Meijers Committee
standing committee of experts on international immigration,
refugee and criminal law
[redacted]

CM1708 Comments on the proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS), COM(2016) 731 final

6 July 2017

With regards to this proposal the Meijers Committee will like to comment on the following:

I. Necessity and proportionality

The ETIAS proposal lacks sufficient evidence with regard to necessity and proportionality of this measure and the added value compared to other existing large-scale databases: Visa Information System (VIS), Eurodac, Schengen Information System (SIS), the Europol database, the proposed Entry Exit System, and the effect of existing obligations for air carriers to submit information on their passengers based on the Advanced Passenger Information (API) and Passenger Name Record (PNR) Directives.[1] Many of the recent terrorist events in European cities, have been committed by EU citizens and not third-country nationals. Furthermore, after the attacks, it has been established that several of the terrorists were already targeted or followed as potentially radicalised and dangerous persons. In some cases, prior to the attack, it has been submitted that foreign security agencies provided information on the terrorists involved, which information did not result in any preventive measures. The Meijers Committee finds that before developing new tools or large-scale databases, it is necessary to set up an extensive and in depth analysis within the EU, addressing both the effectiveness of current data information systems and the (follow up of) exchange of information between national authorities, EU agencies, and third states.

The European Commission states that data sharing on the entry and exit of visa-exempted travellers is currently lacking. Moreover, the ETIAS proposal will reinforce EU internal security in two ways, first through the prior identification of persons that pose a security risk before they arrive at the Schengen border. Second it will do so 'by making information available to national law enforcement authorities and Europol', thus also when the person already entered the Schengen territory, and considering the five years data retention, also when the person has left the EU. Considering the goal of ETIAS, which is the identification of migration, security and health risks, it is unclear why the current available systems should not provide sufficient information. First, the current directives obliging air carriers to submit PNR and API data to EU border guards of their passengers, allow prior security checks of these individuals, thus before they arrive at the EU borders. Second, SIS II allow for the registration of alerts on persons who have no right to stay within the Schengen area, as those to be considered a security risk (including EU citizens and visa-exempted travellers), which data is also checked prior to arrival (during visa applications for those who need a visa, and at the borders on the basis of Article 6 of the Schengen Borders Code). Third, Eurodac and VIS include information on asylum seekers and irregular migrants, respectively visa applicants and are already accessible for law enforcement purposes, even if these individuals are unsuspected or have no connection to any criminal procedure.

[1] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, 4 May 2016.

The current ETIAS proposal is not based on a data protection impact assessment, whereas the implementation of this proposal will likely result in a high risk to the rights and freedoms of natural persons, as further formulated below.[2] The Meijers Committee suggests that the European Parliament asks the European Commission to conduct such an impact assessment, before further progress is made in the legislative process.

II. Grounds for refusal of travel authorisation

The proposal may result in a differentiated practice in the EU with regard to the issuing and refusal of travel authorisations, hampering the access of individuals to Europe, even if there are no sufficient or substantiated grounds for such refusal. According to the proposal, the refusal (or annulment or revocation) of an entry authorisation (Article 31, 34, 35) is to be based on the non-fulfilment of the conditions mentioned in 31 (1) of which three categories entails the assumption of a risk to health, security and migration. The risk for public health however is the only risk that is defined in the proposed text. It is unclear from the proposal what is precisely meant by the risks for security and illegal migration. The Meijers Committee suggests to include a precise definition of 'irregular migration' and 'security' risk, in accordance with existing EU laws, including the SIS II Regulation, the Return Directive, and the European Arrest Warrant.[3]

To enable the assessment of these risks and thus whether a person is eligible to enter the EU, three levels of information sorting will be used:

1) An automated comparison of national and EU databases, for example whether the travel documents have been reported as stolen, lost or invalidated in SIS or national databases, or the person has been reported for the purpose of refusal of entry into the SIS, and checking both national as other EU databases;
2) ETIAS screening rules, according to Article 28, '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. The ETIAS screening rules shall be registered in the ETIAS Central System', and;
3) the watch list established by Europol (Article 29, 67).

All three levels contain the risk of automated decision making, in violation of the safeguards included in data protection law, more precisely in Article 22 General Data Protection Regulation and Article 11 of Directive 2016/680.[4] These provisions prohibit decision making based solely on automated processing, including profiling, which produces adverse legal effects concerning the data subject or significantly affects him or her, unless authorised by Union or Member State law.

This proposal should provide appropriate safeguards in cases of automated decision making, to ensure the rights and freedoms of the data subject. These safeguards include at least the right to obtain human intervention on the part of the controller, an independent supervision of the establishment

[2] See also the European Data Protection Supervisor in Opinion 3/17.

[3] SIS II Regulation 1987/2006, *OJ* L381, 28 December 2008, Return Directive 2008/115, *OJ* L 348, 24 December 2008, and the SIS II Decision 2007/533, *OJ* L 205, 5 August 2007.

[4] Regulation (EU) 2016/679, *OJ* L 119, 4 May 2016, and Directive (EU) 2016/680, *OJ* L 119, 4 May 2016.

and use of screening rules and the Europol watch lists, and the right to effective legal remedies with regard to the refusal of a travel authorisation and incorrect or unlawful registration of personal data. Furthermore, the Meijers Committee notes that as both the refusal based on screening rules or watch lists entail the use of 'soft data', this hampers the individual's right to effective remedies and control by supervisory data protection authorities. It will be very difficult to address the information which resulted in the assumed 'risk' of the person involved.

In this regard, the Meijers Committee refers to the recent judgment of the CJEU in *Fahimian*, in which the CJEU held that national authorities when deciding on an application for a visa for study purposes, even if they have wide margin of discretion to ascertain whether this person represents 'a threat, if only potential, to public security', must make this decision 'in light of all the relevant elements of the situation of that national'. Furthermore, according to the CJEU, national courts must be able to ascertain that the decision is based on 'sufficient grounds and a sufficiently solid factual basis'.[5] Based on this conclusion, it is clear that when deciding upon an entry authorisation, based on the aforementioned comparison of databases, risk profiling or Europol watch list, national authorities must always take into account the individual situation of the applicant and any refusal must be based on a sufficiently solid factual basis.

Finally, the addition in Article 31 of the proposal that the travel authorisation shall also be refused 'if there are reasonable doubts as to the authenticity of the data, the reliability of the statements made by the applicant, the supporting documents provided by the applicant or the veracity of their contents' (underlining Meijers Committee) allows for a very wide discretionary power of the deciding authorities. The Meijers Committee proposes to replace the wordings 'reasonable doubts' in Article 31 by 'reasonable, serious, and substantiated doubts' to limit the discretionary power of the decision making authorities and to allow an effective scrutiny by supervising authorities or courts.

III. The rights of individuals – effective judicial protection

1) Vague definitions

It is unclear what is meant with 'irregular migration' and 'security' risk: this is specifically problematic in the context of the current proposals which is based on not only automated check of available databases, but also on the use of risk profiling: this results not only in a differentiated approach in the different EU states, which runs counter the harmonised refusal grounds in the Schengen Borders Code, but also makes it difficult, if not impossible for the data subject to lodge any effective remedy against a decision, refusing him or her authorisation to enter the EU territory. The Meijers Committee suggests to define the 'irregular migration' and 'security' risk in the text.

2) Processing of wide range personal data

The ETIAS proposal includes the processing of a wide range of personal data. The list included in Article 15 of the proposal has a broad scope and includes "education (level and field)" and "current occupation". For these types of data, it is unclear why they could be necessary for the risks mentioned above. The Meijers Committee suggest taking these categories out of the list of Art 15.

3) Access and interoperability between existing databases and purpose limitation

5 CJEU, *Fahimian*, 4 April 2017, C-544/15, para. 50.

The Meijers Committee is concerned about the proposal's introduction of a system that will be interoperable with other police, judicial and immigration systems for the purpose of cross-checking information in ETIAS against data registered in such systems. We highlight the need for clearly defined access rights for competent authorities that should be strictly limited to what is necessary and proportionate for the purpose ETIAS is set up for.[6]

4) Access to effective remedies

Article 32 (2) provides applicants who have been refused a travel authorisation only 'the right to appeal', without any further definition of the content of this appeal and without any guarantee that the individual has the right to effective protection. According to Article 32 (2) of the proposal, appeals against refusal to issue an ETIAS must be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State.

- This provision leaves it to the discretionary power of MS as to whether the individual has access to judicial remedies, the time limits, or the availability of legal aid, or legal advisor or translator. It also restricts the accessibility of remedies of the applicant to the state refusing the ETIAS.
- The Meijers Committee suggests the EU legislator to build in safeguards to protect the right in Article 47 of the Charter on Fundamental Rights (CFR) ensuring every individual whose rights and freedoms guaranteed by EU law, a right to effective remedies. The conclusions of the CJEU in the *Schrems* judgment[7] and in the *DRI* judgment[8], addressing the necessity of effective and judicial protection with regard to the processing of personal data and the rights of privacy and data protection protected in Articles 7 and 8 CFR should be respected.[9]
- Article 48 (6) of the proposal provides for a right to an effective judicial remedy with regard to 'ensure the data is deleted', however it is unclear how this right, if granted by a judicial authority of one of the MS will be effectuated, lacking a provision in the ETIAS proposal which is comparable to the provision in Article 43 SIS II Regulation, obliging MS to enforce mutually the national judicial decision dealing with SIS alerts. The Meijers Committee proposes as follows to insert a specific provision on the right to effective remedies, comparable with Article 43 of the SIS II Regulation and taking into account the case-law of the CJEU, allowing every individual access to a judicial remedy in any of the Member States involved in the application of ETIAS and obliging the national authorities of those Member States to mutually enforce the judicial decisions.

5) Data retention

In accordance with the ETIAS proposal, as a general rule the duration for the storage of the ETIAS application data will be 5 years after the last use of the travel authorisation or from the last decision to refuse, revoke or annul a travel authorisation. The Meijers Committee submits that the necessity of

[6] See also EDPS Opinion 3/17, point 51: '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.'

[7] CJEU, *Schrems v. Data Protection Commissioner*, 6 October, 2015 C-362/14, para. 95.

[8] CJEU, *Digital Rights Ireland Ltd*., 8 April 2014, C-293/12, para. 62 and 68.

[9] In *Schrems* , C-362/14, para. 95, the CJEU stated 'The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law'.

the general data retention period of five years has not been substantiated and that especially the retention period of five years when it concerns data on denied, revoked or annulled ETIAS applications, should be further justified.

IV. Applicability of different legal frameworks for data protection – lack of transparency

The ETIAS system as proposed will process personal data with the purpose of preventing the risks mentioned above. The personal data to be processed by the ETIAS system will fall within the scope of different legal instruments (see also Article 49 of the proposal):

- Personal data processed by the national ETIAS units will fall within the scope of the General Data Protection Regulation;
- Personal data processed by the law enforcement authorities of the member states will fall within the scope of Directive 2016/680 on data protection for law enforcement purposes;
- Personal data processed by Europol will fall within the scope of the 2017 Europol Regulation, and
- Personal data processed by the European Border and Coast Guard will fall within the scope of Regulation 45/2001 (or its successor).

The Meijers Committee stresses that this will create a complex construction where personal data that are inserted into the system by one person or authority may fall within the scope of different legal instruments, adversely affecting the legal certainty of the data subject. It is not clear which legal instrument will prevail in case of conflicting provisions and, even more, which is the applicable legal remedy. For example, when personal data of a citizen is unlawfully processed by a national ETIAS unit and is subsequently used for the purpose of investigating a criminal offence by a law enforcement authority of another member state, which data protection authority should the citizen then address in case of a complaint?

The Meijers Committee proposes that the proposal specifies which legal instrument will prevail in cases of conflicting provisions, especially with regard to the applicable legal remedy.

V. Accountability

The Meijers Committee is worried about the number of authorities in the ETIAS proposal, listed with responsibility or any other form of control or management with regard to the functioning of ETIAS. The ETIAS proposal provides a complicated set of rules defining a high number of actors and agencies accountable for different issues connected to the operation of ETIAS which may hamper the accessibility of effective remedies, based on unclarities but also possible conflicts of responsibility, and thus accountability, between the actors involved**:**

1. euLISA: developing the ETIAS Information System and ensuring its 'technical management', according to the proposal Article 6. 4, and according to Article 51, as data processor 'eu-LISA shall ensure that the ETIAS Information System is operated in accordance with this Regulation', see also 63(3));
2. ETIAS National Units: according to Article 52 (1) these units together with eu-LISA 'shall ensure the security of processing of personal data takes place pursuant to the application of this Regulation. Furthermore, eu-LISA and the ETIAS National Units shall cooperate on security related tasks.';
3. European Border and Coast Guard Agency (EBCG), Article 65 provides that the EBCG shall be responsible for: (a) the setting up and operation of the ETIAS Central Unit; (b) the automated processing of applications; and (c) the screening rules;

4. Europol: According to Article 67, Europol shall be responsible for the establishment of the ETIAS watch-list, as meant in Article 29;
5. Individual Member States: Article 66 provides that Each Member State shall be responsible for:
   (a) the connection to the National Uniform Interface;
   (b) the organisation, management, operation and maintenance of the ETIAS National Units for the examination of and decision on travel authorisations' applications rejected during the automated processing of applications;
   (c) the organisation of central access points and their connection to the National Uniform Interface for the purpose of law enforcement;
   (d) the management and arrangements for access of duly authorised staff of the competent national authorities to the ETIAS Information System in accordance with this Regulation and to establish and regularly update a list of such staff and their profiles;
   (e) the set up and operation of the ETIAS National Units.

The Meijers Committee underlines that any proposal involving the use of large-scale databases, screening-list, and watch-lists, must provide clear and precise rules on the definition of the actors and Member States responsible for errors, incorrect or unlawful storage or use of personal information, or inappropriate security measures. The Meijers Committee proposes to appoint one processor or Member State to be held responsible for any breach of EU law or violation of individual rights, to allow accessible and effective legal remedies for the data subject. The involvement of different actors may not obstruct the practical implementation of the right to effective judicial protection.

About

The Meijers Committee is an independent group of legal scholars, judges and lawyers that advises on European and international migration, refugee, criminal, privacy, anti-discrimination and institutional law. The Committee aims to promote the protection of fundamental rights, access to judicial remedies and democratic decision-making in EU legislation.

The Meijers Committee is funded by the Dutch Bar Association (NOvA), Foundation for Democracy and Media (Stichting Democratie en Media) the Dutch Refugee Council (VWN), Foundation for Migration Law Netherlands (Stichting Migratierecht Nederland), the Dutch Section of the International Commission of Jurists (NJCM), Art. 1 Anti-Discrimination Office, and the Dutch Foundation for Refugee Students UAF.

Contact info:

Ph +31(0)20 362 0505

E post@commissie-meijers.nl

W www.commissie-meijers.nl