Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 27/07/2015 - Document attached to the procedure

European Data Protection Supervisor (EDPS) recommendations on the EU's options for data protection reform.

On 24 June 2015, the European Parliament, the Council and the European Commission entered co-decision negotiations on the proposed General Data Protection Regulation (GDPR), a procedure known as an informal 'trilogue'. The three institutions are committed to dealing with the GDPR as part of the wider data protection reform package which includes the proposed directive for police and judicial activities.

This opinion **updates the opinion published in March 2012** (which remains valid) to engage more directly with the positions of the co-legislators and to propose specific recommendations to assist the participants in the trilogue in reaching the right consensus on time.

A rare opportunity: the EDPS recalled that data protection reform is of central importance:

> **1. The EU is in the last mile of a marathon effort to reform its rules on personal information**. The General Data Protection Regulation will potentially affect, for decades to come, all individuals in the EU, all organisations in the EU who process personal data and organisations outside the EU who process personal data on individuals in the EU.
>
> **2. Effective data protection empowers the individual and galvanises responsible businesses and public authorities**. Laws in this area are complex and technical, requiring expert advice, in particular that of independent data protection authorities who understand the challenges of compliance. The GDPR is likely to be one of the longest in the Union's statute book, so now the EU must aim to be selective, focus on the provisions which are really necessary and avoid detail which as an unintended consequence might unduly interfere with future technologies. The texts of each of the institutions preach clarity and intelligibility in personal data processing: so the GDPR must practice what it preaches, by being as concise and easy to understand as possible.
>
> **3. The EU needs a new deal on data protection**. The rest of the world is watching closely. The quality of the new law and how it interacts with global legal systems and trends is paramount.
>
> **EDPS recommendations**: the options on the table, in the form of the respective texts preferred by the Commission, Parliament and Council, each contain many worthy provisions, but **each can be improved**.

The recommendations are driven by three abiding concerns:

- **a better deal for citizens**: for the EDPS, the starting point is the **dignity of the individual** which transcends questions of mere legal compliance. The point of reference is the principles at the core of data protection, that is, Article 8 of the Charter of Fundamental Rights. In this regard, the EDPS concentrated on the following issues:

- **clarify the term 'personal information'**: individuals should be able to exercise more effectively their rights with regard to any information which is able to identify or single them out, even if the information is considered 'pseudonymised';
- **all data processing must be both lawful and justified**: for instance: (i) personal data should only be used in ways compatible with the original purposes for collection; (ii) consent is one possible legal basis for processing, but it is necessary to prevent coercive tick boxes where there is no meaningful choice for the individual and where there is no need for data to be processed at all; (iii) the EU should not open the door for direct access by third country authorities to data located in the EU;
- **more independent, more authoritative supervision**: (i) authorities should be able to hear and to investigated complaints and claims brought by data subjects or bodies, organisations and associations; (ii) individual rights enforcement requires an effective system of liability and compensation for damage caused by the unlawful data processing.

2. Rules which will work in practice: each of the three texts demands **greater clarity and simplicity** from those responsible for processing personal information. Equally, technical obligations must also be concise and easily-understood if they are to be implemented properly by controllers. This implies:

- **effective safeguards, not procedures**: the EDPS recommends a scalable approach which reduces documentation obligations on controllers into single policy on how it will comply with the regulation taking into account the risks, with compliance demonstrated transparently, whether for transfers, contracts with processors or breach notifications. It also recommends requiring notification of data breaches to the supervisory authority and data protection impact assessments only where the rights and freedoms of data subjects are at risk;
- **a better equilibrium between public interest and personal data protection**: data protection rules should not hamper historical, statistical and scientific research which is genuinely in the public interest;
- **trusting and empowering supervisory authorities**: supervisory authorities should be allowed to issue guidance to data controllers and to develop their own internal rules of procedure in the spirit of a simplified, easier application of the GDPR by one single supervisory authority (the '**One Stop Shop'**) close to the citizen ('**proximity'**).

3. Rules which will last a generation: it is reasonable to expect a similar timeframe before the next major revision of data protection rules, **perhaps not until the late 2030s**. Long before this time, data-driven technologies can be expected to have converged with artificial intelligence, natural language processing and biometric systems.

These technologies are challenging the principles of data protection. A future-oriented reform must therefore be predicated on the dignity of the individual and informed by ethics. It must redress the imbalance between innovation in the protection of personal data and its exploitation, making safeguards effective in our digitised society.

Faced with these challenges, the EDPS:

- considers that the **reform should reverse the recent trend towards secret tracking and decision making on the basis of profiles hidden from the individual;** fuller transparency from controllers is needed;
- strongly supports the introduction of the principles of data protection **by design and by default** as a means of kick-starting market-driven solutions in the digital economy;
- allows a **direct transfer of data** from one controller to another on the data subject's request and entitling data subjects to receive a copy of the data which they themselves can transfer to another controller.

Unfinished business: the EDPS noted that the adoption of a future-oriented EU data reform package will be an impressive but nonetheless incomplete achievement.

Directive 2002/58/EC (the 'ePrivacy Directive') will have to be amended.

The EU requires a **clear framework for the confidentiality of communications**, an integral element of the right to privacy, which governs all services enabling communications, not only providers of publicly available electronic communications. This must be done by means of a legally-certain and harmonising regulation.

At a time when people's trust in companies and governments has been shaken by revelations of mass surveillance and data breaches, the EDPS stresses that this confers considerable responsibility on EU law-makers whose decisions this year can be expected to have an impact not beyond Europe.