MAYER·BROWN

Complete Reform of European Data Protection Law:
How Will This Impact Your Business?

April 19, 2012

Mark Prinsley, Partner
Oliver Yaros, Senior Associate
Isabel Simon, Associate

Privacy & Data Security
Webinar Series on Privacy, Security and Data Protection

Speakers

Mark Prinsley is a partner and head of the Intellectual Property & IT group in London as well as the outsourcing practice. He concentrates on non contentious intellectual property including, in particular, IT project, outsourcing and privacy and data security work. Mark is frequently involved in counseling on privacy issues particularly relating to trans-border data flows in the context of major outsourcing and IT projects.

Oliver Yaros is a senior associate in Mayer Brown's London office. He advises on many data protection and privacy law compliance issues for banking, insurance, pension fund and other clients operating in the financial sector including on the export of personal data from the EEA, appropriate measures necessary to protect personal data inside and once transferred outside of the EEA, conflicts between data protection compliance requirements and foreign law, liability from loss of data due to theft abroad and notification or registration procedures. He also works on large IT and business process outsourcing projects and IT systems procurement transactions

Isabel Simon is an associate in the Litigation & Dispute Resolution (Antitrust / Competition) practice in the Brussels' office. Her practice focuses on antitrust and competition matters. From 2008 until 2010 Isabel did her legal clerkship in Düsseldorf. Between 2005 and 2008 she was an academic assistant at the Institute for Information, Telecommunications and Media Law at the Westfälische Wilhelms-Universität Münster. Isabel is a guest lecturer at the Westfälische Wilhelms-Universität Münster for International Data Protection Law.

Agenda

- The reforms: The rationale for change and an overview of the proposals
- The potential impact: key issues for business and steps organisations will need to take in order to comply
- Next steps: The process for approving and implementing the new law, expected time frames and the potential opportunities for changes to the proposed legislation
- Questions?

The reforms: Rationale for change

- Existing European Data Protection Directive adopted in 1995
- Covers personal data processed by data controllers established in the EU. Does not cover data controllers established outside the EU or data processors
- Enacted unevenly throughout the EU, compliance required with different sets of procedures in each member state
- Has led to spiralling bureaucracy, costing businesses around €2.3b a year
- Scale of data collection and sharing has increased dramatically but does not adequately address increasing concerns over loss of data / security breaches, length of time data can be held and issue of consent

The reforms: The key proposals

- Reform by regulation: One set of rules throughout the EU, concept of "main establishment"
- Will apply to both data controllers established inside the EU and those outside the EU
- Data processors to also be directly responsible for compliance in certain circumstances
- At least a minimum standard of contractual obligations from data processors must be obtained
- Requirement to report security breaches to authorities and data subjects
- Greater emphasis on internal controls: No notifications but requirements for record keeping, internal impact assessments, policy making and the appointment of a data protection officer responsible for monitoring and ensuring compliance

The reforms: The key proposals

- Strengthening of the data subjects' position including:
  - Wider definition of identifying data
  - Right to seek redress in data subject's home state
  - Data portability right
  - Right to be forgotten
  - Any processing carried out on basis of data subject's consent will not be valid unless explicit consent has been obtained
  - Special rules on collecting / processing personal data about children
  - Prohibition on processing any sensitive personal data about data subjects unless certain conditions met
- Revised rules on transferring personal data to recipients based outside of the EEA
- Greater enforcement: Fines of up to 2% global annual turnover

The impact: Key issues for Businesses

- The Expanded definition of Personal Data:
  - Genetic Data to be "Sensitive Personal Data"
  - No changes to status of "financial data" about an individual
- Geographical impact:
  - Businesses outside the EU which process personal data about EU residents /offer goods and services to EU residents/monitor the behaviour of EU residents will be caught by the legislation

Proposed geographical impact of the Regulation

Geographic scope	Covered by existing legislation
Processing of personal data in the context of the activities of an establishment of a controller or processor in the Union.	Yes.
Processing of personal data of data subjects residing in the Union by a controller not established in the Union where the processing activities are related to: (a) the offering of goods and services to such data subjects in the Union or; (b) monitoring of their behaviour.	No – although note that there is potential liability based on location of equipment used for the processing.
Processing of personal data by a controller not established in the Union, but in a place where the national law of a member state applies by virtue of public international law.	No.

Key issues for Businesses
Data Processor liability

Current Position	Proposed Position
No direct liability to individuals or administrative authorities - liability dealt with in contractual arrangements between the controller and processor	- liable as a controller for processing outside scope of instructions from contracting party
	- individuals to have rights against controllers and processors for damage suffered as a result of unlawful processing
	- potential exposure to administrative fines

The impact: How will we need to comply?

- Increased Administrative Burdens
  - Data Impact Assessments where a company's processing operations presents specific risks to the rights of data subjects, will be necessary to complete an internal impact assessment before carrying it out and to seek their supervisory authority's authorisation where required by that authority
- Data breach notifications
  - Rigid timetable for notification of data subjects and supervisory authority
- Data exports

The impact: How will we need to comply?

- All businesses with over 250 employees:
  - Will be necessary to conduct an internal audit of how personal data is processed in your organisation. Will be necessary to produce a record of what / how personal data is being processed and for which purposes, including transfers outside of the EEA. Will be necessary to establish internal policies to ensure data protection compliance and to keep both up to date
- All businesses with over 250 employees / engaging in regular and systematic monitoring:
  - Will be necessary to appoint a data protection officer to be responsible (acting independently) for monitoring and ensuring compliance, informing / advising their organisation and subcontractors of their responsibilities and for being the contact person for supervisory authorities and data subjects. Must be appointed on terms of at least 2 years and may only be dismissed during term of office if no longer fulfils the conditions required for performance of their duties

Next steps: Legislative Process

- Ordinary legislative procedure involving European Parliament and European Council
  - Max. three readings in both European Parliament and European Council
  - Current status: First reading
  - Most legislative proposals are adopted in the first reading
- Timetable
  - First reading: No time limit (usually 13-15 months)
  - Second reading: Max. 6-8 months
  - Third reading: Max. 6 months
- Possible implementation date: Mid 2013

Next steps: Legislative Process

- Key Actors
  - European Commission: Directorate-General for Justice, Fundamental Rights and Citizenship (Commissioner Viviane Reding)
  - European Parliament: Responsible Parliamentary Committee LIBE (Civil Liberties, Justice and Home Affairs)
  - European Council: JHA (Justice and Home Affairs) Council configuration
- Reactions to the European Commission‘s legislative proposal
  - Harmonization is widely welcomed
  - Aspects under discussion are *inter alia* the proposed rules on the imposition of fines, on the data breach notification and on the right to be forgotten
- Next step: Report of the Responsible Parliamentary Committee and subsequently adoption of a European Parliament position

Questions?

Mark Prinsley
Partner, London
+44 20 3130 3900
mprinsley@mayerbrown.com

Oliver Yaros
Senior Associate, London
+44 20 3130 3698
oliveryaros@mayerbrown.com

Isabel Simon
Associate, Brussels
+32 2 551 5966
isimon@mayerbrown.com

MAYER·BROWN

Privacy & Data Security

Webinar Series on Privacy, Security and Data Protection