Asylum: Eurodac system for the comparison of fingerprints of third-country nationals or stateless applicants; requests for comparison with Eurodac data. Recast

2008/0242(COD) - 12/06/2013 - Text adopted by Parliament after reconsultation

The European Parliament adopted by 502 votes to 126, with 56 abstentions, a legislative resolution on the proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] 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).

Parliament adopted its position at first reading under the ordinary legislative procedure. The amendments adopted in plenary are the result of a compromise negotiated between the European Parliament and the Council. They amend the proposal as follows:

Purpose of Eurodac: Eurodac shall assist in determining which Member State is to be responsible pursuant to Regulation (EU) No …/… (Dublin Regulation, as amended) for examining an application for international protection lodged in a Member State by a third-country national or a stateless person.

The Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the Central System for **law enforcement purposes**.

Member States' designated authorities for law enforcement purposes: Member States shall designate the authorities that are authorised to request comparisons with Eurodac data. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. **Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security**.

Member States' verifying authorities for law enforcement purposes: each Member State shall designate a single national authority or a unit of such an authority to act as its **verifying authority**. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. The verifying authority shall act independently when performing its tasks. The verifying authority shall not receive any instructions as regards the outcome of the verifications it undertakes. Member States may designate **more than one verifying authority** to reflect their organisational and administrative structures, in accordance with their constitutional or legal requirements.

The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled. **Only duly empowered staff** of the verifying authority shall be authorised to receive and transmit a request for access to Eurodac.

Tasks devolved to Europol: Europol shall designate **a specialised unit with duly empowered Europol officials** to act as its verifying authority, which shall act independently of the designated authority when performing its tasks and shall not receive instructions from the designated authority as regards the outcome of the verification. The unit shall ensure that the conditions for requesting comparisons of fingerprints with Eurodac data are fulfilled. The designated authority shall be an operating unit of Europol which is competent to collect, store, process, analyse and exchange information to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling within Europol's mandate.

Collection, transmission and comparison of fingerprints: each Member State shall promptly take the fingerprints of all fingers of every applicant for international protection of at least 14 years of age and shall, as soon as possible and no later than 72 hours after the lodging of his or her application for international protection, transmit them to the Central System. In the event of serious technical problems, Member States may extend the 72-hour time-limit by a maximum of a further 48 hours in order to carry out their national continuity plans.

Advance data erasure: data relating to a person who has acquired citizenship of any Member State shall be erased from the Central System as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship. The Central System shall**, as soon as possible and no later than after 72 hours**, inform all Member States of origin of the erasure of data.

Storage of data: each set of data relating to a third-country national or stateless person shall be stored in the Central System for **18 months** from the date on which his or her fingerprints were taken. Upon expiry of that period, the Central System shall automatically erase such data.

Comparison of fingerprint data: with a view to checking whether a third-country national or a stateless person found illegally staying within its territory has previously lodged an application for international protection in another Member State, a Member State may transmit to the Central System any fingerprint data relating to fingerprints which it may have taken of any such third-country national or stateless person of at least 14 years of age, together with the reference number used by that Member State. Once the results of the comparison of fingerprint data have been transmitted to the Member State of origin, the record of the search shall be kept by the Central System only for the purposes stipulated in the Regulation. Other than for those purposes, **no other record of the search may be stored either by Member States or by the Central System**.

Marking of data: the Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System. That mark shall be stored in the Central System and the **Central System shall inform all Member States of origin of the marking of data by another Member State of origin having produced a hit with data which they transmitted**.

The data of beneficiaries of international protection stored in the Central System and marked shall be made available for comparison **for a period of three years** after the date on which the data subject was granted international protection. Upon the expiry of the period of three years, the Central System shall automatically block such data from being transmitted in the event of a request for comparison for enforcement purposes, until the point of their erasure.

Conditions for access to Eurodac by designated authorities: authorities may submit a reasoned electronic request for the comparison of fingerprint data with the data stored in the Central System within the scope of their powers only if comparisons with the national fingerprint databases, the automated

fingerprintining identification systems of all other Member States, and the Visa Information System, in addition to other cumulative conditions, **did not lead to the establishment of the identity** of the data subject.

It is also stipulated that the comparison may only take place if there are **reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences** in question.

Equivalent rules are laid down governing access to Eurodac by Europol.

Procedure for carrying out urgent comparisons for enforcement purposes in exceptional cases: new provisions were introduced to make provision for the **urgent** transmission of fingerprint data when there is a need to prevent an imminent danger associated with a terrorist offence or other serious criminal offence.

Quality of fingerprint data transmitted: in a recital, it is stipulated that the Member States should ensure the transmission of fingerprint data of an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. All authorities with a right of access to Eurodac should invest in adequate training and in the necessary technological equipment.

The fact that it is temporarily or permanently impossible to take and/or to transmit fingerprint data, due to reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her fingerprints taken owing to circumstances beyond his or her control, should not adversely affect the examination of or the decision on the application for international protection lodged by that person.

Protection of personal data for law enforcement purposes:

Each Member State shall provide that the provisions adopted under national law implementing Framework Decision 2008/977/JHA are also applicable to the processing of personal data by its national authorities for law enforcement purposes.

The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States for the purposes laid down in this Regulation shall be carried out by the designated national supervisory authorities. The European Data Protection Supervisor shall also play a role in this context.

Security incidents: Member States shall inform the Agency of security incidents detected on their systems. The Agency shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents.

Prohibition of transfers of data to third countries: personal data obtained by a Member State or Europol pursuant to this Regulation from the Central System shall not be transferred or made available to any third country, international organisation or private entity established in or outside the Union. Personal data which originated in a Member State and are exchanged between Member States following a hit shall not be transferred to third countries if there is a serious risk that as a result of such transfer the data subject may be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights.

Audit: Member States shall ensure that every year an audit of the processing of personal data for law enforcement purposes is carried out by an independent body, in accordance with Article 33(2), including an analysis of a sample of reasoned electronic requests.

Reports and evaluation: every four years, the Commission shall produce an overall evaluation of Eurodac, examining the results achieved against objectives and the impact on fundamental rights, including whether law enforcement access has led to indirect discrimination against persons covered by this Regulation, and assessing the continuing validity of the underlying rationale and any implications for future operations, and shall make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

On the basis of Member States' and Europol's annual reports and in addition to the overall evaluation report, the Commission shall compile an annual report on law enforcement access to Eurodac and shall transmit it to the European Parliament, the Council and the European Data Protection Supervisor.

Other provisions: provisions were also made in regard to the following:

- the development of a Business Continuity Plan and System taking into account maintenance needs and unforeseen downtime of the system;

- the compilation of quarterly statistics;

- taking into account the best interests of the child when applying this Regulation; and

- the preparation of a leaflet for persons whose fingerprints in order to provide them with information regarding their rights.