

Eurodac Regulation

2016/0132(COD) - 09/06/2017 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Civil Liberties, Justice and Home Affairs adopted the report by Monica MACOVEI (ECR, RO) 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 604/2013 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], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast).

The committee recommended that the European Parliament's position adopted at first reading should take into account the recommendations of the Consultative Working Party of the legal services of the European Parliament, the Council and the Commission. However, it made some amendments to the recast proposal which may be summarised as follows:

Extension of the system of comparison of Eurodac data to third-country nationals or "resettled" stateless persons: Members called for Eurodac to be extended to resettled third-country nationals and stateless persons for the purposes of identifying **secondary movements** of such persons.

The registration in Eurodac of information on resettled third-country nationals or stateless persons is designed to ensure that such persons enjoy the same level of protection and the same rights applicable to other beneficiaries of international protection as regards the processing of their data. This should also enable Member States to verify whether or not a third-country national or stateless person has **already been resettled in another Member State**.

Alphanumeric and biometric data: Members wanted to compare **the biometric or alphanumeric data** of the persons concerned with Eurodac data rather than fingerprints as proposed by the Commission in its proposal for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences.

In addition, Members considered that **fingerprints should always be preferred over facial images**. Where it is impossible to take the fingerprints of the third-country national or stateless person because his or her fingertips are damaged, either intentionally or not, or amputated, this Regulation should also permit the comparison of a facial image without fingerprints.

Derogation: Member States may derogate from in the case of illegally residing third-country nationals who entered the territory of the Union by lawfully crossing the external borders of the Schengen area and have overstayed the authorised period of stay by **no more than 15 days**.

Interoperability of data collection systems and the role of European agencies in the area of freedom, security and justice: given that the European Border and Coast Guard Agency plays a key role in the Union's efforts for a better management of external borders, and the prevention of illegal immigration and secondary movements, Members requested that it also have **access to Eurodac data** in order to be able to undertake risk analyses to the highest possible standard and to assist Member States with return related tasks. Those data should be processed in compliance with the data protection safeguards provided for in that Regulation.

As one of the tasks of the European Border and Coast Guard Agency and the [European Union Agency for Asylum](#), is the taking and transmitting of biometric data, the European Border and Coast Guard Agency and the European Union Agency for Asylum should also be **provided with their own interfaces so that they no longer need to rely on national infrastructures**. In the long run, those interfaces could be used as a single search interface.

Therefore, technological solutions should be developed to ensure the interoperability of Eurodac with the Schengen Information Systems (SIS), the Visa Information Systems (VIS), Europol, and any new relevant information systems developed in the area of freedom, security and justice, in order to enhance effective cooperation among Member States in managing external borders and combatting serious crime, including the system of entry/exit ([EES](#)) currently under construction.

Eu-LISA and DubliNet: in addition to the interoperability principles defined above, eu-LISA shall establish a **secure communication channel** between the EES Central System and Eurodac in order to allow full interoperability between both systems. A connection between the two systems is necessary in order for the biometric data of a third-country national registered in the EES to be transferred to Eurodac when registration of such biometric data is foreseen under this Regulation.

This specific channel, whose name would be **DubliNet**, would be managed by eu-LISA and would provide direct linkage and secure electronic transmission between the authorities of the Member States. The operational management of DubliNet shall consist of all the tasks necessary to ensure its availability **five days a week** during normal business hours.

Specific role of Europol: the future Regulation shall lay down the conditions under which the **European Police Office (Europol)** may request comparisons with Eurodac data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences falling within its mandate.

Europol shall designate an authority which is authorised to request comparisons with Eurodac data through its designated Europol access point in order to prevent, detect and investigate terrorist offences or other serious criminal offences. The designated authority shall be an operating unit of Europol.

Unaccompanied minors and minors: with a view to strengthening the protection of all migrant and refugee children, including unaccompanied minors who have not applied for international protection and children at risk of being separated from their families, Members requested that their biometric data can be retrieved for storage in the Central System and assist a Member State to find a family member or to identify possible links that these children may have with another Member State.

In the performance of those tasks, Member States should observe the principles laid down in the United Nations Convention on the Rights of the Child of 1989.

The biometric data of minors **from the age of six** shall be taken by officials trained specifically to enrol minor's fingerprints and to capture facial images in full respect of the best interests of the child.

The minor shall be informed in an age-appropriate manner, both orally and in writing, using leaflets and infographics and demonstrations specifically designed to explain the fingerprinting and facial image procedure to minors in a language he or she can understand.

Where a minor, in particular an unaccompanied or separated minor, **refuses to give his or her fingerprints or facial image** and there are reasonable grounds for believing that there are child safeguarding or protection risks, that minor should be referred to the competent national child protection

authorities, national referral mechanisms, or both. Those authorities should undertake an assessment of the minor's special needs in accordance with the relevant law with a view to finding a sustainable solution for the minor in full respect of the best interests of the child. Detention of minors shall be prohibited.

Application of sanctions in case of refusal to collect data: in order to ensure that all the persons concerned by the Regulation are registered in Eurodac, Member States may introduce, where appropriate, well justified administrative sanctions, in accordance with their national law and with full respect for the Charter of Fundamental Rights of the European Union, for non-compliance with the process of taking biometric data. Member States shall ensure that an opportunity for counselling has been provided to those persons in order to persuade them to cooperate with the procedure and to inform them of the possible implications of non-compliance. The administrative sanctions shall be effective, proportionate and dissuasive. **Detention should only be used as a means of last resort.**

Data retention period: Members considered that the maximum period for which the biometric data of third-country nationals or stateless persons who have applied for international protection may be kept in the central system should be limited to a **maximum of 5 years**.

Transfer of data collected from third countries: Members request that personal data obtained as a result of a search in 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 unless such a transfer is strictly necessary and proportionate in cases falling within Europol's mandate.

Personal data which originated in a Member State and are exchanged between Member States shall not be transferred to third countries, including if there is a real 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.

Study on the possibility of introducing facial recognition software to current Eurodac data: lastly, Members requested that, by 2020, eu-LISA should carry out a study on the technical feasibility and reliability of adding facial recognition software to the Central System currently planned.