DPA: European Data Protection Supervisor (EDPS)

TITLE: Opinion 7/2015 - Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability.

DATE: 19 November 2015

KEY WORDS: big data, European Data Protection Supervisor (EDPS), transparency, user control, data protection by design, accountability

WEBSITE LINK:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

ABSTRACT:

On 19 November 2015 the European Data Protection Supervisor issued Opinion 7/2015 entitled "Meeting the challenges of big data". It deals with how big data can bring benefits and represent opportunities for the society as a whole if companies comply with data protection laws and find innovative ways to do so. The opinion outlines the strategy of the European Data Protection Supervisor to reach that goal, also in light of the ongoing data protection reform.

ASSESSMENT:

Opinion 7/2015 can be considered as the manifesto of the European Data Protection Supervisor (EDPS) for more responsible big data practices in the EU. The EDPS strategy consists in achieving a "Big Data Protection Ecosystem" through the implementation of four main principles, namely: transparency, user control, data protection by design and accountability. One of the main arguments stressed by the EDPS is that in order to build the above-mentioned ecosystem it is not only necessary that companies and organisations enact more transparent data processing practices but also that individuals get a higher degree of control over their personal data. Although Opinion 7/2015 does not deal with cooperation among data protection authorities (DPAs), it touches upon several aspects which are relevant to the PHAEDRA project. They are illustrated as follows.

The EDPS is aware and concerned about the potential impact of processing of huge amount of data on the rights and freedoms of individuals. However, it argues that big data and fundamental rights should not be incompatible. Instead, it is necessary to apply data protection law to big data but in an innovative way. As the EDPS points out, this would be possible by protecting fundamental rights more dynamically in the world of big data and by

implementing new principles which have been developed in data protection law over the years, namely transparency, user control, data protection by design (and by default) and accountability.

1. Transparency

The EDPS argues that companies that process large volumes of personal data should implement transparent policies by providing data subjects with clear information on what data about them is processed and on how and for what purposes such data is used. This obligation should include also information on profiling and in particular on the logic used in algorithms. In addition, companies should implement effective notices regarding their data processing practices.

2. User control

Individuals should have (and be given) greater control over their personal data. As the EDPS notes, this will allow them to make more genuine and better informed choices. The concept of user control implies that the individual should have a clear understanding of what he agrees to and consequently have a freely-given choice.[1] These objectives could be reached by strengthening access rights, by putting into practice the idea of data portability and by implementing effective opt-out mechanisms.

3. Data protection by design

The EDPS holds that data protection should be embedded into products and services. Although law, regulations, contractual terms and privacy policies can ensure compliance with data protection laws, they do not suffice on their own. Instead, innovative and privacy-friendly engineering can contribute to that aim, as well as privacy-friendly organisational arrangements and business practices.

4. Accountability

According to the EDPS it is necessary that data controllers put in place internal mechanisms and control systems to demonstrate compliance with data protection laws, in order to be held accountable to data subjects and supervisory authorities. Accountability should not be a one-off exercise but should entail regular and continuous verification of data processing practices. In particular, this verification should be aimed to assess "whether any secondary use of data

[1] As the EDPS underlines "mere ticking of a box without understanding of what we agree to, and without meaningful choice whether we do so, is not sufficient to signify our consent for complex big data applications". See p. 11 of Opinion 7/2015.

complies with the principle of purpose limitation"; "whether data initially used in one context can be considered adequate, relevant, and proportionate to be reused in another context"; and "whether, in the absence of obtaining consent from the individuals, an organisation can rely on its legitimate interest to process any data".[2]

It is worth mentioning that opinion 7/2015 acknowledges that the role of DPAs will be crucial in the development of the above-mentioned Big Data Protection Ecosystem. Hence, the EDPS stresses that they must be equipped not only with legal powers and strong instruments (such as the power to apply meaningful remedies and impose effective fines), but also with adequate resources to meet the challenges of big data.

[2] See pp. 15-16 of Opinion 7/2015.