Automated data exchange for police cooperation (“Prüm II”)

2021/0410(COD) - 08/02/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 451 votes to 94, with 10 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Purpose

The proposed regulation establishes a framework for the exchange of information between authorities responsible for the prevention, detection and investigation of criminal offences. The purpose of the Prüm II framework is to:

- **step up cross-border cooperation** particularly by facilitating the exchange of information between Member States’ competent authorities, in full respect of the fundamental rights of natural persons, including the right to respect for one’s private life and the right to the protection of personal data, in accordance with the Charter of Fundamental Rights of the European Union;

- allow Member State’s competent authorities to **search for missing persons** in the context of criminal investigations or on humanitarian grounds and to identify human remains provided that those authorities are empowered to conduct such searches and to carry out such identifications under national law.

DNA reference data

Member States should ensure the availability of DNA reference data from their national DNA databases for the purposes of automated searches by other Member States and Europol.

For the investigation of criminal offences, Member States should, at the time of initial connection to the router via their national contact points, conduct an **automated search** by comparing all the DNA profiles stored in their DNA databases with all the DNA profiles stored in all other Member States’ DNA databases and Europol data. The initial automated search should be conducted bilaterally.

Following the initial automated search of DNA profiles, Member States should conduct automated searches by comparing all the new DNA profiles added to their databases with all the DNA profiles stored in other Member States’ databases and Europol data. That automated searching of new DNA profiles should take place regularly.

The **national contact point** of the requesting Member State may decide to confirm a match between two sets of dactyloscopic data. Where it decides to confirm a match between two sets of dactyloscopic data, it should inform the requested Member State and shall ensure that at least one qualified member of staff conducts a manual review in order to confirm that match with dactyloscopic reference data received from the requested Member State.

Dactyloscopic data

Member States should allow national contact points of other Member States and Europol access to the dactyloscopic reference data in their national databases established for that purpose to conduct automated searches by comparing dactyloscopic reference data. They should take appropriate measures to ensure the **confidentiality and integrity** of dactyloscopic data sent to other Member States or Europol, including their encryption. Europol should inform the Member States, the Commission and eu-LISA of its maximum search capacities per day for identified and unidentified fingerprint data. Member States or Europol may temporarily or permanently increase these search capacities at any time, in particular in an emergency.

Automated searching of vehicle registration data

Member States should allow national contact points of other Member States and Europol access to the following national vehicle registration data to conduct automated searches in individual cases. Searches conducted with data related to the owner or holder of the vehicle shall only be conducted in the case of suspects or convicted persons.

Automated searching of facial images

For the prevention, detection and investigation of criminal offences **punishable by a maximum term of imprisonment of at least one year** under the law of the requesting Member State, Member States should allow national contact points of other Member States and Europol access to the facial image reference data in their national databases to conduct automated searches.

Member States should take appropriate measures to ensure the confidentiality and integrity of facial images sent to other Member States or Europol, including their encryption.

Police records

Given the sensitivity of the data concerned, exchanges of national police record indexes under this Regulation should only concern the data of **persons convicted or suspected of having committed a criminal offence**. In addition, it should only be possible to conduct automated searches of national police record indexes for the purpose of preventing, detecting and investigating a criminal offence punishable by a maximum term of imprisonment of at least one year under the law of the requesting Member State.

Missing persons and unidentified human remains

Where a national authority has been so empowered by national legislative measures, it may conduct automated searches using the Prüm II framework for the following purposes only: (a) searching for missing persons in the context of criminal investigations or on humanitarian grounds;

(b) identifying human remains.

Data protection

Prior to connecting their national databases to the router or European Police Record Index System (EPRIS), Member States should conduct a data protection impact assessment.

Member States and Europol should ensure the accuracy and relevance of personal data which are processed pursuant to this Regulation. Where a Member State or Europol becomes aware of the fact that data which have been supplied are incorrect or no longer up to date or should not have been supplied, it should notify the Member State which received the data or Europol, as appropriate, without undue delay. All Member States concerned or Europol, as the case may be, should correct or delete the data accordingly without undue delay.

Three years following the start of operations of the router and EPRIS and every four years thereafter, the Commission should produce an evaluation report that includes an assessment of the application of this Regulation by the Member States and Europol, in particular of their compliance with the relevant data protection safeguards.