the information and clean documentation desks (clean desks) to minimize possibilities of unauthorized access to personal information
	Establish procedures, which guarantee revocation of permissions to access personal data when they are no longer necessary (abandonment of the organization, transfer, change of functions, etc.)

12.7.11.Security

	Inventory the resources they contain personal data accessible through networks of telecommunications
Technical deficiencies in the control of accesses that allow people unauthorized access and subtract personal information	Install hardware or software tools that help efficient management of the security and commitments or obligations legal aspects of the organization in the area of personal data protection If necessary, install detection tools for intrusions (IDS or Intrusion Detection Systems) and / or intrusion prevention (IPS or Intrusion Prevention Systems) with the necessary information to workers about their installation, features and implications for your privacy To the extent that may be necessary, implement Data Loss Prevention (DLP or Data Loss Prevention) systems with the necessary information to the workers about their installation, characteristics and implications for your privacy
Inability to attribute to users identified all the actions that are carried out in a system of information. Establish registration mechanisms for actions on personal data or logging as well as flexible and flexible tools of exploitation of audit firms resulting	Establish registration mechanisms for actions on personal data or logging as well as flexible and flexible tools of exploitation of audit firms resulting.
Use of identifiers that reveal information on the data subject	Establish policies for assigning user codes by the organization that avoid trivial data such as date of birth, name and surname, etc. Avoid the use of identifiers linked to authentication items, such as numbers of credit cards or similar, favour fraud in identification and even phishing.