EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON THE ETIAS DPIA (Case 2021-0640)

1. INTRODUCTION

- This Opinion relates to eu-LISA's data protection impact assessment ('DPIA') for the European Travel Information and Authorisation System ('ETIAS').
- The EDPS issues this Opinion in accordance with Articles 57 (1) (g) and 58 (3) (c) of Regulation (EU) 2018/1725[1] ('the Regulation').

2. BACKGROUND

The ETIAS is established by Regulation (EU) 2018/1240[2] ('the ETIAS Regulation'). It will collect and store personal data about visa-exempt travellers to the Schengen States to determine whether these travellers pose security, irregular immigration or epidemic risks.

The ETIAS will consist of a large-scale information system composed by the ETIAS Information System[3] (developed by eu-LISA), the ETIAS Central Unit[4] (established within the European Border and Coast Guard Agency - Frontex) and the ETIAS National Units[5] (established within a competent authority designated in each Member State).[6] The ETIAS Information system is composed of several elements including the ETIAS Central System (which includes the watchlist), National Uniform Interfaces, communication infrastructures, carrier gateway, etc. [7]

[1] Regulation (EU) 2018/1725 of the European Parliament and 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, OJ, L 295, 21.11.2018, pp. 39-98.
[2] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation system (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19.9.2018, p. 1–71.
[3] Article 6 of the ETIAS Regulation.
[4] Article 7 of the ETIAS Regulation.
[5] Article 8 of the ETIAS Regulation.
[6] Article 3 of the ETIAS Regulation.
[7] Article 6 (2) of the ETIAS Regulation.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

The ETIAS Regulation requires eu-LISA to develop the ETIAS Information system and to ensure its technical management.[8] In that regard, eu-LISA is mandated to follow the principles of privacy by design and by default during the entire lifecycle of the development of ETIAS.[9] The EDPS notes that the term 'Privacy by design and by default' designates the broad concept of technological measures for ensuring privacy. In this opinion, the EDPS is using the term Data Protection by Design and by Default ('DPbD') referred to in Article 27 of the Regulation, which requires the controller to implement technical and organisational measures designed to implement data protection principles. [10]

In addition to his role of developer of the system, Articles 57 and 58 of the ETIAS Regulation designate eu-LISA as controller in relation to information security management of the ETIAS Central System and as processor in relation to the processing of personal data in the ETIAS Information system.

Frontex (the European Border and Coast Guard Agency), is considered as controller for the processing of personal data in the ETIAS Central System while the ETIAS National Unit of each Member state is considered as controller in relation to the processing of personal data in the ETIAS Central System by that Member State. [11]

Given the size and complexity of ETIAS, the EDPS organised on 6 December 2019 and 24 March 2020, two meetings at staff level with members from Frontex and from eu-LISA (including their DPOs) as well as from the EU Commission.[12] The goal of these meetings was to obtain a clear understanding of the process in place for the development of the ETIAS, in particular with regard to the drafting of the Data Protection Impact Assessment (DPIA), which is a key tool to correctly implement the principles of data protection by design and by default.

The drafting of the DPIA is an obligation incumbent to the controller of a given data processing activity. In the case of ETIAS, this obligation jointly falls upon Frontex, ETIAS National Units and eu-LISA. As joint controllers of ETIAS, each of them should address not only the data protection risks linked to their own data processing operations within the system but also the ones linked to their interactions with other data protection operations and other systems. These DPIAs cannot thus be performed in isolation from each other.

---

[8] Articles 6 (1) and 73 of the ETIAS Regulation.

[9] Article 73(3) of the ETIAS Regulation.

[10] While measures taken under Article 27 of the Regulation will also contribute to achieving the more general objective of 'privacy by design', the EDPS considers that a wider spectrum of approaches may be taken into account for the objective of 'privacy by design' which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU (EDPS preliminary opinion on Privacy by design (Opinion 5/2018), available at: https://edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf)

[11] Article 57 of the ETIAS Regulation.

[12] Staff Level meetings took place on 6 December 2019 (with Frontex and eu-LISA) and 24 March 2020 (with Frontex, eu-LISA and the EU Commission).

It resulted from these discussions that eu-LISA, in its quality of developer of the system,[13] had taken over the responsibility to coordinate the whole technical development of the system, including the DPIA.[14]

As a result, on 13 May 2020, the EDPS addressed a preliminary guidance to eu-LISA with regard to the ETIAS DPIA[15], supplementing the orientations already provided in his Accountability toolkit. [16]

On 17 June 2021, eu-LISA asked for the EDPS opinion on the DPIA it has performed for ETIAS and indicated that the document sent for consultation is the final DPIA.

3. ANALYSIS OF THE DPIA

3.1. Need for a DPIA in accordance with Article 39 of the Regulation

Under Article 39 of the Regulation, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must - prior to the processing - carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

In accordance with Article 39(4) of the Regulation, the EDPS has established a list of the kinds of processing operations that are subject to the requirement of a data protection impact assessment.[17] Eu-LISA has identified two processing operations from this list (i.e. 'exclusion databases' and 'large-scale processing of special categories of personal data') justifying the need for a DPIA.[18]

The EDPS considers that eu-LISA should further explain the identification of these two processing operations in the context of ETIAS. This explanation step is particularly important as it provides a first analysis of the risks stemming from the use of the system that the DPIA needs to address carefully through the definition of mitigation measures.

---

13 Articles 6 and 73 of the ETIAS Regulation.
14 Staff Level meeting on 24 March 2020 (with Frontex, eu-LISA and the EU Commission).
15 Letter to eu-LISA DPO on 13 May 2020 (DH/GC/vm/ D(2020) 1207 C 2019-0495).
16 The EDPS Accountability toolkit consists of three documents:
- a summary: Guidance on documenting processing operations for EU institutions, bodies and agencies (EUIs)
- Part I: Records, Registers and when to do Data Protection Impact Assessments and,
- Part II: Data protection impact assessments and prior consultation.
These documents are available at https://edps.europa.eu/node/4582_en.
17 Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA lists issued under Articles 39(4) and 39(5) of Regulation (EU) 2018/1725.
18 See Table 4 'legal basis' on page 20-21 of the DPIA.

In this regard, the EDPS points out his non-exhaustive list of criteria for assessing whether processing operations are likely to result in high risks[19] as well as his 'Accountability toolkit'.[20]

As part of the explanation for conducting a DPIA, the EDPS notes that the ETIAS will collect and process a huge volume of personal data (including on criminal offences) about millions of individuals and will crosscheck these data with data stored in several other large scale IT systems including central databases for law enforcement cooperation. These data will be used to support decisions that may adversely affect individuals. In addition, a set of screening rules will be used to profile data subjects and to determine automatically the potentially risky individuals for whom a manual processing of their applications will be required.

The impact might be significant as denial of entry on the Schengen territory based on the data processing in ETIAS may create a series of negative consequences for individuals. These consequences include a restriction on the enjoyment of their freedom of movement, a financial impact if they travel to the EU for business purposes or health issues if they travel to the EU to get a medical treatment they cannot obtain in their own country. Besides, the access to the data stored in the ETIAS by law enforcement authorities may also harm the individuals, who could become the focus of law enforcement attention and be subject to investigative measures.

In light of the above, the EDPS considers that eu-LISA should further explain the identified kinds of processing operations leading to the decision to conduct a DPIA, for example by taking into account the EDPS non-exhaustive list of criteria for assessing whether processing operations are likely to result in high risks.

Thorough identification of high-risk criteria can assist the DPIA team, by providing an overview of high-risk indicators that should be addressed during the assessment phase. This is also a good exercise to train eu-LISA staff and ensure that in the future no criteria will be missed, leading to unjustified decisions on not to conduct a DPIA, while the relevant data processing could have high risk on data subjects' fundamental rights.

The EDPS recommends that eu-LISA further explain the identified kinds of processing operations leading to the decision to conduct a DPIA, taking into account the EDPS non-exhaustive list of criteria for assessing whether processing operations are likely to result in high risks.

[19] Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA lists issued under Articles 39(4) and 39(5) of Regulation (EU) 2018/1725.

[20] In particular, chapter 4 of the Accountability toolkit (Part I) contains criteria to decide when a DPIA is mandatory, as well as a list of risky operations.

3.2. Structure of the DPIA

The EDPS welcomes that the DPIA generally follows the template structure of the DPIA report provided for in the Accountability toolkit.[21] After a detailed analysis of each of the elements of the DPIA to see whether they provide the information required by the Regulation as further developed in the Accountability toolkit, we provide the following recommendations and suggestions for improvement in the sections below.

3.3. Scope of the DPIA

Eu-LISA has provided a description of the scope of the DPIA in the executive summary. More particularly, it mentions that 'this DPIA assesses the data protection risks identified within 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' (p. 8). At the same time, the risk analysis focuses on eu-LISA's responsibilities for the design, development and information security management of ETIAS.

The EDPS understands that given the complexity of the system and the different roles of the involved actors, the received DPIA is not the final version of the ETIAS DPIA. Since eu-LISA is coordinating the implementation of the system and applying the principle of Data Protection by design and by default, eu-LISA is responsible to update this DPIA with the inputs received from Member States and Frontex as regards the risks identified from their respective DPIAs.

The EDPS recommends eu-LISA to draft a comprehensive DPIA that includes the risks identified by all stakeholders (i.e. Frontex, Member States, Europol, eu-LISA) and the ones stemming from the ETIAS development and operation, prior to the system's entry into operation.

3.4. Proactive identification of risks from main actors involved

Given the complexity of the ETIAS, in particular regarding its connections with other systems and the key role of several stakeholders, it is essential to ensure a good coordination between all its stakeholders in order to devise appropriate strategies addressing all the identified risks. In particular, three main actors are involved in the ETIAS: eu-LISA, Frontex (the ETIAS central unit) and the Member States (the ETIAS national units). Also, Europol is an important actor involved in the ETIAS, as it will enter data in the ETIAS watchlist[22] and will be part of the ETIAS Screening Board, advising Frontex on the ETIAS Screening rules.[23]

[21] See Annex III of the toolkit, Part II
[22] Article 34 of the ETIAS Regulation.
[23] Articles 9 and 33 of the ETIAS Regulation.

When developing and designing the ETIAS, eu-LISA has to consider all risks for the data subjects resulting from the use of the system overall. Only once the ETIAS is operational, some parts of the processing will be under the responsibility and controllership of Frontex (the ETIAS central unit) and of Member States (the ETIAS national units).

Frontex and the Member States need to perform their own DPIAs on their processing activities, prior to ETIAS' entry into operation. However, these may introduce some new functional requirements for the ETIAS, as part of mitigation measures. Apart from expecting these at a later stage of the design, eu-LISA should take a supporting pro-active position in identifying such risks and ways in which the system could contribute towards their avoidance or mitigation. The overall analysis of the data flows and the involvement of the other stakeholders in the review of this DPIA is helpful in this direction.

The DPIA indicates that eu-LISA has consulted multiple external stakeholders (including Frontex, Member States' representatives and Europol) and that the outcome of these consultations has been included as inputs in the drafting of the DPIA (subsection 4.5.2). However, the EDPS has not found in the DPIA examples of risks stemming from these data processing activities or related to the interactions of the system with processing operations under the responsibility of the ETIAS central unit, the ETIAS national units or Europol.

Examples of such risks that could be identified in early stages include:

- Delays in the manual processing of the ETIAS application by the ETIAS Central Unit, the ETIAS National Unit or by Europol (as part of the Article 29 consultation) or in the processing of data subjects' access requests.

  Although the ETIAS Regulation has taken into account legal thresholds in which the applications should be processed, there may be cases of urgency when third country's nationals ('TCNs') need to travel in the time interval before the deadline, but due to the manual processing are prevented from travelling. As part of the mitigation for such risks, eu-LISA and the involved stakeholders should consider if and how the system could contribute to minimising them, e.g. by providing reports of pending applications or alerts for applications that are reaching either the deadline or the travel date.

- Errors or delays in the manual processing of the ETIAS application due to non-adequately trained personnel, leading to TCNs' inability to travel.

  As part of the mitigation for such risks, eu-LISA and the involved stakeholders should consider if and how the system could help identify such errors by officers using the system, e.g. by providing statistics on how many applications the user has rejected in comparison to following access requests by the TCN.

- Risks linked to data quality, such as errors in data inserted into the ETIAS watchlist by Member States and/or Europol or in other databases consulted by the ETIAS system (5.5.-automated processing).

  Eu-LISA and the involved stakeholders should consider if and how the system could help identify such errors.

The EDPS recommends including in the DPIA, risks related to the interactions of the system with processing operations under the responsibility of other stakeholders (i.e. the ETIAS central unit, the ETIAS national units and/or Europol) in close consultation with them.

3.5. Description of processing

Establishing the context and describing the processing operations is the foundation of a solid DPIA and is essential to identify properly the risks for the fundamental rights of the individuals. As highlighted in the Accountability toolkit,[24] the description should allow the reader (e.g. those affected by the processing, the EDPS or other stakeholders) to have a clear understanding of the processing operations including why and how they are carried out.

In particular, the description should include:

- a data flow diagram of the process (flowchart): what is collected from where/whom, what is done with it, where is it kept, who is it given to?
- a description of the purpose(s) of the processing: as with the other elements, this explanation should be carried out step-by-step, distinguishing between purposes where necessary;[25]
- a description of its interactions with other processes - does this process rely on personal data being fed in from other systems? Are personal data from this process re-used in other processes?
- a description of the supporting infrastructure: databases, incorporation of new technologies etc.

Chapter 4 of the DPIA aims at providing a general description of the processing while Chapter 5 shows in a more detailed way the different processing activities.

Given the complexity of the system, the EDPS considers appropriate to adopt a top-down approach, i.e. describing the big picture with the main processing operations and then moving towards more detailed and specific description of these operations. However, as

[24] See EDPS Accountability toolkit, Part I, Page 7.

[25] As part of this description, a brief explanation should be provided on why the organisation needs to carry out this processing operation and how it limits itself to what is necessary for the aim of the processing (necessity and proportionality).

further developed below (points 3.4.1 and 3.4.2), the EDPS notes that the big picture is incomplete while some intermediary steps are missing and some specific steps are not detailed enough to have a clear visualisation and understanding of the system.

3.5.1. General description (Chapter 4 of the DPIA)

The EDPS notes that many elements for a general description of the data processing activity are mentioned in Chapter 4. However, the way they are presented and described does not allow a clear, smooth and comprehensive understanding of the data processing activity. This is exacerbated by the lack of a data flow diagram showing the way personal data move through the system (where the data comes from, where it goes, how it changes, and where it ends up).

The EDPS stresses the importance of having a clear visualisation of the whole system. This could start with the broad view of the system, which is then decomposed into main data processing operations, which in turn are divided into sub-processes. Data flow diagrams could be made in several nested layers. A single process on a high-level diagram could be expanded to show a more detailed data flow diagram. In other words, a hierarchy of data flows diagram could be produced, starting with an abstract view of the system and ending with a number of diagrams representing the lowest-level sub-processes.

The highest level ('0 level') could simply show the system, the external entities with which it interacts, and the data flows between the system and the external entities. The first level could include the main data processing operations while a second level would go into deeper the main processing operations. The EDPS notes that the DPIA misses the '0 level' and the 'first level' data flows diagrams to allow a clear visualisation and understanding of the system.

The ETIAS synthetic overview on p.29 provides a good overview of the system's components, prompting to the system's architecture but it lacks a visualisation of the data flows and the main data processing operations.

This visualisation is also difficult to extract from the general description.

Section 4.3 (general description of the data processing activity) contains either too detailed aspects (e.g. the fact that the ETIAS central unit should be operational 24 hours a day) or incomplete ones (e.g. identification of external entities).

Information related to the data processing activity (e.g. data collected, recipients, etc.) are merely listed in section 4.2 but not interlinked. This is however essential to get a comprehensive overview of the data processing activity. For instance, not all the recipients of the data listed under point 4.3.4 are integrated in the description.

Furthermore, several expected data flows were not found in the system description. Examples include the revocation of the ETIAS travel authorisation (which could lead to risks from not notifying the user) or the TCNs' verification of their application or ETIAS validity.

In light of the above, the EDPS recommends adding two data flow diagrams ('0 level' and '1st level') in Chapter 4 of the DPIA to allow a clear visualisation of how information in general enters and leaves the system, what changes it, and where the information is stored. The first one should show the system, the external entities with which it interacts, and the data flows between the system and the external entities. The second one should expand the first one and include the main data processing operations.

The EDPS also recommends reviewing the structure of Chapter 4 to describe in a clear, focused and comprehensive way these two data flow diagrams.

3.5.2. Systematic description (Chapter 5 of the DPIA)

Chapter 5 further describes the main processing operations identified in the general description (see Chapter 4). This could be considered as the '2d level' data flow diagram.

For each main processing operation, the DPIA provides:
- a flowchart,
- a table listing the different steps mentioned in the flowchart including for each of them,
    - a reference to the subsection describing each step,
    - the purpose,
    - the data supporting asset,
- a description of the process for each step,
- an overall view.

The EDPS welcomes this approach. However, he notes some lack of clarity, comprehensiveness and/or consistency.

The flow chart, the table and the descriptions of each step are not always present or aligned. For instance, section 5.6 on manual processing does not include a table. In section 5.5, different steps mentioned in the table do not appear neither in the flowchart nor in the description (e.g. disclosing/transferring the data). In Section 5.5, elements in the overall view do not appear in the flowchart (e.g. CIR) and vice versa (e.g. screening rules). The users that perform each action step are not always indicated. A different wording is used for a same step (e.g. the table in section 5.5 mentions 'merging data sets' while the flowchart and the description refer to 'consolidated result').

Besides, the DPIA should further clarify and describe some main data processing operations rather than merely copying the legal provisions. For instance, section 5.5 on automated processing operations should describe for each system (SIS, VIS, etc.) which data contained

in the TCN application will be used for the comparison as well as what situations (i.e. which data or combination of data) will trigger a hit.

In light of the above, the EDPS recommends ensuring that:
- a flowchart, a table and a description are included for each main data processing operation,
- all steps are identified in the flowchart and the table and are described in a clear and consistent way,
- the description of each step includes the user, the action, the data and the supporting asset.

3.6. Assessment of necessity and proportionality

Chapter 6 of the DPIA mentions that it aims at assessing the necessity and proportionality of the ETIAS processing activities listed in Chapter 4.

However, instead of assessing the technical design and functionalities chosen by eu-LISA to implement the ETIAS regulation, Chapter 6 mainly assesses the ETIAS Regulation. The EDPS stresses that such an assessment is the responsibility of the legislator, not of eu-LISA.

Eu-LISA has to comply with the legislation and implement it as adopted. The DPIA to be carried out by eu-LISA as data controller concerns its selections in the technical design.[26]
It should seek to answer the question 'how can eu-LISA fulfil its tasks given by the legislator in a compliant and privacy-friendly way?'

For instance, when the draft application is submitted and stored, the system collects information from the user (TCN) such as IP address, timestamp and device information (section 5.3.10). This could be for logging, audit and statistics purposes on the browser of the user (to ensure adequate statistics are provided about the browsers to be supported).

Eu-LISA should assess the necessity and proportionality on each data collected in this context. It should ensure that only the necessary data for the user's device are collected and that there is adequate policy not to reveal such information to other entities (e.g. law enforcement authorities) if this not relative to the investigation on who submitted an application for another person or for non-repudiation. The risk of failing to identify and process only the necessary data could lead to the risk of the user being subject to profiling or unauthorised use of such information.

Another example could be about the use of specific tools. Under certain conditions, the applicant is allowed to do the required interview remotely.[27] The ETIAS National Unit officer along with the TCN agree on the tool to be used from a list of tools, preselected by eu-LISA.

[26] See EDPS Accountability toolkit, Part I, Page 7-8.
[27] Article 27 (4) of the ETIAS Regulation provides that: 'If the consulate located the nearest to the place of residence of the applicant is at a distance of more than 500 km, the applicant shall be offered the possibility to conduct the interview by remote means of audio and video communication. If the distance is less than 500 km, the applicant and the ETIAS National Unit of the Member State responsible may jointly agree to the use of such means of audio and video communication.'

If the interview tool collects more personal data on the TCN than necessary (e.g. connection data), there is a risk of profiling and unauthorised use of such data.

Eu-LISA's responsibility includes the analysis of the personal data these preselected tools collect about the TCNs and of their devices as well as whether these are the minimum required to accomplish the goal of the interview conduction. Also, any transfers of personal data (content of the communication or metadata) to third parties and third-countries should be thoroughly analysed under the legality but also the necessity and proportionality lenses.

The EDPS recommends reviewing Chapter 6 and explaining:
- why the proposed design and technical functionalities of the ETIAS are effective means to implement the ETIAS Regulation,
- whether eu-LISA has considered alternatives and,
- why the solutions chosen are the least intrusive means from the fundamental rights perspective.

3.7. Analysis of risks and establishment of controls for identified risks

A risk is a possible event that could cause harm or loss or affect the ability to achieve objectives. When defining a risk in the context of a DPIA, the objective is the protection of data subjects' fundamental rights and freedoms and/or following the data protection principles provided by the applicable legal framework (that also have a goal to protect data subjects' rights). While there is also a compliance risk for the organization, the focus is on the impact to the rights and freedoms of data subjects.[28]

As developed above (points 3.4 and 3.5), the description provided in the DPIA for the system and the data processes does not promote a clear concept of the whole system, which is necessary to identify high-level related risks and to understand the impact they could have on the data subjects (TCNs).

The risk assessment in a DPIA includes identifying[29]:
- what could go wrong (the risk),
- what might lead to the risk taking place (the source),
- how likely it is that the risk could harm individuals (the likelihood),
- what would be the adverse impact for individuals (impact),
- how serious would the adverse impact be (severity),
- what would be suitable control measures to eliminate, reduce or minimize the risks (mitigation measures).

[28] See EDPS Accountability toolkit, Part II, Page 8-10.
[29] See WP29, "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", adopted on 04 April 2017 by EDPB, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en , pages 17 and 22.

Chapter 7 (p. 120) lists the risks identified throughout Chapter 5, which describes the functionality (e.g. Risk 1 on p.60). The EDPS notes that most of the risks are related to an action being wrong in the processing (e.g. unauthorised access to private data in Risk 1) or a data protection principle being affected (e.g. fairness, transparency, accuracy, security in Risk 1). However, the impact on the data subject is not provided. The EDPS stresses the importance to describe all the four elements, i.e. the source, the risk, the impact and the mitigation measure(s) to allow a proper risk assessment.

An example of the elements expected is given below for Risk1:

- source: erroneous email entered by the data subject.
- risk: unauthorised access - the unauthorised person accessing the application can withdraw the application, communicate the information to other people or use the information for other purposes.
- impact: financial, reputational, identity theft.
- mitigation: validation of the email before the user enters any personal data.

The EDPS notes that the DPIA contains a knowledge base for impact ratings, which lists examples of physical, material and moral impacts on the individual. He suggests describing the impact of each risk based on this knowledge base.

In addition, the EDPS notes that the DPIA lists 21 risks that eu-LISA considers limited or negligible after the application of the mitigation measures. This list however does not include risks eliminated or considered low risks after their mitigation through the eu-LISA's security base line measures. The EDPS stresses that such risks and mitigation measures should be presented in the DPIA to demonstrate that all relevant risks have been identified but are considered to be mitigated. Such a practice would also guide the incorporation of these measures in the design of the ETIAS system implementation in the next stages.

Furthermore, the EDPS notes that the security analysis (section 7.1.7) is incomplete, due to the fact that the security risks assessment for ETIAS is not performed yet. As the Information Security Management Process includes a security risk assessment for the assets of the organization (including personal data), with a focus on the organization, any decision on implementing mitigation measures will be based on the costs and impact on the organization.

The outcome of the security risks assessment (residual risks after mitigation measures), should be input to the DPIA, to also assess the risk from the perspective of the data subjects. While analytical explanation of security risks (e.g. by type of attack of malicious users) would not be necessary, a general description of such risks should be provided (e.g. malicious external actors gaining unauthorised access to the applicant's data via the website), mapped to data protection risks (e.g. unauthorised access) and re-assessed.

The EDPS welcomes that Eu-LISA has already identified some security risks, as part of the DPIA process (e.g. R17 - lack of adequate encryption for data in transit and at rest (for the watchlist)). It has also pre-identified specific security risks that will have significant impact on personal data, by assuming vulnerabilities of the web interface/mobile app/carrier interface in order to gain unauthorised access to personal data either transferred during a specific transaction or stored in the ETIAS databases.

However, the EDPS notes that no risks related to security incidents on the central unit of ETIAS have been identified. He reminds that eu-LISA acts as a data controller in relation to information security management of the ETIAS Central system and expects a thorough assessment of data protection risks, stemming from information security risks.

Overall, examples of risks to be considered are:

- Risks related to unauthorised access of the submitted application, e.g. due to:
  - another person accessing the email of the user and getting access to the application's link, then withdraws or edits the application,
  - a technical error of the system sending the link to another applicant,
  - the user mistyping their email address and the hyperlink of the application goes to another email address,
  - the user being misled to think that by saving the draft application his/her application is submitted,
  - the user losing access to the email account or the email provider shutting down.

- Risks related to the automated processing of the application (including the watchlist management), e.g. providing the applicant's data to Europol due to:
  - a HIT with Europol data, when the applicant is registered as a victim or a witness,
  - a false positive HIT which is the result of an erroneous technical implementation of risks indicators of article 33 (subsection 5.5.1),
  - a watchlist not updated (subsection 5.9.5).

- Risks related to the payment of the ETIAS application fee, e.g. due to:
  - abuse of the payment data by the applicant's bank (they know the holder of the card has made a transaction for a fee to ETIAS but not details of the application),
  - a technical problem resulting to missing confirmation of the payment.

- Risks related to access by law enforcement or border control agencies, e.g. due to:
  - identifying wrong hit from the results the applicants' data are entered in LEA systems,
  - extensive search of the system, without fulfilling the criteria for search (serious crime, applicant present at the border, information is already present in EES, etc),

- storing and using accessed data for other purposes.

- Risks related to access by ETIAS national units to the ETIAS central system:
  - unauthorised data export by ETIAS national units of data stored in the ETIAS central system and import of these data into national systems for other processing purposes.

- Risks related to access by carriers, e.g. due to:
  - searching for applicants that are not going to travel,
  - accessing not up to date data in the read-only database (an ETIAS has been issued in the last 24 hours).

- Risks related to exercising data subjects' access rights, e.g. due to:
  - non-proper verification of the identity for an applicant submitting an access/rectification/erasure request,
  - inability to clearly identify the authority that introduces data in relation to the applicant in one of the systems consulted by the ETIAS central system;

- Risks related to data security incidents or data retention, e.g. due to:
  - failure to inform the data subject when a data breach happens (either if their data are accessed or modified or deleted),
  - failure to delete data from applications or logs according to the data retention policy.
  - failure to combine logs from different systems to investigate a security incident like unauthorised access.

In light of the above, the EDPS recommends:
- Reviewing the DPIA once the overall description of the data flows in the system are complete to ensure that no high level risks are overlooked.
- Ensuring that for each specific risk identified, the source, the impact and the mitigation measure are described.
- Listing *all* identified risks including low risks.
- Reviewing the DPIA and reassessing data protection risks, based on security risks identified after the ETIAS security risk assessment.

4. CONCLUSIONS

The EDPS welcomes that the DPIA generally follows the template structure of the DPIA report provided for in the Accountability toolkit. He also welcomes the top-down approach of the report (i.e. describing the big picture with the main processing operations and then moving towards more detailed and specific description of these operations) given the complexity of the ETIAS.

As a living tool, the DPIA does not need to be fixed once and for all but may be further completed and developed along the implementation and running of the ETIAS. However, the analysis above has shown that, at this early phase of implementation, important elements are still missing or not presented in a clear and comprehensive way to enable a proper and comprehensive identification and assessment of the risks for the individual's fundamental rights.

Given the complexity of the ETIAS system including - among others - its connections with other systems and the key role of several stakeholders, the EDPS recommends eu-LISA to draft a comprehensive version of the DPIA, which would include the risks and mitigation measures identified by other data controllers in their own data protection risk assessments,

before the roll-out of the system. This will allow ensuring that risks stemming from the overall use of ETIAS are adequately tackled.

The EDPS makes the following recommendations to eu-LISA to ensure compliance with the ETIAS Regulation (in particular as regards the implementation of the principle of data protection by design and by default) and with the Regulation:

- Indicate and describe all applicable criteria leading to the decision to conduct a DPIA.

- Provide a comprehensive DPIA, including the risks identified from the DPIAs of the other stakeholders (i.e. the ETIAS central unit, the ETIAS national units and/or Europol), prior to the ETIAS entry into operation.

- Include in the DPIA, risks related to the interactions of the system with processing operations under the responsibility of other stakeholders (i.e. the ETIAS central unit, the ETIAS national units and/or Europol) in close consultation with them.

- Add two data flow diagrams ('0 level' and '1st level') in Chapter 4 of the DPIA to allow a clear visualisation of how information in general enters and leaves the system, what changes it, and where the information is stored. The first one would show the system, the external entities with which it interacts, and the data flows between the system and the external entities. The second one would expand the first one and include the main data processing operations.

- Ensure in Chapter 5 that:
  - a flowchart, a table and a description are included for each main data processing operation,
  - all steps are identified in the flowchart and the table and are described in a clear and consistent way,
  - the description of each step includes the user, the action, the data and the supporting asset.

- Explaining in Chapter 6:
  - why the proposed design and technical functionalities of the ETIAS are effective means to implement the ETIAS Regulation,
  - whether eu-LISA has considered alternatives and,
  - why the solutions chosen are the least intrusive means from the fundamental rights perspective.

- Review the DPIA once the overall description of the data flows in the system are complete to ensure that no high level risks are overlooked.

- Ensure that for each specific risk identified, the source, the impact and the mitigation measure are described.

- List *all* identified risks including low risks.

- Review the DPIA after the ETIAS security risk assessment.

Done at Brussels on 13 September 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI