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) - 19/12/2012 - Committee final report tabled for plenary, reconsultation

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Monica Luisa MACOVEI (EPP, RO) on the amended 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 to request comparisons 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).

The parliamentary committee recommends that the European Parliament’s position adopted at first reading under the ordinary legislative procedure should be to amend the Commission’s proposal as follows:

Right of the applicant for international protection to have his or her application processed in due course: Members consider it important that Member States do not put in place practices which would link a possible result in EURODAC to the success of the asylum application since only a final judgment should have a bearing on this. As a result, the fact that the law enforcement authorities of the Member States consult EURODAC s**hould not be grounds for slowing down the process of examining the applicant's claim** for international protection.

Strict conditions of access: Members consider that access to EURODAC should be very restricted. They therefore ask that access to EURODAC data by EUROPOL should be allowed **only in specific cases**, under specific circumstances and under strict conditions. Likewise, EURODAC should only be used n cases where there are reasonable grounds for believing that the perpetrator or victim may fall under one of the categories covered by this Regulation.

Erasure of fingerprint data: once the results of the comparison have been transmitted to the Member State of origin, the Central System shall **immediately** erase the fingerprint data and other data transmitted to it. The Central System shall inform all Member States of origin no later than after 72 hours about the erasure of data.

Quality of fingerprint data transferred: Member States should ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the **computerised fingerprint recognition system**. All authorities with right of access to EURODAC should invest in adequate training and in the **necessary technological equipment**. The authorities with right of access to EURODAC should inform the Agency of specific difficulties encountered with regard to the quality of data, in order to resolve them.

Impossibility to provide fingerprints: a temporary or permanent impossibility for an applicant for international protection to provide fingerprints ('failure to enrol') should not adversely affect the legal situation of that applicant.

Verifying authorities and "designated" authorities: each Member State shall appoint a single national body to act as its **verifying authority** which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. It shall act **completely independently** of all other authorities and shall not receive instructions from them as regards the outcome of the verification. Likewise, **Europol** shall appoint a specialised unit with duly empowered Europol officials to act as its verifying authority. It shall also act independently of designated authorities.

Only designated authorities are permitted to consult EURODAC data. The designated authority and the verifying authority may be part of the same organisation if so stipulated under national law, but the verifying authority should have **independence** within the institutional structure. Designated authorities shall not include agencies or units exclusively responsible for intelligence relating to national security.

Reasoned electronic request for comparison of fingerprint data: designated authorities may submit a reasoned electronic request for the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases, of the Automated Fingerprint Databases of other Member States and of the Visa Information System, when possible, return **negative results** and where the cumulative conditions defined in the report are met.

Searches for fingerprint data in EURODAC should only be authorised in **restricted cases**, in the context of criminal enquiries under way or where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist or other serious criminal offence has applied for international protection. In any event, EURODAC searches should not become an 'automatic' search carried out by the law enforcement authorities.

It is also stipulated that the Commission shall publish an indicative, non-binding model EURODAC request form.

Verification by a trained fingerprint expert: the results of the comparison should be immediately checked in the Member State of origin by a **trained fingerprint expert**.

Data protection: the record of the search shall be kept by the EURODAC central system and the verifying authorities and Europol for the purpose of permitting the national data protection authorities and the European Data Protection Supervisor to monitor the compliance of data processing with Union data protection rules. **Personal data**, as well as the record of the search, **shall be erased** in all national and Europol files **after a period of one month**, if the data are not required for the purposes of the specific ongoing criminal investigation.

Information of the person concerned on the processing of his/her data: the person concerned should be informed regarding the purpose for which his or her data will be processed within EURODAC, and the use that could be made of them by the enforcement authorities.

Request to erase or correct data: provisions are added to take into account the wish of a person to see their data erased or corrected and the procedures whereby these data could be corrected or erased.

Prohibition of transfer to third countries: personal data obtained by a Member State or Europol and subsequently processed in national databases cannot be communicated or made available to third countries or international organisations or private entities, whether or not they are established in the Union.

Interests of the child: the best interests of the child should be a primary consideration in the fingerprinting procedure.

Audits: the national data protection authority should annually audit the use of EURODAC specifically as a law enforcement tool. The Member States have to present the European Parliament with annual reports. The EDPS should also produce every two years (and not every four, as in the Commission's proposal) an audit of the activities of personal data processing undertaken by the supervisory agencies. It is, moreover, stipulated that the supervisory agencies, both national and at Union level, should be provided with sufficient financial and human resources to be able adequately to supervise the use of and access to EURODAC data.

Technical provisions: lastly, technical provisions are proposed in regard to:

- a compilation of the quarterly (and not monthly) statistics on the effects of the new Regulation;
- a Business Continuity Plan to be developed taking into account maintenance needs and unforeseen downtime of the system;
- how data are transmitted in the event of a technical defect in the system;
- blocking of data relating to an applicant for international protection if that person is granted international protection in a Member State;
- the publication of a leaflet providing information on their rights to people whose fingerprint data are taken;
- a requirement for reports (in particular looking at the impact of the future Regulation on the protection of fundamental rights).