

## EUROPEAN DATA PROTECTION SUPERVISOR

### **Executive Summary of the Opinion of the European Data Protection Supervisor on ‘Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability’**

*(The full text of this opinion can be found in English, French and German on the EDPS website [www.edps.europa.eu](http://www.edps.europa.eu))*

(2016/C 67/05)

#### **‘The right to be let alone is indeed the beginning of all freedom’<sup>(1)</sup>.**

Big data, if done responsibly, can deliver significant benefits and efficiencies for society and individuals not only in health, scientific research, the environment and other specific areas. But there are serious concerns about the actual and potential impact of processing of huge amounts of data on the rights and freedoms of individuals, including their right to privacy. The challenges and risks of big data therefore call for more effective data protection.

Technology should not dictate our values and rights, but neither should promoting innovation and preserving fundamental rights be perceived as incompatible. New business models exploiting new capabilities for the massive collection, instantaneous transmission, combination and reuse of personal information for unforeseen purposes have placed the principles of data protection under new strains, which calls for thorough consideration on how they are applied.

European data protection law has been developed to protect our fundamental rights and values, including our right to privacy. The question is not whether to apply data protection law to big data, but rather how to apply it innovatively in new environments. Our current data protection principles, including transparency, proportionality and purpose limitation, provide the baseline we will need to protect more dynamically our fundamental rights in the world of big data. They must, however, be complemented by ‘new’ principles which have developed over the years such as accountability and privacy by design and by default. The EU data protection reform package is expected to strengthen and modernise the regulatory framework<sup>(2)</sup>.

The EU intends to maximise growth and competitiveness by exploiting big data. But the digital single market cannot uncritically import the data-driven technologies and business models which have become economic mainstream in other areas of the world. Instead it needs to show leadership in developing accountable personal data processing. The internet has evolved in a way that surveillance — tracking people’s behaviour — is considered as the indispensable revenue model for some of the most successful companies. This development calls for critical assessment and search for other options.

In any event, and irrespective of the business models chosen, organisations that process large volumes of personal information must comply with applicable data protection law. The European Data Protection Supervisor (EDPS) believes that responsible and sustainable development of big data must rely on four essential elements:

- organisations must be much more transparent about how they process personal data,
- afford users a higher degree of control over how their data are used,
- design user-friendly data protection into their products and services, and
- become more accountable for what they do.

When it comes to transparency, individuals must be given clear information on what data are processed, including data observed or inferred about them; better informed on how and for what purposes their information is used, including the logic used in algorithms to determine assumptions and predictions about them.

<sup>(1)</sup> *Public Utilities Commission v Pollak*, 343 U.S. 451, 467 (1952) (Justice William O. Douglas, dissenting).

<sup>(2)</sup> On 25 January 2012, the European Commission adopted a package for reforming the European data protection framework. The package includes: (i) a ‘Communication’ (COM(2012) 9 final); (ii) a proposal for a general ‘Data Protection Regulation’ (‘proposed Regulation’) (COM(2012) 11 final); and (iii) a proposal for a ‘Directive’ on data protection in the area of criminal law enforcement (COM(2012) 10 final).

User control will help ensure that individuals are more empowered to better detect unfair biases, to challenge mistakes. It will help prevent the secondary use of data for purposes that do not meet their legitimate expectations: With a new generation of user control, individuals will, where relevant, be given more genuine and better informed choice and enjoy greater possibilities themselves to use their personal data better.

Powerful rights of access and to data portability and effective opt-out mechanisms may serve as a precondition to allow users more control over their data, and may also help contribute to the development of new business models and more efficient and transparent use of personal data.

By building data protection into the design of their systems and processes, and adjusting data protection to allow more genuine transparency and user control, accountable controllers will also be able to benefit from the advantages of big data while at the same time ensuring that individuals' dignity and freedoms are respected.

But data protection is only part of the answer. The EU needs to deploy in a more coherent way the modern tools available, including in the area of consumer protection, antitrust, research and development, to ensure safeguards and choice in the marketplace where privacy-friendly services can thrive.

In order to answer the challenges of big data we need to allow innovation and protect fundamental rights at the same time. It is now up to companies and other organisations that invest a lot of effort into finding innovative ways to make use of personal data to use the same innovative mindset when implementing data protection law.

Building on previous contributions by academia and many regulators and stakeholders, the EDPS wants to stimulate a new open and informed discussion in and outside the EU, by better involving civil society, designers, companies, academics, public authorities and regulators on how best to use industry's creative potential to implement the law and safeguard our privacy and other fundamental rights the in best possible way.

## 6. Next steps: putting the principles into practice

In order to answer the challenges of big data we need to allow innovation and protect fundamental rights at the same time. To achieve this, the established principles of European data protection law should be preserved but applied in new ways.

### 6.1. Future-oriented Regulation

Negotiations on the proposed General Data Protection Regulation are in the final stages. We have urged the EU legislators to adopt a data protection reform package that strengthens and modernises the regulatory framework so that it remains effective in the era of big data by strengthening the individuals' trust and confidence online and in the digital single market <sup>(1)</sup>.

In Opinion 3/2015, accompanied by recommendations for a full text of the proposed Regulation, we made it clear that our current data protection principles, including necessity, proportionality, data minimisation, purpose limitation and transparency must remain key principles. They provide the baseline we need to protect our fundamental rights in a world of big data <sup>(2)</sup>.

At the same time, these principles must be strengthened and applied more effectively, and in a more modern, flexible, creative, and innovative way. They must also be complemented by new principles such as accountability and data protection and privacy by design and by default.

Increased transparency, powerful rights of access and data portability, and effective opt-out mechanisms may serve as preconditions to allow users more control over their data, and may also help contribute to more efficient markets for personal data, to the benefit of consumers and businesses alike.

<sup>(1)</sup> EDPS Opinion 3/2015.

<sup>(2)</sup> We must resist the temptation to water down the current level of protection in an attempt to accommodate a perceived need for a more lax regulatory approach when it comes to big data. Data protection must continue to apply to processing in its entirety, including not only use of the data but also its collection. There is also no justification for blanket exceptions for processing of pseudonymous data or for processing publicly available data. The definition of personal data must remain intact but could do with further clarifications in the text of the Regulation itself. Indeed, it must cover all data that relate to any individual who is identified, singled out, or may be identified or singled out — whether by the data controller or any other party.

Finally, extending the scope of EU data protection law to organisations targeting individuals in the EU, and equipping data protection authorities with the powers to apply meaningful remedies, including effective fines, as the proposed Regulation would provide, will also be a key requirement to effectively enforce our laws in a global environment. The reform process plays a key role in this respect.

To ensure that the rules are effectively enforced, independent data protection authorities must be equipped not only with legal powers and strong instruments, but also with the resources required to match their capacity with the growth of data driven business.

#### 6.2. How EDPS will advance this debate

Good regulation, while essential, is insufficient. Companies and other organisations that invest a lot of effort into finding innovative ways to make use of personal data should use the same innovative mindset when implementing data protection principles. Data protection authorities, in turn, should enforce and reward effective compliance, and avoid imposing unnecessary bureaucracy and paperwork.

The EDPS, as announced in the EDPS strategy 2015-2019, aims to contribute to fostering these efforts.

We intend to establish an external ethics advisory group composed of distinguished and independent personalities with a combined experience in multiple disciplines that can '*explore the relationships between human rights, technology, markets and business models in the 21st century*', analyse the impact of big data in depth, assess the resulting changes of our societies and help indicate the issues that should be subject to a political process <sup>(1)</sup>.

We will also develop a model for honest information policies for EU bodies offering online services which can contribute to best practice for all controllers.

Finally, we will also facilitate discussions, for example, with the view to identify, encourage and promote best practice to increase transparency and user control and explore opportunities for personal data stores and data portability. The EDPS intends to organise a 'big data protection' workshop for policymakers and persons handling large volumes of personal information in the EU institutions and external experts, and to identify where further specific guidance is needed, and to facilitate the work of the Internet Privacy Engineering Network ('IPEN') as an interdisciplinary knowledge hub for engineers and privacy experts.

Done at Brussels, 19 November 2015.

Giovanni BUTTARELLI

*European Data Protection Supervisor*

---

<sup>(1)</sup> EDPS Opinion 4/2015.