Interoperability between EU information systems (borders and visa)

2017/0351(COD) - 16/04/2019 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 511 votes to 123, with 9 abstentions, a legislative resolution on the amended proposal for a regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the euLISA Regulation].

The European Parliament's position adopted at first reading under the ordinary legislative procedure amended the Commission's proposal as follows:

Framework for the interoperability of EU information systems

The proposed Regulation, together with the Regulation of the European Parliament and of the Council on police and judicial cooperation, asylum and migration, shall establish a framework to ensure interoperability between the entry/exit system (EES), the visa information system (VIS), the European Travel Information and Authorisation System (ETIAS), Eurodac, the Schengen Information System (SIS) and the European Criminal Records Information System for third-country nationals (ECRIS-TCN). It would also establish a framework for verifying the identity of individuals and identifying individuals.

This framework shall include the following interoperability components: (i) a European search portal (ESP); (ii) a shared biometric matching service (shared BMS); (iii) a common identity repository (CIR); (iv) a multiple-identity detector (MID).

Objectives

Interoperability shall improve the management of external borders by establishing rapid, simple and efficient access to EU information systems. According to the amended text, this Regulation has the following objectives:

- to improve the effectiveness and efficiency of border checks at external borders;

- to contribute to the prevention and the combating of illegal immigration;

- to contribute to a high level of security within the area of freedom, security and justice of the Union including the maintenance of public security and public policy and safeguarding security in the territories of the Member States;

- to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences;

- to facilitate the identification of unknown persons who are unable to identify themselves or unidentified human remains in case of a natural disaster, accident or terrorist attack.

Non-discrimination and fundamental rights

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly, persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration.

Access to the European Search Portal (ESP)

The use of the ESP shall be reserved to the Member State authorities and Union agencies having access to at least one of the EU information systems in accordance with the legal instruments governing those EU information systems. Those Member State authorities and Union agencies may make use of the ESP and the data provided by it only for the objectives and purposes laid down in the legal instruments governing those EU information systems.

The ESP shall provide no information regarding data in EU information systems, Europol data and the Interpol databases to which the user has no access under the applicable Union and national law.

Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.

Access to the common identity data repository (CIR) for identification

Under the amended text, queries of the CIR shall be carried out by a police authority only in the following circumstances:

- where a police authority is unable to identify a person due to the lack of a travel document or another credible document proving that person's identity;

- where there are doubts about the identity data provided by a person and to the authenticity of the travel document or another credible document provided by a person;

- where a person is unable or refuses to cooperate.

Such queries shall not be allowed against minors under the age of 12 years old, unless in the best interests of the child.

Terrorist offences

In specific cases, where there are reasonable grounds to believe that searching EU information systems will contribute to the prevention or detection of terrorist offences or other serious criminal offences, designated authorities and Europol could consult the CIR to determine whether data on a particular person are stored in the EES, VIS or ETIAS.

In this context, a reply from the CIR should not be interpreted or used as a ground or reason to draw conclusions on or undertake measures in respect of a person, but should be used only for the purpose of submitting an access request to the underlying EU information systems, subject to the conditions and procedures laid down in the respective legal instruments governing such access.

As a general rule, where a match-flag indicates that the data are recorded in the EES, VIS, ETIAS or Eurodac, the designated authorities or Europol should request full access to at least one of the EU information systems concerned. Where exceptionally such full access is not requested, for example

because designated authorities or Europol have already obtained the data by other means, or obtaining the data is no longer permitted under national law, the justification for not requesting access should be recorded. Europol shall record the justification in the relevant file.

Results of multiple identity detection

The MID should create and store links between data in the different EU information systems in order to detect multiple identities, with the dual purpose of facilitating identity checks for bona fide travellers and combating identity fraud. These links will be classified into four categories: white, yellow, green and red.

In order to facilitate the implementation of the necessary safeguards in accordance with applicable Union data protection rules, individuals who are subject to a red link or a white link following manual verification of different identities should be informed in writing without prejudice to limitations to protect security and public order, prevent crime and guarantee that national investigations are not jeopardised. Those individuals should receive a single identification number allowing them to identify the authority to which they should address themselves to exercise their rights.

Where a yellow link is created, the authority responsible for the manual verification of different identities should have access to the MID. Where a red link exists, Member State authorities and Union agencies having access to at least one EU information system included in the CIR or to SIS should have access to the MID. A red link should indicate that a person is using different identities in an unjustified manner or that a person is using somebody else's identity.

Web portal

As the interoperability components will involve the processing of significant amounts of sensitive personal data, persons whose data are processed by these elements should be able to effectively exercise their rights as data subjects. To this end, the amended text provides for the provision of a web portal to facilitate the exercise by data subjects of their rights of access to their personal data and their rights to rectify, delete and limit the processing of such data. The implementation and management of the portal should be the responsibility of eu-LISA.

The Regulation also contains clear provisions on liability and the right to compensation in the event of unlawful processing of personal data or in the event of any other act incompatible with the Regulation.