How will the data protection reform help fight international crime?

Factsheet | January 2016 EN

Věra Jourová
Commissioner for Justice, Consumers and Gender Equality

Directorate-General for Justice and Consumers

The Data Protection Police Directive is part of the new EU's data protection rules adopted in April 2016.
The reform was made to make the EU's data protection standards fit for the digital age, and future-proof for technological developments.
The Directive protects individuals when their personal data are processed by authorities for the purposes of **prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties**.
The rules deliver on the EU's Agenda on Security, the EU's strategy in the fight against terrorism, organised crime and cybercrime. The exchange of such data is essential in the **fight against terrorism and cross-border crime**. Thanks to the new rules, sharing such data will be more efficient both at EU-level and international level. They will build trust and ensure legal certainty cross-border.

HOW DOES THIS DIRECTIVE UPHOLD FUNDAMENTAL RIGHTS?

Under the new Directive, everyone's personal data must be processed lawfully, fairly, and only for a specific purpose, a purpose that is always linked to the fight against crime.

The Directive ensures that personal data processing across the EU complies with the principles of legality, proportionality, and necessity, with appropriate safeguards for individuals. It also ensures completely independent supervision by national data protection authorities, and effective judicial remedies.

Introducing data protection as a standard

Police and criminal justice authorities will apply the *principles of data protection by design and data protection by default* at the beginning of any process to do with personal data, for example when developing new databases. Those responsible for processing personal data will be held more accountable for their work. For

The right to personal data protection is a fundamental right in the EU. Victims and witnesses, but also suspects of crimes have the right to have their data duly protected in the context of a criminal investigation or a law enforcement action. At the same time, more harmonised laws will make it easier for police or prosecutors to work together in cross-border investigations and to combat crime and terrorism more effectively across Europe.

example, authorities must appoint data protection officers to take care of personal data protection within their organisation. They must also ensure the national supervisory authority is notified of serious data breaches as soon as possible.

HOW DOES THE DIRECTIVE IMPROVE LAW ENFORCEMENT AUTHORITIES' WORK?

In order to effectively fight crime, law enforcement needs efficient and robust rules on personal data exchanges at national, European and international level. Setting EU-wide rules related to personal data protection in the field of criminal justice will make cooperation easier for the police and criminal justice authorities across the EU.

Saving time and money

Data processing will be less costly and time-consuming. Police and criminal justice authorities will no longer have to apply different sets of data protection rules according to the origin of the personal data. The new rules apply to both domestic processing and cross-border transfers of personal data.

Stronger international cooperation

Cooperation between EU police and criminal justice authorities with non-EU countries will also be strengthened since there will be clearer rules for international data transfers related to criminal offences. The new rules will ensure that transfers take place with an adequate level of data protection.

Any questions? http://ec.europa.eu/justice/data-protection/index_en.htm Contact Europe Direct: 00 800 67 89 10 11 http://europa.eu/europedirect/

With the old rules

Individuals across EU already have the right to access their personal data processed by police, prosecutors or criminal courts. However, exercising that right differs from one Member State to another.

For example, some national authorities charge fees. Others do not reply to individual requests within reasonable deadlines, and only allow indirect access to personal data (e.g. through national supervisory authorities.) The reply often leaves the requester doubting about the status of his or her personal data and the available legal remedies. This puts individuals in a difficult situation, in particular considering that ever more personal data are being processed cross-border.

With the new rules

Every citizen in the EU has an equal right of access to their personal data. Individuals always have the right to approach the police and criminal justice authorities directly and ask for access to their personal data.

If those authorities decide to accept such a request, they have to provide the personal data free of charge. The authorities may also decide to limit the right of access, in particular when they want to prevent hindering an ongoing investigation or to protect national security or the rights and freedoms of others. Such limitations must be in line with the necessity and proportionality requirements of EU law, as interpreted by the Court of Justice of the European Union and the European Court of Human Rights.

In specific cases where the authorities give a neutral reply to an individual ("we can neither confirm nor deny we are processing your personal data"), they have to inform them about the right to lodge a complaint with the national data protection supervisory authority. These authorities carry out the necessary verifications or a review of personal data held by the authorities. Finally, individuals always have the right to ask for judicial supervision of this entire procedure.

Publications Office

Print ISBN 978-92-79-60497-3 doi:10.2838/355814 DS-02-16-740-EN-D
PDF ISBN 978-92-79-60494-2 doi:10.2838/57129 DS-02-16-740-EN-N