APPENDIX

Already in its basic approach, the Working Party 29 (WP 29) finds that the proposal encounters considerable doubts. The envisaged storage of sensitive personal data from applications in a central repository, the automated comparison of these data with other information systems during the approval procedure, further automated comparisons during the retention period and access by security authorities are to be considered as interferences with the fundamental rights to privacy and data protection, as enshrined in Articles 7 and 8 of the European Charter of Fundamental Rights. These interferences require a sufficient legal basis. This legal basis must also justify that interference whilst pursuing legitimate objectives of general interest within the EU. As with existing relevant large-scale IT systems at EU level, the principle of proportionality must be maintained. In this regard, the WP 29 regrets, that the proposal is not accompanied by a comprehensive data protection impact assessment, which would allow for a full and proper assessment of the necessity and the proportionality of the ETIAS. The feasibility study that was conducted does not consider the different less intrusive options. The Working Party 29's opinion is that the following issues need to be addressed.

To begin with, there are considerable doubts as to whether the proposal will achieve the objectives referred to in Art. 4:

- An additional benefit to a high level of security brought by this proposal seems questionable. Border controls as foreseen in the Schengen Borders Code (SBC) already include a check of relevant alerts in the Schengen Information System II (SIS II) and relevant national data bases. The recent proposal for the introduction of an Entry-Exit-System (EES) accompanied by adaptions of the SBC foresees that future border procedures for third country nationals would include checks against the EES, the SIS II, the Interpol database on stolen and lost travel documents, national databases on stolen, misappropriated, lost and invalidated travel documents and if necessary a consultation of the VIS. Why the anticipation of this comparison should bring about any obvious increase in security is not evident in itself. There is also a lack of convincing examples for how the comparison with screening rules and the foreseen watch list should lead to any security-relevant hits at all. Persons travelling in bad faith are unlikely to provide sincere answers to background questions. The general reference to good experiences in other countries is not convincing at this point. Furthermore, at least with regard to air passengers, PNR-data will also be available in the future, after the PNR Directive has been implemented.

- The contribution to the prevention of irregular migration is unclear and unquantified. The assessment of migration risks requires information on the purpose, terms and duration of the intended stay in the Schengen area as well as the proof of sufficient financial means for the stay and return (such as in the visa procedure). The proposal

does not explain convincingly how it should be possible to make a viable assessment by means of the data set stored in ETIAS. The linking of the unverified data elements such as country of origin, educational level and professional occupation seems to be hardly sufficient and/or potentially discriminatory. There are discrepancies with the VISA procedures (namely, visa-free travellers having to provide more information than in visa application procedures e.g. regarding their educational level and current occupation) which are also difficult to understand in this regard.

- The relevant contribution to the protection of public health seems disproportionate. Information about the state of health is often subject to short-term changes and in order to serve its purpose effectively, it has to be accurate and updated in border controls at the time of entry, anyway, as foreseen in Art. 8 para. 3 lit. a, in combination with Art. 6 para. 1 lit. e SBC. Therefore there should be at least a shorter validity and retention period for health data or refusals based on health data.

- A facilitation of effective border checks by reducing refusals of entry at borders seems possible as to the extent that the conditions for issuing / refusing an ETIAS authorisation match the entry conditions of the SBC or are even stricter. However, if facilitation of borders controls is the main benefit of the proposed system, this raises questions regarding the necessity of the system in all its particulars (e.g. retention periods) and regarding possible alternatives for the facilitation of border controls.

- With a view to supporting the objectives of the SIS II, this is only assumed but not made clear for all categories of SIS II alerts. Some types of alerts (e.g. as witnesses in a judicial procedure) seem quite irrelevant for the ETIAS risk assessment. The relevant types of alerts (e.g. European arrest warrant), on the other hand, would be checked during border procedures at the latest and the added value of anticipating these checks is questionable. More detailed justification is required in order to explain why an earlier comparison of data is necessary and proportionate.

- The assumed contribution to the prevention, detection and investigation of terrorist or other serious criminal offences by law enforcement access to the ETIAS data is not yet justified convincingly. It has not been sufficiently explained which cases genuinely require this procedure. At this point, the general reference to the VIS as an important source of information for law enforcement authorities is not convincing. Specific situations which are not already covered by other sources of information are - also due to the lack of concrete examples - difficult to imagine. At this point, it must be assumed that the intention of the proposal is rather to establish a possibility of access as a "just in case" measure, which is similar to the possibility of access in the EES proposal.

In addition to the overall opinion, the following Articles have been assessed in detail:

Definitions (Art. 3)

The following terms should be taken up in the definitions: “security risk”, “irregular migration risk”, “carrier gateway” as well as “identity data”. Furthermore, the definition of “public health risk” should be clarified and narrowed down (e.g. to contagious illnesses). By not defining those terms or defining them too broadly, every ETIAS National Unit could use them in their own way, which would lead to a non-consistent application of the regulation.

Interoperability (Art. 10)

ETIAS is intended to perform an automated comparison of data with numerous systems, which were created for different purposes (Art. 18). At this point, the question arises to what extent and on what grounds the comparisons that shall be carried out go beyond the check of the entry conditions under the Schengen Borders Code. The comparison with the EES replaces, to that extent, the examination of the entry and exit stamps. (At this point, it is not intended to delve into fundamental concerns about the establishment of storage of the respective data in the EES instead of the previous on-the-spot-checks of the data only held by a person.) The extension to EURODAC and ECRIS requires a detailed explanation of the necessity in order to assess their suitability, and, in view of the involved change of purpose, this requires an appropriate balance between the objectives and the interferences with fundamental rights associated with the data comparison. In addition, the details concerning the modalities and the data that will actually be “necessary” are still lacking. Through the mixed purposes of ETIAS, the purpose limitation principle loses its essence.

Personal data of the applicant (Art. 15)

In principle, only data which are necessary for the respective purpose shall be collected. This data minimisation principle seems to have been ignored in particular with regard to the mandatory completion of the education level (Art. 15 para. 2 lit. h) and the current occupation fields (lit. i). These data are not even part of the application procedures for a Schengen visa (category C). Therefore it is questionable why visa-free travellers should be required to provide more information. As regards the current occupation field, this is easily subject to changes and does not constitute a secure indicator of the risks to be assessed. Therefore the mandatory fields on educational level and current occupation seem to be disproportionate and should be erased.

Furthermore, the domestic permanent residence address should rather be an obligatory field than an optional field, which results in a hit when not filled in (see Art. 18 para. 3).

In addition, we ask ourselves, whether it is really necessary to require an application with an electronic signature. This provision could be potentially restrictive, especially for applicants from less developed countries.

Another discrepancy to the visa procedure relates to the background questions, which partly go beyond the respective questions in the Schengen visa procedure. Again, there is a lack of sufficient justification as to why visa-free travellers should be asked to provide in advance more background data than travellers requiring a visa. We wonder if this is still proportionate with regard to conceded visa liberalisation. Previously, it was up to the border officials' discretion to ask further questions when a person entered a country. The extent to which a systematic advanced questioning is suitable, necessary and proportionate in the strict sense has neither been convincingly explained yet, nor been apparent.

Regarding background questions on criminal convictions, there needs to be a limitation as to which criminal offences need to be declared. These offenses should have a strong link to ETIAS purposes like terrorist or other serious offences. Furthermore there needs to be some kind of time limit regarding which 'spent' convictions are necessary to declare.

In addition, whenever an application is made, the IP-address from which the application has been submitted is stored automatically. This leads to numerous additional possibilities for comparisons and access. The IP address is allowed as a single search criterion for police authorities, as well as an admissible single criterion for systematic comparison by means of the watchlist. However, the facilitation of searches on its own is not a sufficient reason for the need and necessity and could lead to erroneous hits.

A special regime should be foreseen for sensitive data, like health data. In any case, further restrictions should be placed on the processing of sensitive personal data and different retention periods should be foreseen for each category of personal data.

<u>Screening rules and profiling (Art. 28)</u>

The screening rules are algorithms allowing a comparison between the data stored in ETIAS with certain risk indicators. These risks shall be determined on the following basis:

- Statistics generated by the EES indicating abnormal rates of overstayers and refusals of entry for a "specific group of travellers",
- Statistics generated by the ETIAS indicating abnormal rates of refusals of travel authorisations for a "specific group of travellers",
- Statistics generated by the ETIAS indicating correlations between information collected through the application form and overstay or refusals of entry,
- Information from the MS on certain risk indicators,
- Information from the MS on abnormal rates of overstayers or refusals of entry,
- Information on specific public health risks.

On this basis the ETIAS Central Unit is intended to describe specific risk indicators by combining different characteristics such as age, sex, nationality, place of residence, educational level or current employment. Thereby, the specific risk indicators are to be targeted and proportionate. In our view, the latter does not seem to be possible according to the aforementioned provisions, as these are much too vague. How exactly can the ETIAS Screening Board, by using the catalogue of characteristics available in the ETIAS, describe "certain categories of travellers" having unusually high rates of refusal of entry or overstays? There is a risk that there is no possibility to describe sufficiently targeted patterns and that whole groups of persons are generally refused as a precautionary measure. The fact that an application can be rejected on the basis of screening rules, based on statistics and information from the Member States, could be questionable from a fundamental right protection point of view as it might lead to mass discrimination.

Whether being able to describe sufficiently targeted patterns or not, it is in any case the objective of the ETIAS screening rules to single out applicants who pose irregular migration, security or public health risks by the use of targeted algorithms. And the ultimate objective is to prevent them from entering the territory of the Member States i.e. the processing might result in negative consequences for the individual. This constitutes profiling in our view. It should be labelled as such explicitly and be provided with all the necessary safeguards.
With regard to the non-discrimination rule, we wonder why, in so far as the same grounds of discrimination are mentioned as in Art. 12, not the same terminology is used (eg race or ethnic origin versus racial or ethnic origin, religions or philosophical beliefs versus religion). The formulation should be aligned with the usual formulation of non-discrimination rules, such as Art. 14 of the ECHR or Art. 21 (1) of the EU Charter of Fundamental Rights. Moreover, the ground "trade-union membership" seems to be somewhat unusual or unimportant in relation to the other possible grounds for discrimination. Concerning lit. f we ask ourselves whether self-declarations can actually provide an added value with a view to the protection of public health.

<u>ETIAS watchlist (Art. 29)</u>

The necessity of the ETIAS watchlist remains unclear, and the WP29 would urge the Commission to be specific on the legal basis for this watchlist. We assume that information on internationally wanted war criminals as well as terrorist or other serious offences or equivalent risks can already be found in the available police information systems which are to be checked anyway. It is not evident who else shall be listed especially for the ETIAS. At present, a need for a particular ETIAS watchlist is not apparent. Rather, the possibility to compare a single piece of personal data with the whole ETIAS data store is opened up. This also applies to a pure check of IP addresses which can be on the watchlist without any additional information (see Art. 29 para. 3).

Refusal of a travel authorisation (Art. 31)

If the applicant has not provided any supplementary information within the required seven days (Art. 23, para. 2), which appears to be a short deadline (especially for the health data proof), this should not yet be a final ground for refusal. A possibility of subsequent provision of information, of restitutio in integrum, or similar means should be opened up or the proceedings should be suspended.

Furthermore, Article 31 para. 1 simply states that the national authority has to indicate the reason for the refusal of the permit (the risk of irregular migration, security risk, etc.). An efficient system of redress requires, however, a clear indication on the refusal as to what information or which data in the system are the reasons for the rejection.

Revocation of a travel authorisation (Art. 35)

Under Art. 35 para. 3 each new refusal of entry alert or each new entry on stolen/lost travel documents in the SIS II, as well as each change of the ETIAS watchlist leads to an automated check of all data records stored in ETIAS. In the event of a hit, the ETIAS National Unit, which has granted the authorisation, will automatically be notified and it will have to assess a revocation.

Once they are stored, the applicant's data are subject throughout the entire retention period to a permanent automated comparison with new findings. This seems disproportionate given the fact that in future border procedures as foreseen in the proposals for the EES and the respective amendments of the SBC would include not only checks against the EES, the SIS II, the Interpol database on stolen and lost travel documents, national databases on stolen, misappropriated, lost and invalidated travel documents and if necessary a consultation of the VIS. We assume that there are possible less intrusive measures (e.g. non-permanent checks at the time of border procedures). Such alternatives should have been assessed in a proper data protection impact assessment.

Procedure for access to the ETIAS Central System for law enforcement (Art. 44)

We do not understand why only where the consultation of data referred to in Article 15(2)(i) and (4)(b) to (d) is sought, the reasoned electronic request shall include a justification of the necessity to consult those specific data. This justification should be requested in each case. In fact, the LEA are only allowed to have access to data when this access is necessary (Art. 45) or when the requirements of Article 45 are fulfilled. The necessity should arise from the grounds of the application (Article 44 para. 1).

Retention period (Art. 47):

Data are, in principle, only to be stored as long as they are necessary. Therefore, we are astonished that the period of validity of the travel authorisation is not taken into account as the general rule. It is during this period that a potential cross-check is carried out by carriers and border guards. The period of validity of the travel authorisation is anyway limited by the period of validity of the travel document.

It is not clear why a storage for a period of five years from the date of the last decision on refusal, revocation or withdrawal of an ETIAS travel authorisation is appropriate, especially as this automatically results in a hit and a manual risk assessment when an application is submitted at a later stage (cf. Art. 18 para. 2 lit. e). This corresponds to an increased risk of refusal. It seems doubtful whether the risk assessment, which was once carried out or which was later revised, can justify this for five years.

It also requires further justification why a five-year retention period from the last entry record in the EES is deemed appropriate. Pure aspects of interoperability between both systems - in the EES a five-year retention period for the data records stored there is envisaged - cannot be sufficient.