Debunking EU Data Protection Reform

fieldfisher

10 things you should know

1

The pool of data which is potentially personal gets deeper

Unique identifiers (e.g. IP addresses) that can single individuals out will be included within the definition of personal data. Pseudonymous data (e.g. information that can single individuals out, but does not directly identify them) will benefit from certain relaxations of the GDPR. "Sensitive data" will include "genetic data" and "biometric data".

2

Out-of-scope today, in scope in the future – what is caught?

The GDPR expands the territorial scope of application of EU data protection law to capture not only the processing of personal data by a controller or a processor established in the EU, but also any processing of personal data of data subjects residing in the EU, where the processing relates to the offering of goods or services to them, or the monitoring of their behaviour.

3

You may need to "rethink" your legal justification for processing personal data

Businesses that receive personal data as a third party will need to carefully assess whether they can rely on the "legitimate interests" ground for processing. Further, "consent" as a lawful ground for processing will be subject to strict conditions. Businesses should revisit existing data collection practices and consider consent mechanisms which provide more flexibility in the future.

4

"Souped-up" individual rights

The GDPR requires the provision of additional information in response to individual access requests and a prescribed way of presenting the right to object to direct marketing. New rights for individuals will also be introduced, e.g. "the right to be forgotten", and a right of "data portability" in certain circumstances.

5

Your Big Data analytics and profiling activities may be seriously curtailed

Explicit consent will be required to process personal data for profiling in certain circumstances. Businesses should identify the nature of any profiling activities that they undertake and think creatively about possible consent mechanisms.

6

You should design for compliance

Under the "privacy by design" requirement of the GDPR, you will need to design compliant policies, procedures and systems at the outset of product development. The "privacy by default" principle will require that, by default, only personal data that are necessary for a specific purpose are to be processed.

7

Accountability principles = more paperwork?

The GDPR introduces an accountability principle which imposes significant documentation requirements. Businesses should review their existing data protection policies and procedures to ensure that they meet the expected standards.

8

You may need to appoint a DPO

The GDPR requires both data controllers and data processors to appoint a DPO in certain specified circumstances, e.g. if its core activities involve the regular and systematic monitoring of individuals on a large scale. Businesses that carry out profiling activities as a core activity are likely to caught by the new requirement.

9

Data transfer restrictions are here to stay, but so are BCR

You will still have to jump through hoops in order to legitimately transfer data outside of Europe. The GDPR expressly acknowledges the validity of Binding Corporate Rules (BCR) as a valid legal solution – BCR are here to stay.

10

Enforcement under the GDPR – What happens if you get it wrong?

The GDPR introduces fines for non-compliance of up to 4% of total worldwide annual turnover for undertakings, or 20,000,000 EUR, whichever is greatest. Controllers and processors may also be subject to court proceedings initiated by individuals and may have to pay compensation to individuals in respect of GDPR infringements.

Europe's new General Data Protection Regulation (GDPR) will come into force on 25 May 2016. Businesses then have a two year window in which to become GDPR compliant before the Regulation becomes applicable on 25 May 2018. Any business touching upon personal data should start considering the future rules now and what they mean for their business, not least because there are some significant changes to prepare for. The changes the GDPR brings will ensure that the EU data protection framework is appropriate for a digital age. It will also introduce a much more harmonised data protection regime across EU Member States. This "infographic" and the associated Fieldfisher "Getting to Know the GDPR" Blog Series prepares you for some of the likely practical consequences of the GDPR.

Click Here