COMMISSION DELEGATED DECISION (EU) 2019/971

of 26 February 2019

on the definition of the requirements of the secure account service pursuant to Article 6(4) of Regulation (EU) 2018/1240 of the European Parliament and of the Council, enabling applicants to provide any additional information or documentation required

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [1], and in particular Article 6(4) thereof,

Whereas:

(1) Regulation (EU) 2018/1240 established a European Travel Information and Authorisation System (ETIAS) as a system for third-country nationals exempt from the requirement to be in possession of a visa when crossing the external borders. It laid down the conditions and procedures to issue or refuse a travel authorisation.

(2) ETIAS National Units manually processing of ETIAS applications may request applicants to provide additional documentation or information. This Decision should set out conditions on how the applicants can provide those additional documents or information using a dedicated tool.

(3) The secure account service should be accessible through the dedicated public website and the app for mobile devices and through a secure link.

(4) The secure account service should enable confirming the identity of the applicant and ensure secure access to the tool. It is therefore necessary to set out the authentication requirements, including the provision of a unique code to the applicant.

(5) It is also necessary to set out the procedure for the submission of additional information or documentation as well as outputs of the secure account service.

(6) Applicants should be able to submit additional information or documentation at any time, within the time allocated according to Article 27(2) or Article 44(3) from the receipt of the request for additional information or documentation. Applicants should be able to save and resume their progress within that time limit. After those deadlines have passed, applicants should no longer have access to the secure account service.

(7) The communication channels of the secure account service with the ETIAS Central System should be set out. Furthermore, the message format, standards and protocols as well as the security requirements should be established.

(8) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2017/2226 and is not bound by it or subject to its application. However, given that Regulation (EU) 2018/1240 builds upon the Schengen *acquis*, Denmark notified on 21 December 2018, in accordance with Article 4 of that Protocol, its decision to implement Regulation (EU) 2018/1240 in its national law.

(9) This Decision constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC [2]; the United Kingdom is therefore not taking part in the adoption of this Decision and is not bound by it or subject to its application.

[1] OJ L 236, 19.9.2018, p. 1.

[2] Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).

(10) This Decision constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC ([3]); Ireland is therefore not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(11) As regards Iceland and Norway, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* ([4]), which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC ([5]).

(12) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([6]), which fall within the area referred to in Article 1, point A of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/146/EC ([7]).

(13) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([8]) which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([9]).

(14) The European Data Protection Supervisor was consulted on 28 January 2019 and delivered an opinion on 8 February 2019,

HAS ADOPTED THIS DECISION:

Article 1

Access to the secure account service

1. The secure account service shall be accessible via:

(a) the dedicated public website referred to in Article 16 of Regulation (EU) 2018/1240;

(b) the app for mobile devices referred to in Article 16 of Regulation (EU) 2018/1240;

(c) a link provided through the ETIAS email service referred to in point (f) of Article 6(2) of Regulation (EU) 2018/1240.

2. The secure account service shall be accessible until:

(a) final submission of additional information or documentation confirmed by the ETIAS applicant; or

(b) until expiry of the time limit, referred to in Article 27(2) of Regulation (EU) 2018/1240; or

(c) until expiry of the duration set by the ETIAS National Unit pursuant to Article 44 of Regulation (EU) 2018/1240.

([3]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).
([4]) OJ L 176, 10.7.1999, p. 36.
([5]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).
([6]) OJ L 53, 27.2.2008, p. 52.
([7]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).
([8]) OJ L 160, 18.6.2011, p. 21.
([9]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

Article 2

Two-factor authentication for access to the secure account service

1. In order to connect to the secure account service, two-factor authentication shall be used.

2. The first authentication shall consist of entering the following data:

(a) application number;

(b) travel document number.

3. Where the applicant does not provide his or her application number, the first authentication shall consist of entering following data:

(a) travel document number;

(b) country of issue of the travel document to be selected from a predetermined list;

(c) date of issue and of expiry of the travel document; and

(d) first names of both parents.

4. The application number shall be the same as the one provided to applicants via the ETIAS email service on submission of their application. The other data, referred to in paragraph 2 or paragraph 3, submitted by the applicant shall also be the same as those provided by applicants at the time of the submission of their application.

5. The second authentication shall consist of a unique code to be entered into the secure account service to confirm authentication.

6. Upon submission of the information in paragraph 2 or paragraph 3, the unique code referred to in paragraph 4 shall be automatically generated and sent to the applicant through the email service referred to in point (f) of Article 6(2) of Regulation (EU) 2018/1240.

7. The unique code shall be sent to the same email address provided in the submitted application.

8. The unique code shall expire after a short period of time. Sending a new unique code shall invalidate unique codes previously sent to the same applicant.

9. The unique code shall be usable only once.

Article 3

Submission of additional information or documentation to the secure account service

1. For the purpose of Article 27 of Regulation (EU) 2018/1240, ETIAS applicants shall submit additional information or documentation, in one of the following formats:

(a) Portable Document Format (PDF);

(b) Joint Photographic Experts Group (JPEG); or

(c) Portable Network Graphics (PNG).

2. The secure account service shall accept a final upload of a maximum of 20 files and a final size of submission not exceeding 50 MB.

3. ETIAS applicants shall be able to save their progress and resume their submission of additional information or documentation in the secure account service within the time limit referred to in Article 27(2) of Regulation (EU) 2018/1240 or the time limit allocated by the ETIAS National Unit where the provisions of Article 44 of that Regulation are applied. The secure account service shall allow applicants to clearly indicate whether the submission is final or not. The secure account service shall allow applicants to verify that the documents are uploaded correctly before confirming submission.

4. Applicants shall be allowed to delete documents uploaded before the final submission within the allocated time, referred to in Article 27(2) of Regulation (EU) 2018/1240 or the time allocated by the ETIAS National Unit where the provisions of Article 44 of that Regulation are applied.

5. Applicants shall be asked to confirm their submission through the ticking of an appropriate box in the secure account service.

Article 4

Output of the secure account service

1. Upon final submission of the additional information and/or documentation:

(a) a read-only version of the submitted additional information and/or documentation shall be available accompanied by the reference 'submitted';

(b) the applicant shall, via the ETIAS email service, receive an email confirming submission of additional information and/or documentation, including the names and formats of the uploaded documents, the time stamp of final submission and an alphanumeric value of a fixed length that uniquely identifies data ('hash values') for the submitted files.

2. After submission of the additional information and/or documentation, applicants shall no longer have access to the secure account service.

3. The secure account service shall have a built-in technical solution to help guarantee that every document stored in the application file is the same as the one uploaded by the applicant in the secure account service.

Article 5

Communication of the secure account service with the ETIAS Central System

1. Following a request for additional information or documentation by an ETIAS National Unit, pursuant to Articles 27 or 44 of Regulation (EU) 2018/1240, the ETIAS Central System shall immediately inform the secure account service of such request via the secure web service, referred to in point (l) of Article 6(2) of Regulation (EU) 2018/1240.

2. Upon submission of additional information or documentation by the applicant, the secure account service shall:

(a) calculate hash values of the submitted files; and

(b) transmit the additional information or documentation to the ETIAS Central System through the secure web service.

3. The secure web service shall conduct the necessary verification processes to ensure that the documents are safe and secure prior to transmitting them to the ETIAS Central System.

4. The ETIAS Central System shall record and store the additional information and/or documentation on the application file in accordance with Articles 27(9) and 44(3) of Regulation (EU) 2018/1240.

Article 6

Message format, standards and protocols

The message format and the protocols to be implemented shall be included in the technical specifications referred to in Article 73(3) of Regulation (EU) 2018/1240.

Article 7

Specific security considerations

1. The secure account service shall be designed and implemented in a way that precludes unlawful access to it. For this purpose, the secure account service shall limit the number of attempts to access the secure account service with the same travel document, application number or unique code. The secure account service shall also include measures to protect against non-human behaviour.

2. The secure account service shall include time-out measures after some minutes of inactivity.

3. Additional details concerning the confidentiality, integrity and availability of processed data shall be subject of the technical specifications referred to in Article 73(3) of Regulation (EU) 2018/1240.

Article 8

Logs

1. The secure account service shall keep activity logs containing:

(a) authentication data including whether the authentication was successful or not;

(b) the date and time the unique code was sent;

(c) date and time of access;

(d) number of documents uploaded;

(e) verification of safety and security of the documents.

2. In addition, for each document, the following logs shall be kept:

(a) date and time of uploaded document(s);

(b) document name(s);

(c) size of document(s);

(d) hash values of the documents uploaded.

3. Activity and document logs of the secure account service shall be copied to the Central System. They shall be stored for no longer than one year after the end of the retention period of the application file, unless they are required for monitoring procedures which have already begun. After that period, they shall be automatically erased.

Such logs can only be used for the purpose of Article 69(4) of Regulation (EU) 2018/1240.

Article 9

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 26 February 2019.

For the Commission
The President
Jean-Claude JUNCKER