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

You may be subject to the new regime even if you are not required to comply with the current one. Even if you are not established in the EU, you may be caught by the new rules if you are a data controller whose processing activities are directed at EU residents and/or you process personal data in relation to offering goods or services to, or monitoring the behaviour of, EU residents. One of the more significant changes is that data processors established in the EU will fall within aspects of the proposed Regulation (with new obligations on processors specifically outlined).

The pool of data which is potentially personal gets deeper

The definition of personal data proposed under the new regime is very broad. Unique identifiers (e.g. IP addresses) that can single individuals out are likely to be included expressly within the definition. It is possible that pseudonymous data (e.g. information that can single individuals out, but does not directly identify them) would be subject to lower data protection standards. However, such data would become personal data if profiling activities enable the identification of individuals from the data. The updated concept of “sensitive data” is likely to include genetic data.
If you receive personal data from a third party, you may need to “re-think” your legal justification for processing it

Under the current regime, the “legitimate interests” pursued by a business or a third party to whom the business discloses personal data is a valid lawful justification for processing personal data. The ability of third parties to whom personal data are disclosed to rely on this lawful ground for processing is under threat under the proposed new regime. In addition, “consent” as a lawful ground for processing is likely to be subject to very tight and strict conditions. It may be necessary to revisit the prior basis of consent for certain data and this is an area where businesses may be able to vary existing data collection practices and pre-empt the changes with consent mechanisms which provide more flexibility in the future.

You are likely to need to take account of individuals’ new and enhanced rights

There are a number of proposed tweaks to existing rights, for example, a requirement to provide additional information in response to a subject access request and a prescribed way of presenting the right to object to direct marketing. New data subject rights are also proposed, e.g. “the right to be forgotten” and a new right of “data portability”. This latter right may mean that businesses will be required to provide copies of personal data records in a standardised electronic data format.

Your Big Data analytics and profiling activities may be seriously curtailed

Under the proposed new regime, explicit consent is likely to be required in most instances in order to process personal data for profiling. Business should identify the nature of any profiling activities that they undertake and think creatively about possible consent mechanisms.

Think privacy - you will need to design your products and services for compliance and minimise the personal data processed

Under the proposed “privacy by design” requirement, you will need to design compliant policies, procedures and systems at the outset of product development and keep them under review. One of the key aspects of the proposed “privacy by default” principle is that, by default, only personal data that are necessary for a specific purpose are to be processed. This principle is likely to have a significant impact on some businesses’ processing operations if the implications are that cookies that process personal data will need to be switched off by default.

Accountability principles = more paperwork?

The draft proposal 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.

You may need to appoint a Data Protection Officer

Under the EU Commission’s proposal, a data controller or processor must designate a data protection officer (DPO) for a minimum initial period of 2 years in certain specified circumstances, if it regularly and systematically monitors individuals. Any business that carries out profiling activities is likely to be regarded as engaging in processing operations which satisfy this description.

Data transfer restrictions are here to stay

You will still have to jump through hoops in order to legitimately transfer data outside of Europe. It may well transpire that “Binding Corporate Rules (BCRs) gain even more compliance prominence. The Commission’s proposal expressly acknowledges the validity of BCRs, including BCRs for Processors, as a valid legal solution to EU’s strict data export rules. To date, BCRs have had only regulatory recognition, and then not consistently across all Member States, casting a slight shadow over their longer term future. Express legislative recognition ensures the future of BCRs – they’re here to stay.

Enforcement to have more teeth and non-compliance greater consequences

There are likely to be serious financial repercussions for non-compliance – now is a good time to get data protection priorities right! The Commission’s proposal includes very harsh fines for breaches of data protection law – as high as 2% of the global revenue of a commercial enterprise. Where you are established as a data controller in more than one Member State, it is the data protection authority of your country of main establishment that will be competent to decide – this is known as the “one stop shop” principle.
Your contacts

London

Hazel Grant
Partner
  t: +44 (0)20 7861 4217
  e: Hazel.Grant@fieldfisher.com

Antonis Patrikios
Partner
  t: +44 (0)207 861 4354
  e: Antonis.Patrikios@fieldfisher.com

Leonie Power
Senior Associate
  t: +44 (0)207 861 4907
  e: Leonie.Power@fieldfisher.com

Silicon Valley

Mark Webber
Partner
  t: +1 (650) 513 2684
  e: Mark.Webber@fieldfisher.com

Phil Lee
Partner
  t: +1 (650) 513 2687
  e: Phil.Lee@fieldfisher.com