Council of the
European Union

Brussels, 9 March 2017
(OR. en)

7136/17

Interinstitutional File:
2016/0357 (COD)

FRONT 111
VISA 91
DAPIX 78
DATAPROTECT 29
CODEC 350
COMIX 182

COVER NOTE

From:	European Data Protection Supervisor
date of receipt:	6 March 2017
To:	President of the Council of the European Union
Subject:	Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624

Delegations will find attached a copy of the above-mentioned opinion.

EUROPEAN DATA PROTECTION SUPERVISOR

E-MAIL / FAX

GIOVANNI BUTTARELLI
SUPERVISOR

President of the Council of the European Union
General Secretariat
Council of the European Union
Rue de la Loi 175
B-1048 Brussels

Brussels, 06 MAR 2017
GB/LS/ssp/D(2017)0482 C2016-1041
Please use edps@edps.europa.eu for all correspondence

Subject: **Opinion on the European Travel Information and Authorisation System (ETIAS)**

Dear Mr President,

With regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 28(2), I send you an Opinion on the Proposal for a European Travel Information and Authorisation System.

I have written in similar terms to the President of the European Commission and the President of the European Parliament.

Yours sincerely,

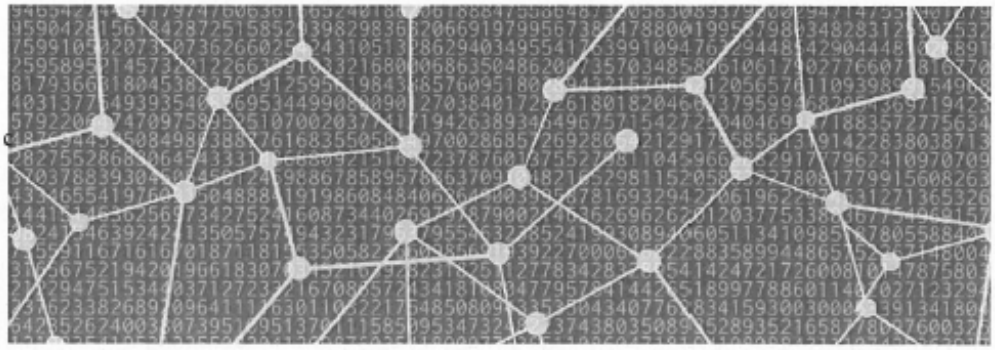
Giovanni BUTTARELLI

Annex: Opinion on the Proposal for a European Travel Information and Authorisation System

Cc: Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General
Ms Marlene BONNICI, Permanent Representative of Malta
Mr Ralph KAESSNER, Secretariat General of the Council

Contact persons: *Lara Smit (tel: 02 2831966), Priscilla de Locht (tel: 02 2841246)*

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 3/2017

EDPS Opinion on the Proposal for a European Travel Information and Authorisation System (ETIAS)

EDPS

6 March 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data ... for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '...for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on the data protection implications of their policies and foster accountable policymaking - in line with Action 9 of the EDPS Strategy: 'Facilitating responsible and informed policymaking'. The EDPS considers that compliance with data protection requirements will be key to the success of the future European Travel Information and Authorisation System.

Executive Summary

EU border management policy has witnessed notable developments over the past years, due to the challenges posed by the influx of refugees and migrants, as well as security concerns heightened by the attacks in Paris, Brussels and Nice. The situation at present and the need to guarantee safety within the territory of the Member States prompted the Commission to launch several legislative initiatives aiming at improving control over persons accessing the Schengen Area.

One of these initiatives is the Proposal for a Regulation establishing a European Travel Information and Authorisation System ('ETIAS'), tabled by the Commission on 16 November 2016.

According to the Proposal, the system would require visa-exempt travellers to undergo a risk assessment with respect to security, irregular migration and public health risks prior to their arrival at the Schengen borders. This assessment would be carried out by means of cross-checking applicant's data submitted through ETIAS against other EU information systems, a dedicated ETIAS watchlist and screening rules. This process will result in granting -or denying- an automated authorisation for entering the EU.

With the ETIAS Proposal, the EU legislator appears to follow the increasing trend of addressing security and migration management purposes jointly, without taking into account the substantial distinctions between these two policy areas. The establishment of ETIAS would have a significant impact on the right to the protection of personal data, since various kinds of data, collected initially for very different purposes, will become accessible to a broader range of public authorities (*i.e.* immigration authorities, border guards, law enforcement authorities, etc). For this reason, the EDPS considers that there is a need for conducting an assessment of the impact that the Proposal will entail on the right to privacy and the right to data protection enshrined in the Charter of Fundamental Rights of the EU, which will take stock of all existing EU-level measures for migration and security objectives.

Moreover, the ETIAS Proposal raises concerns regarding the process of determining the possible risks posed by the applicant. In this regard, specific attention should be given to the definition of those risks as such. Given that the consequence for an individual could be a denial of entry, the law should clearly define what the assessed risks are. The EDPS also questions the existence of the ETIAS screening rules. The EDPS understands that the legislator's objective is to create a tool enabling the automatic singling out of visa-exempt third country nationals suspected of posing such risks. Nonetheless, profiling, as any other form of computerised data analysis applied to individuals, raises serious technical, legal and ethical questions. Therefore, the EDPS calls for convincing evidence supporting the necessity of using profiling tools for the purposes of ETIAS.

Furthermore, the EDPS questions the relevance of collecting and processing health data as envisaged in the Proposal. He asks for better justification of the chosen data retention period and of the necessity of granting access to national law enforcement agencies and Europol.

Finally, he provides recommendations for instance on the division of roles and responsibilities between the different entities involved and the architecture and information security of ETIAS.

TABLE OF CONTENTS

I. INTRODUCTION 5

II. AIM OF THE PROPOSAL 6

III. MAIN RECOMMENDATIONS 6

1. IMPACT OF ETIAS ON PRIVACY AND DATA PROTECTION 6
2. DEFINING THE OBJECTIVES OF ETIAS 8
3. ETIAS SCREENING RULES AS A PROFILING TOOL 9
4. HEALTH DATA 12
5. ACCESS BY LAW ENFORCEMENT AUTHORITIES 13

IV. ADDITIONAL RECOMMENDATIONS 14

1. DATA QUALITY AND DATA MINIMISATION 14
2. DATA RETENTION 15
3. INTERACTIONS WITH OTHER INFORMATION SYSTEMS 17
4. DATA SUBJECT RIGHTS AND REMEDIES 17
5. INDEPENDENT REVIEW OF THE CONDITIONS FOR ACCESS 18
6. DIVISION OF ROLES AND RESPONSIBILITIES 18
7. PRIOR VERIFICATION OF EUROPOL REQUESTS OF ACCESS BY THE EDPS 19
8. VERIFICATION BY THE ETIAS CENTRAL UNIT 20
9. ARCHITECTURE AND INFORMATION SECURITY 21
10. STATISTICS 22
11. ROLE OF THE EDPS 23

V. CONCLUSION 23

NOTES 25

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty of the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[2], and in particular Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[3],

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. The European Commission's initiative of establishing a European Travel Information and Authorisation System (hereinafter referred to as 'ETIAS') dates back to a Communication of 2008 entitled "Preparing the next steps in border management in the European Union"[4]. In this Communication, the Commission suggested new tools for the future management of European borders -notably the Entry/Exist System ('EES') and the Registered Traveller Programme ('RTP')- and considered for the first time the introduction of ETIAS, called an EU Electronic System of Travel Authorisation ('ESTA') at the time. The EDPS issued preliminary comments[5] on this Communication the same year.

2. In February 2011, the Commission issued a Policy Study[6] analysing four different options for the introduction of an EU ESTA. The Study reached the conclusion that the conditions were not met at the time to justify building an EU ESTA. In a Communication[7] of 2012 related to Smart Borders, the Commission considered that the establishment of an EU ESTA should be temporarily discarded but announced its intention to continue the work on the EES and the RTP.

3. In the Communication[8] "Stronger and Smarter Information Systems for Borders and Security" of 6 April 2016, the Commission announced that it will assess the necessity, technical feasibility and the proportionality of establishing a future European Travel Information and Authorisation System. The same year, the Commission carried out a Feasibility Study, which used as a benchmark three other existing travel authorisation systems in the world: the ESTA in the USA, the eTA in Canada and the eVisitor in Australia.

4. On 16 November, the Commission released the Final Report of the Feasibility Study[9] (hereinafter referred to as '2016 Feasibility Study') as well as the Proposal for ETIAS (hereinafter referred to as 'the Proposal").

5. The EDPS welcomes that he was informally consulted by the Commission services before the adoption of the Proposal. However, he regrets that due to the very tight deadline and the importance and the complexity of the Proposal it was not possible to provide a meaningful contribution at that time.

II. AIM OF THE PROPOSAL

6. The EDPS understands from the Proposal and the accompanying documents, that ETIAS would be an automated IT system created to identify migration, security and health risks associated with a visa-exempt visitor travelling to the Schengen Area. He notes that data processed in ETIAS could also be accessed by national law enforcement authorities and Europol when this is necessary to prevent, detect and investigate terrorist offences and other serious criminal offences.

7. Under the Proposal, all visa-exempt third country nationals will have to insert a set of data in an online application prior to the date of their trip. When verifying and assessing the information submitted by visa-exempt travellers in order to grant or deny a travel authorisation, the system will automatically cross-check each application against:
   - other EU information systems: the Schengen Information System ('SIS'), the Visa Information System ('VIS'), Europol data, the Interpol database for Stolen and Lost Travel Documents ('SLTD'), as well as possibly the Eurodac database, the future European Criminal Records Information System ('ECRIS') for third country nationals and the future EES,
   - a dedicated ETIAS watchlist which will be established by Europol and will consist of data related to persons who are suspected of having committed or taken part in a criminal offence or persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences,
   - and screening rules defined within the ETIAS Central System.

8. Where the automated processing does not report any hit, the system will automatically issue a travel authorisation. If there is one or several hits, the application shall be manually processed by the ETIAS National Unit of the Member State of the traveller's intended first entry as declared in the application form. The task of the responsible ETIAS National Unit would be to assess the irregular migration, security or public health risk and decide whether to issue or refuse a travel authorisation.

III. MAIN RECOMMENDATIONS

1. Impact of ETIAS on privacy and data protection

9. The EDPS notes the growing number of EU policy measures on security and migration issues. In his role as advisor to the legislator, the EDPS is not a priori for or against any

measure but focuses on the question to what extent the choice of the legislator is constrained by -and if so in accordance with- the principles of data protection.

10. The EDPS recalls that the right to the protection of personal data, as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter referred to as 'the Charter'), applies to every individual whose data are processed by a controller in the EU whether or not he/she is an EU citizen, a migrant (irregular or not), an asylum seeker or a presumed innocent. Pursuant to the necessity and proportionality principles, as enshrined in Article 52 (1) of the Charter, any interference with or limitation on the exercise of the right to the protection of personal data must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. The EDPS stresses that these principles are high-level legal requirements of EU law and as such inevitably come under scrutiny of the Court of Justice of the EU.

11. The EDPS first welcomes the attention paid to data protection throughout the Proposal. In particular, he notably welcomes the alignment with the definitions in the General Data Protection Regulation[10], the Directive for the police and justice sectors[11] and Regulation 45/2001 (Article 3(2), (3) and (4)); the provision of training on data security and data protection for the European Border and Coast Guard Agency's staff working in the ETIAS Central Unit and the staff of ETIAS National Units before they are authorised to process data recorded in the ETIAS Central System (Article 65(2) and Article 66(3)); the reference to the data protection legal frameworks applicable to the different stakeholders (Article 49); and the prohibition of transfers and onward transfers of ETIAS data to third countries, international organisations and private parties in or outside the EU (Article 55).

12. According to the Explanatory Memorandum and the documentation accompanying the Proposal, the ETIAS as currently proposed, would contribute -amongst others- to prevent irregular migration, ensure enhanced internal security and protect public health. In this context, the EDPS notes that the Proposal establishes another additional system in the area of immigration and security that will collect an even more significant amount of data on third country nationals (including health and judicial data). The EDPS recalls that both necessity and proportionality of this scheme are to be assessed globally, taking into account the already existing systems in the EU, the nature of the data (including judicial and health data) and the scale of the envisaged processing operation (all visa-exempt third country nationals travelling in the Schengen area).

13. The EDPS notes that the Proposal is not accompanied by a data protection impact assessment, that would analyse various policy options to achieve the stated objectives, taking into account all EU-level measures in the same policy area and assess impact on (the fundamental rights of) individuals for each option. **The EDPS underlines that the lack of a data protection impact assessment, which is a fundamental prerequisite, does not make it possible to fully assess the necessity and proportionality of ETIAS as it is currently proposed**. Nevertheless the EDPS underlines a few of the issues which need to be addressed in this data protection impact assessment such as:

    1) The distinct public policy areas of immigration and security

14. The EDPS observes that migration management and security purposes are increasingly associated in the context of granting access to existing systems for law enforcement purposes (*e.g.* VIS and Eurodac[12]), building new information systems (*e.g.* the proposal for

an Entry/Exit System[13]) or extending the competences of an existing body (*e.g.* the European Border and Coast Guard[14]).

15. By addressing irregular immigration and security objectives together and creating a single database which will contain both migration and criminal related data, the ETIAS Proposal is part of this current trend. This has an impact in terms of data protection since more personal data will be collected and be accessed by various authorities (immigration authorities, border guards, law enforcement authorities, etc). In addition, there might be a risk of an overlap of tasks and data processing since under the Proposal, both the European Border and Coast Guard Agency (hereinafter referred to as 'EBCG Agency') and Europol will -to some extent- be involved in security risk assessment. The EDPS would like to stress that, while there might be synergies between migration and internal security, these are two different areas of public policy with distinct objectives and key actors.

2) The risk of unbalanced treatment between visa-exempt travellers and visa-required travellers

16. The EDPS questions whether the Proposal does not create a more intrusive regime for visa-exempt travellers than for visa-required travellers since more data will be centralized at EU level in ETIAS[15] than in the VIS. As a consequence more data may also be accessed by various authorities having an access to ETIAS. Besides, the EDPS notes that data of the applicant for an electronic travel authorisation will be cross-checked with specific risk indicators and a watchlist, which are not used to deliver a visa.

3) The redundancy of ETIAS with API and PNR data processing

17. Moreover, the EDPS questions the redundancy of the ETIAS with Advance Passenger Information ('API') and Passenger Name Record ('PNR') data already collected on visa-exempt travellers before they reach the Schengen area. The EDPS notes that for all visa-exempt third country nationals travelling by air, much of the information to be collected by the ETIAS is already collected through API and PNR data to assess passengers prior to their arrival on the Schengen territory (once the system will be up and running). The EDPS wonders whether the ETIAS would not duplicate available information in this context.

18. In conclusion, the EDPS stresses **that a privacy and data protection impact assessment of ETIAS should take stock of all EU-level measures taken for migration and security objectives and analyse in-depth their concrete implementation, their effectiveness and their impact on individuals' fundamental rights before creating new systems involving the processing of personal data. This analysis should also take into account the policy area in which these measures apply and the respective role of the key actors involved.**

2. Defining the objectives of ETIAS

19. The EDPS recalls that according to the purpose limitation principle, which is at the heart of data protection, personal data must be collected for specified, explicit and legitimate purposes. The purpose(s) must be detailed enough to determine what kind of processing is included within the specified purpose. Only a clear definition of purposes will allow a correct assessment of the proportionality and adequacy of the personal data collected.

20. The EDPS also underlines that a definition of the purposes is not only fundamental from a data protection perspective but is also essential to ensure the efficiency of the system: How could a competent authority assess whether an individual poses an irregular migration and/or security risk without a clear definition of what these terms encompass?

21. Article 1 of the Proposal mentions that ETIAS aims at determining whether the presence of a visa-exempt traveller in the territory of the Member States poses an irregular migration, security and/or public health risk. The EDPS notes that the Proposal defines the public health risk by referring to specific categories of diseases[16] but does not define security and irregular migration risks.

22. (Im)migration is usually identified in a binary way as either legal (regular) or illegal (irregular). However, in practice irregular migration can involve a wide spectrum of violations of immigration and other laws; *e.g.* entering into a Member State without the necessary authorization or documents, overstaying a visa-free travel period, absconding during the asylum procedure or failing to leave a host Member State after a negative decision.

23. The EDPS notes that the Proposal does not clearly specify the categories of violations of immigration (and other) laws that may pose a risk of irregular migration. He understands through various provisions of the Proposal that overstaying or being subject to a return decision would -amongst others- be elements to be considered to assess the risk of irregular migration. The EDPS recommends to better consider which violations of (im)migration laws should be taken into account. The gravity of the infringement is different whether a third country national has entered into a Member State using false documents or he has overstayed for a couple of days.

24. As regards security risks, the EDPS notes that the Proposal also does not define them. Security means at basic level maintaining public order and safety. This may accommodate a plethora of situations, ranging from vandalism to terrorism acts. Although this is not clearly specified in the Proposal, the EDPS understands that a key element to assess security risk would be whether or not the third country national is suspected of or has been convicted for criminal offence(s). As for immigration risks, only serious criminal offences should be considered to determine security risks.

25. **The EDPS recommends to include a definition of irregular migration risks and security risks in the Proposal. The definition of irregular migration risk should specify the categories of serious violations of immigration laws (*for example,* defining a gravity threshold of the violation) that may pose a risk of irregular migration. As regards the definition of security risks, the EDPS recommends to consider which criminal offences are to be targeted, by also considering those defined in Article 3(1)(m) of the Proposal.**

3. ETIAS screening rules as a profiling tool

Profiling through ETIAS

26. Article 28(1) of the Proposal provides that ETIAS application files will be assessed against ETIAS screening rules defined as *"an algorithm enabling the comparison between the data*

recorded in an application file of the ETIAS Central System and specific risk indicators pointing to irregular migration, security or public health risks".

27. Article 28(2) lists the kind of information to be taken into account for the identification of the irregular migration, security or public health risks (*i.e.* statistics and information provided by Member States), while Article 28(4) contains a list of data upon which the ETIAS Central Unit will establish the specific risk indicators. The ETIAS Central Unit will be in charge of defining and adapting these specific risks indicators after consultation with the ETIAS Screening Board, composed of representatives of Europol and of each ETIAS National Units (Article 28(5)). Article 28 further specifies that the algorithm will be stored in the ETIAS Central System and the Commission will adopt delegated acts to further specify the irregular, security and public health risks. Nonetheless, in accordance with what the EDPS mentioned before, prior specification of the exact meaning of these risks is required[17].

28. The EDPS understands that the objective of the ETIAS screening rules is to create a tool enabling the automatic singling out of visa-exempt third country nationals suspected of posing irregular migration, security or public health risks. This tool will potentially have adverse consequences on such persons as the aim is, ultimately, to prevent them from entering the territory of the Member States. **For the sake of clarity and transparency, the technique of data processing proposed in Article 28, which clearly constitutes profiling, should be explicitly named as such, so that all necessary safeguards for such processing be provided for.**

Impact assessment covering profiling

29. Profiling, as any other form of computerised data analysis, when used in the process of decision making that affects individuals, raises serious technical, legal, and ethical questions. One major concern regarding profiling is the fact that it is indispensably related to a high degree of generalisation and uncertainty regarding both the correctness of the predicted behaviours, and the accuracy of attributing detected patterns' correlations to particular features of the individuals. Furthermore, the assessment of individuals from the perspective of a created profile, requires not only prior categorisation of a person, but may also result in the unjust or prejudicial treatment of certain categories or groups of people[18].

30. Therefore, the EDPS is concerned whether the use of the ETIAS screening rules will be fully in line with the fundamental rights enshrined in the Charter, particularly with the rights to privacy, data protection and non discrimination. **The EDPS recommends that the proposed ETIAS screening rules be subject to a prior comprehensive assessment of their impact on fundamental rights, which will also assess the necessity and proportionality of using such tool.**

Necessity of profiling tools

31. In addition to being assessed against ETIAS screening rules, the ETIAS Proposal foresees that every application entered into the ETIAS Central System will also be automatically:
    - cross-checked against information in other EU IT systems listed in Article 18(2), and
    - matched against specific values (*e.g.* a phone number or an IP address) included in the ETIAS watchlist established pursuant to Article 29.

32. While the method of screening rules relies on data analytics and constitutes profiling, these two methods rely on the comparison of ETIAS data with information available in EU databases or gathered in the watchlist in search for potential correspondences ("hits"). Information stored in other IT systems and the watchlist should be more reliable than a screening against a non-transparent profile created by an algorithm. Therefore, the EDPS invites the legislator to reflect on the necessity of using screening rules for the purposes of ETIAS, while the Proposal provides for other instruments for examining whether the presence of the applicant on the territory of the Member States would pose an irregular migration, security or public health risk.

33. **The EDPS calls for convincing evidence supporting the necessity of using profiling tools for the purposes of ETIAS and, *quod non*, encourages the legislator to reconsider to which extent the use of profiling is necessary with the purposes to be achieved.**

Proportionality

34. If proven necessary, the use of profiling tools should also be proportionate. The EDPS welcomes that the Commission draws attention to the fact that the risk indicators shall be targeted and proportionate. The EDPS questions whether the Proposal provides safeguards to achieve this goal and ensure a sufficient level of protection of fundamental rights.

35. The Proposal provides for the assessment of all visa-exempt third country nationals' applications against ETIAS screening rules[19], while only a limited number of them may in reality pose certain types of risks and be denied a travel authorisation. These automated and non-transparent operations on personal data entail as such a serious interference with the fundamental rights of an unlimited number of applicants, who would be subject to profiling; it should be balanced against the expected outcome of such a tool.

36. Furthermore, depending on the method used to develop the specific risk indicators, which could be construed in a very broad manner, the number of people denied automated authorisation due to a hit based on the screening rules may be relatively high, even though these persons do not actually present a risk.

37. The EDPS welcomes that in case of denial, the application will be further processed manually by ETIAS National Units (Article 22). However, a denial of automated authorisation is a decision which can substantially affect the applicant. Given the lack of transparency in the process of creating profiles, one can doubt of the effectiveness of the manual processing of applications carried out by the ETIAS Central Unit or ETIAS National Units. How could a real in-depth scrutiny of the detected potential risks be guaranteed as staff of these units might not themselves know or understand the reason for the refusal of travellers' authorisations? The EDPS does not see in the Proposal any instruments allowing the ETIAS Central Unit or ETIAS National Units to assess the hit based on ETIAS screening rules on its merits.

38. Similarly, the EDPS has doubts regarding the effectiveness of the right to appeal exercised by an applicant, when the authorisation is refused following a match with a profile. In order to provide an applicant with a true legal remedy, the Member State in charge of this procedure would have to be able to know and understand the rationale behind the risks' recognition. The applicant whose authorisation has been denied would also need to understand this decision in order to have a chance to have it overturned by an appeal body.

Risk of discrimination

39. The Proposal prohibits establishing the specific risk indicators based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, sexual life or sexual orientation. This may however not entirely reduce the risk of discrimination based on such criteria. According to Article 28(4), the data used for establishing the specific risk indicators will encompass, among others, current nationality, country and city of residence of an applicant, as well as sex and current occupation.

40. The EDPS would like to point out that, although the risk indicators will not be directly established with the use of such criteria, the outcome might in fact be very similar as if they were used. Information such as nationality and a place of residence, especially while combined with other data, may allow for making a reasonable assumption of the applicant's race or ethnic origin. Similarly, the risk indicators cannot be based on the trade union membership, but they might be established on the information concerning current occupation. These types of information are very closely linked, and therefore profiling on such basis would not truly prevent the risk of discrimination.

41. For all the reasons explained above, **the EDPS calls on the legislator to demonstrate the necessity and proportionality of the profiling in a thorough data protection impact assessment.**

4. Health data

42. One of the objectives of ETIAS is to assess whether a visa-exempt third country national may pose a public health risk prior to his/her arrival in the Member State. For this purpose, applicants for a travel authorisation will have to answer background questions related to their health when filling in their request through ETIAS. Article 15(4)(a) provides that any applicant would be asked whether he or she is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases. The content and format of these questions must be determined later on by the Commission by delegated acts. The only data relevant for public health purposes stored in ETIAS are the "yes" or "no" answers to the background questions related to health. A "yes" answer to any of the background questions would trigger a manual follow-up of the application and require the provision of additional information from the applicant.

43. Data concerning health are particularly sensitive data that deserve a higher level of protection[20].

44. The EDPS welcomes that consultation of health data in ETIAS has been limited in the Proposal in such a way that they could not be accessed for law enforcement purposes, neither by national law enforcement authorities (Article 45(2)), nor by Europol (Article 25(3)). However, the EDPS questions the added value of processing and collecting health data through the ETIAS system for the purpose of contributing to the protection of public health in the EU as provided for in the objectives of the Proposal (Articles 1 and 4).

45. Health data will be collected directly from the traveller without any possibility to check the accuracy of these data. Even if the applicant has answered truthfully to the questions

related to his or her health, the ETIAS authorisation would be valid for 5 years and for multiple travels, while a person's health situation is reasonably expected to change during such a period of time and there is no possibility for the applicant to modify the data submitted in the online application form. Therefore the health data stored could become outdated and irrelevant to serve the public health purposes.

46. In this regard, the 2016 Feasibility Study provides that, while public health risks (*e.g.* the elimination of tuberculosis) have recently been highlighted as a priority for the EU, there is a limited link between achieving this goal and collecting health information from all visa-exempt third country nationals[21]. In fact, the Study explains that the countries concerned by those risks are those with which the EU is only in the process of negotiating visa liberalisation agreements. This also brings the EDPS to question the relevance and efficiency of using ETIAS as currently proposed to contribute to the protection of public health.

47. Recital 48 to the Proposal provides that the ETIAS system will be interoperable with existing systems, such as for instance the SIS, the VIS or ECRIS in order to assess the security, irregular migration or public health risk that could be posed by visa-exempt travellers to allow cross-reference between those systems. However, none of these systems concerns health issues and are therefore irrelevant to serve the public health purposes of ETIAS.

48. The EDPS doubts that the processing of this particularly sensitive category of data on such a large-scale and for this period of time would meet the conditions laid down in Article 52(1) of the Charter and accordingly be considered as necessary and proportionate.

49. **The EDPS questions the relevance of collecting and processing health data as envisaged in the Proposal due to the lack of their reliability and the necessity to process such data due to the limited link between health risks and visa-exempt travellers.**

5. Access by law enforcement authorities

50. The Proposal envisages from the outset access by national law enforcement authorities and Europol to ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences (Article 1(2)).

51. Granting access to ETIAS for law enforcement purposes would fit into a general trend observed in the EU in the past years of granting these authorities access to large-scale IT systems for borders and migration - similarly to Eurodac and VIS and the proposed EES and ECRIS[22]. Access to existing and future EU databases by law enforcement authorities and Europol should not become the principle, but rather be allowed in limited cases where the need and proportionality of granting such access is fully justified and demonstrated.

52. The EDPS considers that access to ETIAS for law enforcement purposes should only be provided for in the Proposal on the condition that such access be proven necessary and proportionate.

53. In the Explanatory Memorandum, the Commission provides that "*it is imperative that competent law enforcement authorities, have access to relevant and clearly defined information in ETIAS, when this is necessary to prevent, detect and investigate terrorist offences or other serious criminal offences*"[23].

54. However, the Commission does not mention the future EES that would contain information on all third country nationals -both visa-required and visa-exempt travellers- entering the Schengen Area and would also be accessible to law enforcement authorities. The dataset stored in the EES would be almost similar to the dataset of the VIS (except for data related to the visa itself, *e.g.* the visa sticker)[24] and complements this information by adding records of entries and exits of all travellers. The EES would thus be able to offer at least the same level of information on visa-exempt third country nationals to law enforcement authorities as the VIS for visa-required third country nationals. The EU PNR will also be accessible to law enforcement authorities and Europol and contain further information on all air passengers, whether or not they detain a visa.

55. Furthermore, the Commission refers to the VIS as an example of system for which access for law enforcement purposes has proven effective. The Commission supports this statement by referring to the fact that *"Access to data contained in the Visa Information System (VIS) for law enforcement purpose has already proven effective in helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. The Visa Information System, however, does not contain data on visa-exempt third-country nationals"*[25]. The EDPS points out that "effective" is not the same as "necessary" in terms of data protection[26]. Furthermore, the Report on the evaluation of the VIS system released by the Commission late 2016, concludes that its evaluation as regards law enforcement access *"remain fragmentary and inconclusive"*[27].

56. Given the above considerations, **at this stage the EDPS recalls the need to provide convincing evidence supporting the necessity of making ETIAS data available to national law enforcement authorities and Europol. The EDPS recalls that necessity and proportionality of new schemes are to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, and specifically, in the specific case of the third country nationals concerned who are legally visiting and entering the EU**[28].

IV. ADDITIONAL RECOMMENDATIONS

1. Data quality and data minimisation

57. The EDPS recalls that according to the data quality and data minimisation principles, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

Relevance of the data collected from the applicant

58. Article 15 of the Proposal lists the data on the applicant that will be collected through the application form. The 2016 Feasibility Study on ETIAS explains that there will be maximum 26 data fields in the ETIAS application form to be filled, instead of 44 as it is

in case of visa application[29]. Nonetheless, the EDPS notes that, these numbers are hardly comparable, because according to the Proposal, all collected data (including health and judicial data) will eventually be centralised and stored in ETIAS. Therefore, in practice, more data will be stored in ETIAS than in the VIS.

59. Regarding the specific types of data collected in ETIAS, the EDPS would like to reiterate that there is a need for an in-depth assessment of necessity of each type of data processed for the purposes foreseen in the Proposal. The EDPS fails to consider all types of data listed in Article 15 of the Proposal necessary for the security, migration or public health purposes. Hence, he insists on the need for justification in this respect, with the special attention paid to data such as for instance education of the applicant, current occupation or IP address.

60. In addition, the EDPS notes that while the watchlist established by Europol will be based on terrorist offences and other serious criminal offences (Article 29), the background questions the applicant has to answer to refer to the conviction of *any* criminal offence in any country (Article 15(4)). The EDPS considers that a number of offences (*e.g.* traffic offences subject to criminal sanctions) would a priori not be relevant for the purposes of ETIAS. **He recommends that the information collected in relation to criminal offences should be strictly limited to terrorist offences and serious criminal offences as defined in Article 3 (1) (l) and (m) of the Proposal** (*i.e.* the offences which correspond or are equivalent to those referred to Articles 2(2) of Framework Decision 2002/584/JHA, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years).

Relevance of information collected from other systems

61. The Proposal sets up a system that will be interoperable with other police, judicial and immigration systems in order to cross-check information contained in ETIAS against information recorded in these systems. The EDPS notes that cross-checking data available in ETIAS with all information contained in other systems may not be relevant for the ETIAS purposes. For instance, the EDPS questions how an alert in the SIS on persons sought to assist in a judicial procedure as witness would be relevant to address immigration, security or health risks. Similarly, not all criminal offences for which the applicant have been convicted and that are stored in the ECRIS system are relevant for the purposes of ETIAS. **The EDPS therefore recommends to define precisely which information in other systems is relevant to the purposes of ETIAS and to strictly limit the cross-check of ETIAS data with this information.**

2. Data retention

62. Article 47(1) of the Proposal foresees that each ETIAS application file will be stored in the system:

a) for the validity period of the granted authorisation,
b) for the following five years from the last entry record of the applicant stored in the EES, or
c) for the following five years from the last decision to refuse, revoke or annul the travel authorisation.

63. When choosing the data retention period, EU data protection standards call for a period of time as short as possible in relation to the purpose pursued[30].

Five years of the validity period

64. The EDPS takes note of the five-year period of validity of ETIAS authorisations (Article 30(2)). The period of validity chosen for ETIAS authorisations will directly impact the retention period of personal data stored in the system.

65. The 2016 Feasibility Study argues that *"Convenience for travellers advocates for the longest period possible"* and mentions that *"costs and workload related to application management would also benefit from the longest period possible"*[31]. However, the advantages of a long validity period would be counterbalanced by the fact that *"with time, the risk assessment performed after the application is submitted loses relevance as the person's situation may change"*. The Study concluded that a validity period from two to five years would be the most appropriate solution.

66. The EDPS questions the choice by the Commission of the longest period of five years envisaged by the 2016 Feasibility Study instead of a shorter one.

Five years from the last entry record

67. In the majority of cases[32], the data retention period for ETIAS would in practice match the one of the EES - in accordance with point b) of Article 47(1).

68. According to the Explanatory Memorandum to the Proposal, the Commission wants to ensure *"that both the entry record and the related travel authorisation are kept for the same duration"*[33] to allow that each entry of a visa-exempt third country national in the Schengen Area will be linked to a travel authorisation in ETIAS and a corresponding entry record in the EES.

69. The EDPS considers that the fact that the proposed retention period for ETIAS data would be aligned on and coherent with the retention period of the EES -which is itself aligned on the retention period of the VIS- does not *per se* justify this choice[34].

Five years from refusal, revocation or annulment

70. The EDPS does not see the need to keep the denied, revoked or annulled ETIAS application for a period of time as long as five years - in accordance with point c) of Article 47(1).

Other comments

71. Should the need for the three above-mentioned data retention periods be demonstrated, the EDPS points out that, if the intention of the Commission is indeed to maintain a link between the travel authorisation in ETIAS and the related entry record in EES, it is not clear from point b) of Article 47(1) that the starting point of the five-year retention period for ETIAS application files is the last entry record registered in the EES on the basis of the *corresponding* travel authorisation.

72. Furthermore, the EDPS wonders what would be the added value of keeping the content of the whole ETIAS application file beyond the validity period of the travel authorisation and for as long as the corresponding entry record. The sole information of the status of the application file (*i.e.* "granted" or "denied") and not the content of the whole application file could be sufficient for the purposes of the EES.

73. The EDPS also wonders what would be the added value of storing "yes" and "no" answers to the background questions for such long periods of time. In addition to the fact that ETIAS data are of lower reliability given that they are purely declarative and collected from the applicants, answers to the very same background questions might truly change over the course of five years.

74. **The EDPS asks the legislator to better justify the chosen data retention periods in Article 47(1) (a), (b) and (c) so as to ensure that storage of ETIAS data will be limited to what is strictly necessary for the purposes of the system. The EDPS also recommends setting different data retention periods for the different categories of data stored.**

3. Interactions with other information systems

75. The EDPS notes that ETIAS would be interoperable with other police, judicial and immigration systems. The EDPS stresses that each of these systems has been created for a specific purpose which may not be compatible with the purpose of ETIAS. As an example, the purpose of the Eurodac system is to assist in determining which Member State is to be responsible for examining an application for international protection and to facilitate the application of the Dublin Regulation[35]. It is not intended to assist in identifying immigration risks. Similarly, the pending Proposals to amend the legal basis of existing systems (*i.e.* Eurodac, SIS II, ECRIS) or to create new ones (*i.e.* the EES) also provide for specific purposes which may differ from the purposes of the ETIAS system. In particular, the EDPS understands that the objectives of an ECRIS including convictions on third country nationals is to assist and provide judges and prosecutors with easy access to information on the criminal history of persons concerned.

76. **The EDPS is not aware of any compatibility assessment in-between the respective purposes of the systems referred to in the Proposal and the stated purposes of the proposed ETIAS. He stresses that following the outcome of the assessment, changes in legal bases of the other systems as well as additional conditions may be required. He considers that, before considering the access to and the use of data collected and processed in other systems, such an assessment is essential.**

4. Data subject rights and remedies

77. The EDPS welcomes the possibility for data subjects to appeal the refusal of a travel authorisation, enabling them to file actions in the Member State that took the decision and in accordance with the national law of that country (Article 31).

78. However, the EDPS considers that some of the grounds for refusal listed in Article 31(1) are as such not straightforward enough, *e.g.* the applicant *"(b) poses an irregular*

migration risk" or *"(c) poses a security risk"*. The applicant should receive sufficiently clear indication of the ground(s) for refusal in order to efficiently exercise his appeal and contest the reasons for the refusal. **The EDPS recommends further specifying the information to be provided to applicants in case of a refusal of authorisation, notably if the refusal is due to a hit with any another IT system.** This would also allow the applicant to know for which system he should exercise his rights of access to personal data concerning him in that system, and possibly his rights of rectification and/or deletion in case an error has been found or his data have been processed unlawfully.

79. The same should apply accordingly in case the ETIAS authorisation has originally been granted and is later annulled or revoked (Articles 34 and 35).

5. Independent review of the conditions for access

80. Should the need and proportionality of using ETIAS as a law enforcement tool be demonstrated, the conditions of such access would then have to be strictly regulated. The EDPS takes note of the conditions for such access to ETIAS data in Article 45 of the Proposal. The EDPS welcomes Recital 35 of the Proposal which provides that access request to ETIAS data by law enforcement authorities will *"be subject to a prior review by a court or by an authority providing guarantee of full independence and impartiality"*. **The EDPS considers that such a prior independent review is of utmost importance and recommends to specifically mention it in Article 45.**

81. However, the EDPS considers that Article 44(2) creates a certain ambiguity. On the one hand, Article 44(2) provides that Member States will have to ensure that law enforcement authorities' requests for access undergo an efficient and timely verification that the conditions of Article 45 are fulfilled in accordance with their national law and procedural law. Article 44(3) then says that, if the conditions referred to in Article 45 are fulfilled, the central access point will have to process these requests and transmit the data. On the other hand, Recital 37 of the Proposal provides that ETIAS National Units should act as the central access point and should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.

82. Read together with Recital 35, Article 44(2) suggests that there will be another actor involved, *i.e.* a court or an [other] independent and impartial authority, that will verify the fulfilment of the conditions in-between the transmission of the request to the central access point and the processing of the request by the central access point if the conditions of Article 45 are met. On the contrary, Recital 37 clearly assigns this role to ETIAS National Units acting as central access points. **The EDPS therefore recommends clarifying the procedure for access.**

6. Division of roles and responsibilities

83. In data protection legislation, the term "controller" refers to the entity that defines the purposes and means of the processing. Where the purposes and means of the processing are determined by law, the law may also include (the criteria for) designating the controller.

84. The division of roles and responsibilities as regards the proposed ETIAS system is quite complex and the EDPS appreciates the effort to clearly delineate them in the Proposal. The EBCG Agency will be controller, while eu-LISA will be processor (Articles 50 and 51). The Proposal also provides that eu-LISA will be in charge of the development of the whole system and will be responsible for its security. According to the Proposal, it appears that eu-LISA will carry out these roles without the EBCG Agency's involvement.

85. While of course the purposes (and to a certain extent the means) for ETIAS are defined in the Proposal, the controller is accountable for implementing appropriate technical and organisational measures to ensure that the processing is carried out in accordance with data protection rules, as well as should be able to demonstrate that this is the case (*e.g.* providing evidence that information security is properly managed).

86. With the distribution of roles as included in the Proposal, the EBCG Agency could find itself in a position where it could be held accountable (as controller) for matters being outside of the scope of its influence (*e.g.* how eu-LISA manages information security in ETIAS), as they are exclusively allocated to eu-LISA.

87. **The EDPS recommends a more accurate description of the division of roles between the EBCG Agency and eu-LISA by considering, where appropriate, their designation as joint controllers[36].**

7. Prior verification of Europol requests of access by the EDPS

88. Under certain conditions, ETIAS data would be accessible to law enforcement authorities. Article 44(2) of the Proposal provides that Member States shall ensure *"that according to [their] national law and procedural law a request for consultation undergoes an independent, efficient and timely verification"*. The Explanatory Memorandum clarifies that this refers to verification by *"a court or by an authority providing guarantees of full independence and impartiality"*[37].

89. According to Article 46 of the Proposal, Europol shall also have access to ETIAS data under similar conditions as national law enforcement authorities (*e.g.* the consultation is necessary in a specific case, other databases have yielded no results, etc). Similarly to access by national law enforcement authorities, access by Europol is subject to prior verification, assigned to the EDPS in the Proposal, *"where appropriate in accordance with the procedure of Article 44 of Regulation (EU) 2016/794"*.

90. Most importantly, the EDPS is not a functional counterpart to the authorities in charge of authorising access on the national level. On the national level, the verifying authorities would be courts or other similar authorities (depending on the national legal system: investigating judges, public prosecutors, etc). It is true that there currently is no clear equivalent on the European level - the European Court of Justice does not have such a role in authorising individual investigative measures and the European Public Prosecutor is not established yet (and is likely to have a different remit than Europol). The role of the EDPS is to monitor and check compliance with data protection rules, not to authorise individual investigative activities. The EDPS has recommended that verifying authorities be independent of the authority whose activities they authorise[38], but it does not follow that the EDPS should be the verifying authority.

91. Furthermore, under the procedure of Article 44 of Regulation (EU) 2016/794[39] on Europol, if a case concerns data originating from a Member State, the EDPS has to consult that Member State's Data Protection Authority ('DPA') before taking a decision. In the case of a revoked or annulled travel authorisation (decision taken by an ETIAS National Unit), the data can be considered to fall under this provision. In such consultations, the EDPS can set the deadline for the Member State's DPA to reply between one and three months[40]. In "extremely urgent"[41] situations, the EDPS can take immediate action and inform the concerned DPA afterwards, justifying the urgency as well as the action taken. This appears to be intended to be an exceptional situation, and not as standard operating procedure. While the Proposal does not define or detail what is to be understood by *"efficient and timely"* prior verification (Article 46(3)), it appears that the timescales expected are significantly shorter than what the procedure under Article 44 of Regulation (EU) 2016/794 is capable of delivering. As currently drafted, the procedure could thus put the EDPS in a position where it legally cannot deliver what he is requested.

92. **For the reasons mentioned above, the EDPS recommends to designate an independent verifying authority other than the EDPS.**

8. Verification by the ETIAS Central Unit

93. Two aspects of ETIAS are not described in enough detail neither in the Proposal nor in the Explanatory Memorandum: the kind of searches to be performed on other information systems and the way they would be performed; and the kind and amount of information to be contained in a hit. According to Article 3(1)(k) of the Proposal, *hit* means "*the existence of a correspondence established by comparing the personal data recorded in an application file of the ETIAS Central System with the personal data stored in a record [...] in an information system queried by the ETIAS Central System [...]*". From this definition, the hit can be understood as purely a *Boolean* field which only possible values are *true* or *false*. In relation to how the searches are going to be performed, the EDPS understands from Article 19(3) that they will provide *inconclusive* answers as to the identification of the applicant[42]. In case there are inconclusive searches associated with an application, the ETIAS Central Unit is supposed to have the capacity to "*verify whether the data recorded in the application file corresponds to the data present in one of the consulted information systems/databases [...]*"[43].

94. However, how can the ETIAS Central Unit perform that verification when the only information available to the ETIAS Central Unit is the application file and the hit/no-hit information? There are only two possibilities: a *hit* will contain in reality more information that what is right now in the current Proposal exposing the information in the systems interconnected to ETIAS to the different parties involved in any checking, *i.e.* the ETIAS Central Unit and ETIAS National Units (which may or may not have a legal basis for accessing that kind of information); or ETIAS Central Unit and ETIAS National Units are supposed to have access to all the information systems the ETIAS will be querying. Both scenarios require a revision of both the ETIAS Proposal but also of the legal texts of all the systems accessed by ETIAS.

95. **The EDPS recommends clarifying how the verification by the ETIAS Central Unit can be performed. Once this is clear, the legislator should introduce any required changes in the Proposal so that (a) the access by the ETIAS Central Unit to the**

information required to verify the applications is completely specified and/or (b) eliminating the role of the ETIAS Central Unit as verifier of *inconclusive* applications.

9. Architecture and information security

96. With so many different entities accessing the data, and the ETIAS Central System accessing so many others, the coordination of information security is of paramount importance as any of the information systems or entities involved will be as secure as the weakest link. Also, proper information security can only be achieved through a proper analysis of the information security risks the information system is subject to. Even if the information security measures contained in the Proposal could be considered as a minimum baseline, the EDPS stress the importance of performing a proper information security risk management as mandated by Article 22 of Regulation (EC) No 45/2001, also mentioned in Article 52 of the Proposal.

97. ETIAS would introduce a fundamental change to the current architecture of large scale IT systems hosted and managed by eu-LISA: from a closed environment accessible only to Member States and, maybe, some other European Union entities, a door will now be opened to the whole internet[44]. The information security consequences of such a decision cannot be underestimated and a proper analysis needs to be mandated, performed and revised. Also, no systems before have shared infrastructure like it is proposed to do with ETIAS and EES: again this kind of architectural technical decision needs to be very well thought and documentary supported and a specific analysis of the risks of any solution needs to be envisioned and performed by eu-LISA.

98. Furthermore, the Proposal is very detailed regarding the architecture of the system, limiting the technical choices that may be adopted when analysing and defining the technical solution(s). The proposed regulation should not mandate any specific architectural decision unless it has impacts on other parts of the regulation but it should mandate a proper data protection and security analysis to guide the development of the system.

99. Finally, Article 63 of the Proposal describes the development and operational management responsibilities for the ETIAS system. However, there are not any mentions of data protection or security: Any new system, and any major change to an existing system (in this case not just one but EES, VIS, *the Europol data*, SIS, Eurodac and ECRIS[45]) can only be professionally achieved by: (1) following a proper security process which includes a detailed analysis of the information security risks, and (2) following data protection by design and by default principles.

100. Moreover, the Proposal charges the Commission to "*adopt detailed rules [...] on the data protection and security rules applicable [...]. Those implementing measures shall be adopted in accordance with the examination procedure referred to in Article 79(2)*", *e.g.* concerning the public website and the mobile app for mobile devices[46], access to data for verification by carriers[47] or regarding the use of data for reporting and statistics[48]. In all those cases, the Proposal should impose the need to base those *detailed rules* on data protection and security on information security risk management and data protection by design and by default, respectively.

101. **The EDPS recommends adding the obligation to perform and maintain an information security risk assessment and to follow the principles of data protection by design and by default to Article 63.**

102. Concerning those articles mandating the Commission to adopt detailed rules on data protection and security rules (Articles 14, 39, 40 and 73), **the EDPS recommends adding in those articles the need to consider information security risk management and data protection by design and by default.**

103. **Also, the EDPS recommends changing Article 6 to only mention those elements really needed to the proposed regulation, and leave to eu-LISA and the rest of the stakeholders involved to devise the final architecture of the ETIAS system.**

104. Albeit the EBCG Agency is assigned the role of *controller* by the Proposal in Article 50, it is not assigned any responsibility concerning the security of the processing. However, as a controller is indeed responsible for the security of the processing operation[49]. Even if eu-LISA[50] were to provide all security analysis and measures and assume most or all of the security responsibilities for the ETIAS system, the EBCG Agency should still be responsible for the processing of personal data done by the ETIAS Central Unit.

105. **The EDPS recommends changing Article 52 and/or Article 65 to recognise the EBCG Agency's responsibility concerning information security.**

10. Statistics

106. The EDPS understands the need for the duly authorised staff of the competent authorities of the Member States, the Commission, eu-LISA and the ETIAS Central Unit to produce reporting and statistics on the data contained in the ETIAS. However, the amount of data that may be accessed may allow for identification of individuals, contrary to what is stated in Article 73 of the Proposal. For example, the combination of nationality, gender and date of birth of a third country national may lead to identification.

107. **The EDPS therefore recommends a redrafting of Article 73 recognising that the data listed under Article 73(1), points (a) to (i) may lead to identification of individuals and thus must be protected in a similar way as the rest of the ETIAS.** This includes performing a proper information security risk assessment, and implementing adequate security measures, prior to providing this additional central repository.

108. The EDPS strongly cautions that the current proposed solution for providing statistics would impose a heavy burden on eu-LISA, which would have to maintain and secure appropriately a second repository, and on the EDPS which would have to supervise this second repository. The EDPS would favour a solution which does not require an additional central repository but rather requires eu-LISA to develop functionalities that would allow the Member States, the Commission, eu-LISA and the ETIAS Central Unit to automatically extract the required statistics directly from the ETIAS Central System, without the need for an additional repository.

109. However, if a different repository is implemented, and in line with the expressed willingness to use anonymous information, the Proposal could explore the possibility to implement some kind of privacy enhancing technology like *remote data access* and *differential privacy* so as to indeed allow the processing of personal data without actually accessing it.

110. Finally, contrary to other regulations concerning large scale IT systems, there is no obligation to make the year statistics public in Article 73.

11. Role of the EDPS

111. The EDPS is the data protection authority supervising both eu-LISA and the EBCG Agency[51]. While the EDPS has the power to obtain all relevant information for the performance of his tasks from EU institutions, bodies and agencies[52], the process should be streamlined by including the EDPS in the list of recipients of the reports that eu-LISA or the ETIAS Central Unit will present to the Commission, the Council or the European Parliament[53].

112. Furthermore, **the EDPS recommends that a similar provision to Article 56(2) be added to Article 57 so that the EDPS be allocated the resources necessary to perform an adequate supervision of this new system.**

V. CONCLUSION

113. The EDPS welcomes the attention paid to data protection throughout the Proposal for the establishment of ETIAS.

114. In full respect for the role of the legislator in assessing the necessity and the proportionality of the proposed measures, the EDPS recalls that these two high-level legal requirements enshrined by the Charter can be scrutinised by the Court of Justice of the EU and that the EDPS is tasked with safeguarding them. He underlines that the lack of a (data protection) impact assessment does not make it possible to assess the necessity and proportionality of ETIAS as it is currently proposed.

115. Since the Proposal establishes an additional system involving the processing of a significant amount of personal data of third country nationals for immigration and security objectives, the EDPS advises the legislator to take a stock tacking exercise of all EU-level measures involving data processing for migration and security objectives and to conduct an in-depth analysis in terms of theirs goals and achievements.

116. In this context, the EDPS recommends to include a definition of irregular migration risks and security risks in the Proposal to comply with the purpose limitation principle.

117. Furthermore, the EDPS is concerned whether the use of the ETIAS screening rules will be fully in line with the fundamental rights enshrined in the Charter. He recommends that the proposed ETIAS screening rules be subject to a prior comprehensive assessment of their

impact on fundamental rights. He also wonders whether convincing evidence supports the necessity of using profiling tools for the purposes of ETIAS and, *quod non*, encourages the legislator to reconsider the use of profiling.

118. The EDPS questions the relevance and the efficiency of the collection and processing of health data as envisaged in the Proposal due to the lack of their reliability. He also wonders about the necessity to process such data due to the limited link between health risks and visa-exempt travellers.

119. As regards law enforcement and Europol access to ETIAS data, the EDPS stresses that convincing evidence supporting the necessity of such access is today missing. The EDPS recalls that necessity and proportionality of new schemes are to be assessed both globally, taking into consideration the already existing large-scale IT systems in the EU, and specifically, in the specific case of the third country nationals concerned who are legally visiting and entering the EU.

120. In addition to the main concerns identified above, the recommendations of the EDPS in the present opinion relate to the following aspects of the Proposal:
- the necessity and proportionality of the set of data collected,
- the chosen data retention periods,
- the interoperability of ETIAS with other IT systems,
- the data subjects' rights and provided remedies,
- the independent review of the conditions for access by law enforcement authorities,
- the division of roles and responsibility between the EBCG Agency and eu-LISA,
- the verification by the ETIAS Central Unit,
- the architecture and information security of the ETIAS,
- the statistics generated by the system, and
- the role of the EDPS.

121. The EDPS remains available to provide further advice on the Proposal, also in relation to any delegated or implementing act adopted pursuant to the proposed Regulation, which might have an impact on the processing of personal data.

Brussels, 6 March 2017

Giovanni BUTTARELLI
European Data Protection Supervisor

[1] O.J. L 281, 23.11.1995, p. 31.
[2] O.J. L 8, 12.1.2001, p. 1.
[3] O.J. L 350, 30.12.2008, p. 60.
[4] Communication of 13 February 2008 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Preparing the next steps in border management in the European Union", COM(2008) 69 final.
[5] Preliminary Comments of the EDPS of 3 March 2008, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.
[6] Policy study on an EU Electronic System for travel Authorization (EU ESTA) of February 2011, available at: http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/esta_annexes_en.pdf.
[7] Communication of 25 October 2011 from the Commission to the European Parliament and the Council "Smart borders - Options and the way ahead", COM(2011) 680 final.
[8] Communication of 6 April 2016 from the Commission to the European Parliament and the Council "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final.
[9] Feasibility Study of 16 November 2016 for a European Travel Information and Authorisation System (ETIAS) - Final Report available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf.
[10] 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, O.J. L 119, 04.05.2016, p. 1.
[11] 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, repealing Council Framework Decision 2008/977/JHA, O.J. L 119, 04.05.2016, p. 89.
[12] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, O.J. L 218, 13.08.2008, p. 129; Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), O.J. L 180, 29.06.2013, p. 1.
[13] Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM (2015) 671 final.
[14] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, O.J. L 251, 16.9.2016, p. 1–76.
[15] Including for instance hit/no hit information and answers to background questions on health, criminal convictions, stay in a specific war or conflict zone.
[16] Article 3(1) of the Proposal defines public health risk as *"treath to public health as defined in Article 2(21) of (Regulation (EU) 2016/399", i.e. "any disease with epidemic potential as defined by the International Health Regulations of the World Health Organization and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the Member States".*
[17] See *supra* Chapter III, Section 2. Defining the objectives.
[18] See *e.g. Profiling the European Citizen. Cross-Disciplinary Perspectives*, eds. M. Hildebrandt, S. Gutwirth, Springer 2008, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles*

in Light of the United States Government's National Intelligence Data Mining Practices, L. Colonna, Stockholm 2016.

[19] There is only one minor exception for family members of EU citizens or of other third country nationals enjoying the right of free movement under Union law, see Article 21 of the Proposal.

[20] Health data are defined as *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"* under Article 15(4) of the General Data Protection Regulation . They fall under a stricter data protection regime applicable to special categories of data. Article 9 of the GDPR provides that, if processing of such data is necessary for reasons of substantial public interest, the Union or Member State law should provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[21] See 2016 Feasibility Study, *op. cit.*, Table 41, p. 131.

[22] EDPS Opinion of 7 October 2009 on the Law Enforcement Authorities access to Eurodac, point 18; EDPS Opinion of 18 July 2013 on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), point 68; EDPS Formal comments of 3 November 2015 on the European Commission Public Consultation on smart borders, p. 5; EDPS Opinion 06/2016 on the Second EU Smart Borders Package, point 76.

[23] Explanatory Memorandum, p. 11.

[24] See Article 5 and Articles 9 to 14 of the Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States onshort-stay visas (VIS Regulation), O.J. L 218, 13.8.2008, p. 60-81.

[25] Explanatory Memorandum, p. 11.

[26] The ECtHR found that the notion of necessity does not have the flexibility of expressions such as "admissible", "ordinary" or "useful", but that it "implies a pressing social need"; see ECtHR, Handyside vs United Kingdom, 7 December 1976, Application no. 5493/72, §48.

[27] Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 767/2008 establishing the Visa Information System, the use of fingerprints at external borders and the use of biometrics in the visa application procedure/REFIT Evaluation, p. 11.

[28] EDPS Opinion 06/2016 of 21 September 2016 on the Second EU Smart Borders Package, point 14.

[29] 2016 Feasibility Study, *op. cit.*, p. 156-158.

[30] See *e.g.* EDPS Opinion 06/2016 on the Second EU Smart Borders Package, point 28.

[31] See 2016 Feasibility Study, *op. cit.*, p. 15.

[32] The EDPS understands that the data retention period would only match the validity period of the travel authorisation - in accordance with point a) of Article 47(1) - in few (unlikely) cases in which there is no entry record in the EES linked to this authorisation. This would occur when a visa-exempt traveller has been granted an ETIAS authorisation but either has not used it during the validity period, or has entered the Schengen area on the same day as the ETIAS authorisation was granted, or has been denied entry in the Schengen area despite the granted authorisation.

[33] Explanatory Memorandum, p. 34.

[34] EDPS Opinion 06/2016 on the Second EU Smart Borders Package, point 29.

[35] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, O.J. L 180, 29.6.2013, p. 31.

[36] See Article 28 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by theUnion 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, COM(2017)8 final.

[37] Explanatory Memorandum, p. 12.

[38] EDPS Opinion 06/2016 on the Second EU Smart Borders Package, point 86; EDPS Opinion 7/2016 of 21 September 2016 on the First reform package on the Common European Asylum System, point 58.

[39] 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, O.J. L 135, 24.5.2016, p. 53–114.

[40] Regulation (EU) 2016/794, Article 44(4).

[41] *Ibid.*

[42] This may happen because hits are not based on exact matches but on similarities between the information of the application form and the information in the database searched, or because when searching by using several attributes from the application form, only some of them match the information in the database searched.

[43] Article 20 of the Proposal – Verification by the ETIAS Central Unit.
[44] Article 6 of the Proposal – Set up and technical architecture of the ETIAS Information System.
[45] All (those) listed in Article 10 of the Proposal – Interoperability with other information systems.
[46] Article 14 of the Proposal – The public website and mobile app for mobile devices.
[47] Article 39 of the Proposal – Access to data for verification by carriers.
[48] Article 73 of the Proposal – Use of data for reporting and statistics.
[49] In accordancce with Article 22 of Regulation (EC) No 45/2001.
[50] According to Article 23 of Regulation (EC) No 45/2001, eu-LISA would also need to comply with the obligations of the controller set out in Article 22: "*The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: (a) the processor shall act only on instructions from the controller; (b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor* [...]".
[51] This is reiterated in Article 49(1) of the Proposal, repeating that Regulation (EC) No 45/2001 apply to both eu-LISA and to the European Border and Coast Guard Agency, therefore, the EDPS is their supervisory authority concerning the processing of personal data.
[52] Article 47(2) of Regulation (EC) 45/2001; and the successor provision (Article 59(1)) is similar in the Proposal of 10 January 2017 for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by theUnion 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, COM(2017)8 final.
[53] To do this, the EDPS should be added as a recipient for the reports mentioned in the following Articles: 77(3), 78(4), 81(2), 81(4) and 81(5). Also, in Article 52(4), the EDPS should be informed of the measures eu-LISA takes pursuant to Article 52 not only for the start of the operations of the ETIAS but throughout the whole lifecycle of the ETIAS and its data.