

Peter Hustinx
European Data Protection Supervisor

Ensuring more effective data protection in an age of big data¹

There is no doubt that current legal safeguards for privacy and personal data protection need to be reinforced in view of the challenges posed by technology and globalisation. The rapid growth of big data applications is one of the new phenomena, but certainly not the only relevant development. This is why we are now approaching the final phase of a wide ranging reform of the current EU legal framework for data protection. This will deliver stronger rights for data subjects, stronger responsibilities for data controllers, and stronger supervision and enforcement of data protection rules across the EU.

Stronger rights for data subjects imply more effective means to achieve access, correction or erasure of personal data, or to object to data processing on and off line. The recent judgment of the Court of Justice in the *Google Spain* case has highlighted the potential of rights and remedies available for individuals. Consent - i.e. giving, withholding or withdrawing consent - is another tool for individuals to control or influence the collection and use of their personal data. However, consent is also vulnerable for abuse, particularly online. Where it is needed - not always - it should be real consent: not only free, informed and specific, but also explicit.

Many online operators seem to love consent, but they want it at the lowest possible price. This has resulted in dubious practices, where data subjects are completely left in the dark. Making sure that consent is provided at the right conditions is therefore important, but also seen as a threat for prevailing business practices. In reality, the issue is not consent, but *legitimacy* of data processing. In EU data protection law, unlike in other legal systems, such legitimacy is not assumed, but to be ensured by the data controller. Moreover, consent is only one of the available options to ensure legitimacy, and not always the most appropriate one.

Stronger responsibilities for controllers will therefore also require them to think better about the legitimacy of what they intend to do. The new legal framework will require controllers to verify if - and where necessary demonstrate that - any consent relied upon was valid, and that other legal grounds relied upon are also sound and convincing. This and other requirements will apply to the use of big data technology, whenever personal data are processed in that context. Therefore, if big data operators want to be successful, they should better invest in good privacy and data protection, preferably at the design stage of their projects.

Stronger supervision and enforcement of data protection rules across the EU will help data controllers to keep their focus in this respect. It should be no surprise that the new framework

¹ Contribution to European Voice online debate on big data and consent, 14 July 2014

will also provide for strong sanctions - administrative fines of millions of euros - for the most serious cases where these rules have not been respected. In this context, we have recently also published a preliminary opinion on the question how competition law, consumer protection and data protection might interact in the era of big data.² We have called for closer interaction of the relevant regulators on both sides of the Atlantic. In short: big data will also require big countervailing powers.

² EDPS Preliminary Opinion, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', 26 March 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/EDPS-2014-06-Big-Data_EN.pdf