From: European Data Protection Supervisor
To: 'dpo@eulisa.europa.eu' <dpo@eulisa.europa.eu>
CC: [redacted]
Sent at: 13/05/20 15:52:22
Subject: Our ref.: 2019-0495 - D 1207

Dear Madam,

Please find attached a letter signed electronically by Mrs HAROU for the above mentioned subject.

Kind regards,

EDPS Secretariat

| Tel. (+32) 228 31900 | Fax +32(0)22831950 | ›
Email edps@edps.europa.eu
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

EUROPEAN DATA PROTECTION SUPERVISOR

DELPHINE HAROU
HEAD OF SUPERVISION AND ENFORCEMENT UNIT

[redacted]
Vesilennuki 5,
10415 Tallinn
Estonia

Brussels, 13th May 2020

DH/[redacted]D(2020) 1207 **C 2019-0495**
Please use edps@edps.europa.eu for all correspondence

Subject: **ETIAS data protection impact assessment: preliminary guidance (case 2019-0495)**

Dear Ms [redacted]

I would like to express my appreciation for your continuous work on the implementation of the European Travel Information and Authorisation System (ETIAS), especially under the particular circumstances we are all currently facing.

At this early implementation stage of ETIAS, I would like to provide you with some additional orientations to the ones provided in the Accountability on the Ground Guidelines[1]. They might be useful to achieve full alignment of the ETIAS Data Protection Impact Assessment (DPIA) with the requirements of Regulation (EU) 2018/1725[2] (the Regulation). In order to support your work, we would like to raise awareness about certain best practices in a DPIA and common pitfalls.

To our understanding of the discussions with two of the co-controllers in ETIAS (Frontex and eu-LISA), eu-LISA has been assigned the responsibility to perform the DPIA, for which reason I address this letter to you. We would like to stress again that given the complexity of ETIAS regarding its ecosystem, network and processing operations, a good coordination between all stakeholders is required. We understand that one of the challenges comes from the fact that the distribution of roles under Regulation (EU) 2019/817 (ETIAS Regulation)[3] implies that different stakeholders are involved at different stages. Cooperation between ETIAS

[1] EDPS Guidelines Accountability on the ground Part I and II available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.
[2] OJ L 295, 21.11.2018.
[3] OJ L 135, 22.5.2019.

stakeholders is therefore paramount to ensure coherence, consistency, engagement and coordinated actions. The same reasoning applies to the DPIA, since it involves the joint effort of all stakeholders to identify potential risks and mitigating measures regarding ETIAS' data processing operations. On top of it, the current pandemic crisis is adding another level of complexity.

At this stage of development of ETIAS, it is vital to think carefully about the data processing models, methodologies, risks and how to address them. A DPIA can do this for you. A solid DPIA is crucial for the global understanding of ETIAS processing operations and to develop the roadmap that will help all stakeholders to find the way to comply with the data protection rules.

For the ETIAS DPIA the following concepts require special attention[4]:

- the need for a systematic description of the envisaged processing operations and purposes. The DPIA serves to model the processes you want to put in place from a data protection perspective, i.e. to draw the personal data flows;
- a good understanding of the risks to data subjects' rights and freedoms. The DPIA serves to understand how the personal data processing activities could affect data subjects;
- the adoption of a sound methodology for the performance of the risk assessment. The DPIA should serve to identify ways to mitigate any negative effects on the data subjects whose information is going to be processed.

The ultimate goal of a DPIA is to make sure that controllers are able to understand and ensure that the processing operations are the least intrusive possible and that they comply with data protection rules. They will also be able to demonstrate this, in accordance with the accountability principle. Additionally, a good DPIA substantially contributes to fulfilling the controllers' obligation of implementing data protection by design, in addition to offering a methodological approach for it.[5]

1. Systematic description of the envisaged processing operations and purposes

Establishing the context and describing processing operations is the foundation of a solid DPIA process. In short, you have to describe what you plan to and how you plan to do it. This documentation should allow the reader – be it those affected by the processing, your own top management, who will have to sign off on the DPIA report, the EDPS or other stakeholders – to understand what the processing is about and why you are doing it.

As set out in the Accountability on the ground Guidelines,[6] the description of the processing operations should allow the reader to understand what each of the processes is about and what the reason behind it is. The following elements have been identified in the guidelines as crucial in order to be able to provide an accurate description:

[4] In our view, 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.

[5] EDPS, Preliminary Opinion on Privacy by Design, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

[6] Page 7.

- 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;[7]
- a **data flow** diagram of the process (flowchart): what is collected from where/whom, what is done with it, where is it kept and for how long, who is it given to? The EDPS expects eu-LISA to provide a detailed account of the different steps of the personal data processing operation in a connected matter, so that the lifecycle of the personal data can be more clearly understood. In addition, wherever the data stored in the same repository is used for different purposes, there should be one data flow per purpose;
- 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.

As a starting point for its process description, eu-LISA could use existing documentation of the process development. A lot of the information required most likely already exists at eu-LISA, as part of project or process documentation kept for other reasons. eu-LISA may want to re-use this documentation as far as practicable and expand wherever necessary to entail the above information.

2. Understanding the risks to data subjects' rights and freedoms

A DPIA should identify and propose measures to mitigate the risks to the rights and freedoms of natural persons. These may result from personal data processing that could lead to physical, material or non-material damage. For instance, where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage or where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.[8]

Personal data processing activities taking place in ETIAS are meant to support the decision of Member States to authorise or deny the entry of an individual to the EU territory, wherever this individual is exempted from the visa requirement. It is more specifically aimed at supporting the decision of whether the presence of this individual on the territory of the MS does not pose or will not pose a security, illegal immigration or a high epidemic risk.[9] A travel authorisation therefore "constitutes a decision indicating that there are no factual indications or reasonable grounds to consider that the presence of a person on the territory of the Member States poses such risks".[10]

---

[7] As part of this description, a brief explanation should be provided on why the organisations 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).

[8] Recital 46 Regulation 2018/1725.

[9] Recital 9 ETIAS Regulation. Article 3 (1)(6), (7), (8) define the terms "**security risk**" as the threat to public policy, internal security or international relations for any of the Member States, "**illegal immigration risk**" as 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, and "**high epidemic risk**" as any disease with epidemic potential as defined by the International Health regulations of the WHO or the ECDC and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States.

[10] Recital 9 ETIAS Regulation

Denial of entry may create a series of negative consequences for individuals: a restriction on the enjoyment of their freedom of movement, a financial impact if they travel to the EU for business purposes, impact on their health if they travel to the EU to get a medical treatment they cannot obtain in their own country[11]. Admission to the EU territory may be subject to additional checks at the border, thus interfering into this individual's privacy.

For these reasons, Article 14 of the ETIAS Regulation, entitled "Non discrimination and fundamental rights" puts the emphasis on a series of rights to which the data controllers should pay specific attention when implementing ETIAS system, namely:

- **Ensuring Non-Discrimination**. "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". The right to non-discrimination is a fundamental right recognised by Article 21(1) EU Charter;
- **Protecting Human dignity**. The right to Human Dignity is protected by Article 1 EU Charter which says that "Human Dignity is inviolable". In the context of border management, this right is interpreted as an obligation for border controls to be carried out in a professional and respectful manner and be proportionate to the objectives pursued.[12] This also means that all travelers 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 law[13];
- **Protecting the rights to Privacy and Data Protection** (Articles 7 and 8 EU Charter);
- **Protecting more vulnerable groups of individuals**, in particular children[14], elderly and persons with a disability.

The goal of the DPIA will thus be to identify and address the risks to data subjects' rights and freedoms created by the personal data processing activities taking place in ETIAS at each stage.

3. Adopting a systematic process for risk assessment

To allow for systematic assessment of risks, a DPIA methodology should be adopted. The goal of such a methodology would be:

- to allow for the definition of and justification for mitigating measures for the risks to data subjects;
- to estimate the residual risks to data subjects in order for the controllers' management to take an informed decision as to whether risks are adequately mitigated and proceed with the processing operation.

[11] For instance, there are cooperation agreements between Portugal and the Portuguese-speaking African countries (PALOP) regarding access to health care services to be provided to citizens of the latter in the territory of the first.
[12] Recital 7 of the Schengen Borders Code
[13] Section 1.2 of the Practical Handbook for Border Guards (Schengen Handbook)
[14] The rights of the child are protected under Article 24 EU Charter which mandates public authorities to take childrens' best interest as primary consideration in all actions relating to children.

While you are free to select one of the existing DPIA methodologies[15] or create your own, for it to be of maximum effectiveness it should at least contain:

- a description of the roles and responsibilities of the different actors in the DPIAs exercises (e.g. who within the controllers will assess risks, who will select mitigating controls, who will sign-off the report). In case contractors are involved, explain their role and the relationships with key stakeholders of the system;
- a way to describe the business processes and data flows;
- a way to determine what events could create risks to data subjects ;
- a method to estimate the likelihood and impact of these events;
- a method to calculate the risks to data subjects based on the events, their likelihood and their impact;
- information on how the controllers' management will decide on which risks to data subject to mitigate, and the options they have for taking such a decision;
- a method for the risk analysis to propose the implementation of mitigating measures to reduce the risks to data subjects;
- a method to calculate the residual risks to data subjects;
- information on how the controllers' management will decide on any residual risks to data subjects, and the options they have for taking such a decision.

Usually, the analysis of the risks to data subjects is qualitative *i.e.* estimated on scales (one for likelihoods, one for impacts and one for the risks).

While there is a clear information security risk management (ISRM(aspect to this (not least since keeping data securely is one of the data protection principles), ISRM is far from all there is to this exercise. ISRM tends to focus on risks that stem from unauthorised system behaviour (e.g. unauthorised disclosure of personal data), while parts of the risks to data subjects and compliance risks stem from the authorised system behaviour for which you do the DPIA.

Processes working exactly as planned may have impacts on data subjects. These risks have to be assessed as well, not only the risks of 'things going wrong'. To do so, use the data protection principles as a reference.

The «what-if» scenarios (events) rely on the knowledge of the operational staff as to what happens in the real world and their knowledge of the business processes and data flows. The key is to have a justified reasonable analysis. In case you involve a contractor in the DPIA, ensure you have identified the key stakeholders of the project to provide input (and feedback at the end) and establish a plan of their involvement/consultation in the process.

Furthermore, a justified reasonable **analysis of the business processes and data flows** will enable all stakeholders to better understand their roles and responsibilities.

As the processing operations become more detailed, the evaluation of the risks will need to be revised to ensure that

- the risks already defined are reasonably well evaluated;

[15] refer to the EPDS and WP29 guidelines for DPIA

- new risks are defined and properly analysed.

In the risk analysis, every step should be documented to be able to trace back why a mitigating measure was implemented vis-à-vis a specific risk to data subjects. In case of different opinions on the selection of mitigation measures, such opinions should be documented as well.

We remain at your disposal for the clarification of any further clarification. Please be reminded that you can always send requests for formal and informal consultations you may consider necessary.

Yours sincerely,

(**Signed**)

Delphine HAROU
(Head of Unit Supervision & Enforcement)

CC: [redacted]