#dcsukarticle http://www.dcsuk.info/n/vjmy

The proposed European Union Data Protection Regulation:

Status and highlights by Matthew Byford, Associate, Squire Sanders (U.K.) LLP

On 12 March 2014, the European Parliament adopted a draft Data Protection Regulation[1] to replace the 1995 Directive. The focus of the Draft Regulation is data privacy, specifically the protection of individuals with regard to the processing of their personal data. The draft must now be considered by the EU Council of Ministers, where there is considerable resistance from several Member States.

IN CONTRAST TO THE EXISTING DIRECTIVE, which sets a minimum bar but allows Member States considerable implementation flexibility at national level, the Regulation would be directly enforceable in each Member State. One benefit would therefore be a harmonised approach to data protection regulation across Europe. If adopted in its current form, however, there are concerns that the Regulation would result in a consistently business-unfriendly regime across Europe. Highlights are provided in the Q&A that follows.

Privacy by Design/ Default

What does the Draft Regulation say?

The Draft Regulation requires both data controllers and data processors to "implement appropriate and proportionate technical and organisational measures and procedures" to protect the rights of the data subjects, having regard to the "entire lifecycle management of personal data from collection to processing to deletion". Privacy by default means that privacy settings must be set at a level which ensures that personal data will only be processed for the purpose specified, whilst allowing for data subjects to "opt in" to more extensive processing.

What are the implications for business?

Businesses will be required to develop privacy by design/default tools and procedures that take into account relevant regulatory requirements and evolving industry standards. For the processing of data considered to be "high risk", businesses should consider embedding default settings, checklists, stop points, sign-offs, certifications, etc.

More generally, businesses should identify areas where data minimisation and purpose limitation strategies can be implemented. Default settings should be set at a level that ensures the lowest level of data processing and the highest level of data protection, but allows for consumers to actively consent to increased levels of data processing.

Right to Erasure

What does the Draft Regulation say?
Originally branded as "the right to be forgotten", the "right to erasure" will apply where there is no longer any need to retain the data for the purpose for which it was collected, or where the data subject objects to the processing. The general rule is that a data controller must, without delay: (1) erase all personal data relating to the data subject and prevent further dissemination; and (2) arrange for its Internet or cloud hosting providers to erase "any links to, or copy or replication of that data".

What are the implications for business?
The scope of the "right to erasure" is still unclear and could be interpreted to require the deletion of personal data held on all forms of storage media including back-up devices, business records and archives. The cost would be significant. The Draft Regulation does, however, provide that where "the particular type of storage technology does not allow for erasure and has been installed prior to entry into force of [the] Regulation", further processing of the data should instead be restricted.

Data Portability

What does the Draft Regulation say?
The right to data portability will be merged with the right of data subjects to access and obtain their personal data. Electronically processed data must be provided to data subjects on request "in an electronic and interoperable format" in order to facilitate the transfer of data between service providers. Further, where technically feasible, the data should be transferred directly from controller to controller at the request of the data subject.

What are the implications for business?
The right to data portability will be of concern to businesses that add significant commercial value to an individual's personal data. The new rules are likely to require businesses to (1) create the technical means to facilitate the transfer; and (2) hand over valuable data files of their customers to competing service providers if requested by the data subject.

International Data Transfers

What does the Draft Regulation say and what are the implications for business?
The Draft Regulation takes a cautious approach to international data transfers in light of the Snowden revelations and concerns over the efficacy of the existing US-EU Safe Harbor framework. The Draft provides that companies must seek authorisation from local EU data protection authorities ("DPAs") prior to any disclosure of EU personal data to a non-EU government or court; and (2) inform the relevant data subject of the proposed transfer. These obligations may be directly contrary to national security and law enforcement requirements in foreign countries where EU data is stored (e.g., those applicable to U.S. cloud providers).

As a demonstration of its concern over transfers to the US, the EU Parliament has recently voted to suspend the US-EU Safe Harbor framework (a popular vehicle used to legitimise transfers of data from the EU to the US). The European Commission ("Commission"), meanwhile, has recommended various improvements to the Safe Harbor framework. This raises pertinent issues about the impact on long-term cloud and other outsourcing agreements involving international transfers from the EU.

European Data Protection Seal ("EDPS")
The Draft Regulation would introduce a new certification programme allowing data controllers/processors to have their activities audited and certified by DPAs or accredited third parties. Cloud providers are considered to be prime candidates for the EDPS programme. EU customers would be able to rely on the EDPS as the basis for ensuring their vendors' compliance with EU law.

Sanctions

What does the Draft Regulation say?
The Draft Regulation establishes an Eye-popping maximum penalty of up to €100 million or 5% of turnover (whichever is higher) for a serious breach of the Regulation. There is also a private right of action for individuals who have suffered damage, including non-pecuniary damage, as a result of violations of the Regulation.

What are the implications for business?
This very high level of fines signifies the importance placed by the EU Parliament on the right to data protection. Given the territorial scope of the Draft Regulation, the possibility of the imposition of fines on businesses operating outside the EU should also not be ignored – the Draft Regulation purports to catch all businesses even if they have no physical presence in the EU, so long as they process personal data in connection with the provision of services to, or the monitoring of individuals in, the EU.

Next Steps

The EU Parliament's vote of overwhelming support for the Draft Regulation precedes European elections that could have a significant impact on the make-up of the EU Parliament and the Commission. With strong concerns being raised by several EU Member States, it is difficult to predict whether the Draft Regulation will ultimately be enacted in its current form or when it will pass into law. It is in any event expected that a two-year grace period will apply.

Affected organisations should not be complacent, however, because many of the obligations set out in Draft Regulation will require significant adjustments and could take considerable time to implement.

1. The adopted text of the Draft Regulation is available at the following link which shows the original text proposed by the European Commission in January 2012 (the left column) compared to the text that has recently been adopted by the EU Parliament (the right column): http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201