PRESS RELEASE

EDPS/2017/12

Brussels, 13 December 2017

EDPS calls for consistency in EU approach to criminal records

There is a clear need for the EU to develop a more efficient system for exchanging information on the criminal records of non-EU citizens. At the same time, any proposal to update the current system must ensure consistency with the EU Charter of Fundamental Rights and the Lisbon Treaty and fully respect data protection principles, the European Data Protection Supervisor (EDPS) said today, as he published his Opinion on the Commission's Proposal for a Regulation on ECRIS-TCN.

Member States use the current European Criminal Records Information Service (ECRIS) primarily to facilitate judicial cooperation, through the exchange of information relating to criminal convictions. In 2016, the Commission proposed a Directive on ECRIS aimed at improving this system. They wanted to make it easier for Member States to exchange information on non-EU citizens, known as third-country nationals (TCN). The proposed Regulation on ECRIS-TCN aims to complement the Directive and address some of the technical problems encountered in its application, most notably by changing the system used to identify which Member States hold information on criminal convictions relating to non-EU citizens from a decentralised system to a central system.

Giovanni Buttarelli, EDPS, said: "*There is a clear need to improve the ECRIS system to better facilitate the exchange of information on the criminal records of non-EU citizens, and we support the Commission's efforts to do this. At the same time, it is vital that our approach is consistent. Firstly, this means ensuring that any difference and specificity in the treatment of the personal data of non-EU citizens and EU nationals is fully justified. Secondly, it means ensuring that the Regulation and the Directive fully respect the EU Charter of Fundamental Rights and the requirements for any lawful limitation of these rights.*"

The EDPS notes that the proposed Regulation would establish a central database in which identity information, including fingerprints and facial images, would be stored. It would be hosted by eu-LISA, which currently hosts the majority of the EU's large-scale IT databases in the area of freedom, security and justice, thus facilitating the interoperability of these databases, a key objective for the Commission, outlined in a proposal published yesterday. The EDPS recommends that the Commission complete a thorough impact assessment to determine whether a central database represents the least intrusive way of identifying which Member States hold information on the criminal convictions of non-EU citizens. He also calls attention to his recent Opinion on the Commission's proposal for a Regulation on eu-LISA, in which he stressed the need to assess the impact on fundamental rights of concentrating all such databases in one agency.

The original ECRIS legislation was developed before the Lisbon Treaty and the EU Charter of Fundamental Rights came into force. Any plans to amend this law must therefore bring ECRIS and ECRIS-TCN up to the standards specified in the Charter and Article 16 of the TFEU. This means clearly defining for what purposes, other than for criminal proceedings, the data in ECRIS or ECRIS-TCN will be used, and establishing that these purposes are both necessary and proportionate. This includes demonstrating that any plans to provide EU bodies with access to ECRIS-TCN is truly necessary, proportionate and compliant with their tasks. Access should also be appropriately limited to ensure that any difference in the treatment of non-EU citizens and EU nationals is fully justifiable.

As the data to be stored in ECRIS-TCN is very sensitive, the EDPS stresses that it must only be processed if it is strictly necessary to do so. In cases where Member States carry out a search for a purpose other than criminal proceedings, they should only be notified of a *hit* if the national law of the Member State holding the relevant information permits this. Fingerprints should only be processed in cases where identification of the individual cannot be achieved by other means, and the need to store and process facial images must be clearly established.

Improvements to the ECRIS system are undoubtedly needed. However, we must ensure that these improvements do not come at the expense of the fundamental rights to data protection and privacy applicable to all those whose data is processed in the EU.

Background information

The rules for data protection in the EU institutions, as well as the duties of the European Data Protection Supervisor (EDPS), are set out in **Regulation (EC) No 45/2001**. The EDPS is a relatively new but increasingly influential independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

Giovanni Buttarelli (EDPS) and **Wojciech Wiewiórowski** (Assistant EDPS) are the members of the institution, appointed by a joint decision of the European Parliament and the Council. Assigned for a five year term, they took office on 4 December 2014.

Large-scale IT systems: databases created by the EU are considered to be large-scale according to the number of people using the system for different purposes, the amount of data collected, stored, accessed, manipulated and the number of connections between components, among other things. SIS II, VIS and Eurodac are three examples of large-scale IT systems in the area of border and police control.

Personal information or data: any information relating to an identified or identifiable natural (living) person. Examples include names, dates of birth, photographs, video footage, email addresses and telephone numbers. Other details such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered as personal data.

Processing of personal data: According to Article 2(b) of Regulation (EC) No 45/2001, processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." See the glossary on the EDPS website.

EU Data Protection Reform package:

On 25 January 2012, the European Commission adopted its reform package, comprising two legislative proposals:

- a general Regulation on data protection which was adopted on 24 May 2016, applicable as of 25 May 2018; and
- a specific Directive on data protection in the area of police and justice, adopted on 5 May 2016, applicable as of 6 May 2018.

The official texts of the Regulation and the Directive are now recognised as law across the European Union (EU). Member States have two years to ensure that they are fully implementable in their countries by May 2018.

The European Data Protection Supervisor (EDPS) is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy;
- cooperating with similar authorities to ensure consistent data protection.

The EDPS Opinion is available on the EDPS website
For more information: press@edps.europa.eu
EDPS - The European guardian of data protection
www.edps.europa.eu
Follow us on Twitter:
@EU_EDPS