MAYER·BROWN

# The new European General Data Protection Regulation

## What you need to know

Charles-Albert Helleputte, Partner, Brussels
Mark Prinsley, Partner, London
Guido Zeppenfeld, Partner, Düsseldorf and Frankfurt
Oliver Yaros, Senior Associate, London

20 January 2016

# Speakers

**Mark Prinsley** is head of the Intellectual Property & IT group at Mayer Brown International LLP in London as well as the outsourcing practice. His practice involves acting for customers at all stages of outsourcing transactions. Recent outsourcing projects have included acting for a commodity exchange in the outsourcing of its IT functions; a telecommunications company in IT outsourcing; a global bank in the outsourcing of its human resources functions; a global chemicals company in outsourcing its finance and accounting functions; a global automotive company in the outsourcing of human resources functions; and a consumer goods company in Finance and Accounting outsourcing and the implementation of cloud computing arrangements and on privacy related matters. Mark also works on the technology transactions which generally include real-time licensing of financial markets data.

**Charles-Albert Helleputte** is a partner in the Brussels office of Mayer Brown. In the data protection area, he focuses his practice on the EU policy and Belgian aspects, primarily in the hotels & leisure industry as well as in financial services. At EU level, Charles is a member of the DEC Committee at AmCham EU, closely monitoring and advocating for EU data protection developments. Recent credentials include representing a client in hearing before the WP29 and assistance in the drafting of position papers to increase authorities' awareness on data protection issues in the travel industry.

# Speakers

**Dr. Guido Zeppenfeld** is a partner in the Frankfurt and Düsseldorf offices of Mayer Brown and the Managing partner in Germany. He heads the firm's German Employment & Benefits practice and is responsible for the firm's German Business Technology Sourcing practice. He is also one of the leaders of the firmwide Employment & Benefits Group.

Guido advises and represents national and international client organizations in connection with all legal matters regarding the management of human capital, including employment law, restructuring and reorganization measures, executive compensation, employee incentives, benefits and company pension schemes as well as employee data privacy. Further core areas of Guido's professional experience are compliance reviews and the implementation of compliance measures as well as advising in connection with national and international transactions, in particular (out) sourcing deals, privatizations and M&A transactions. He is the author of various articles on legal aspects of human resources, such as employment, outsourcing, pensions and executive compensation.

**Oliver Yaros** is a senior associate in the Intellectual Property & IT Group of the London office of Mayer Brown International LLP and advises clients on TMT, outsourcing, IT, data protection, privacy, e-commerce and IP issues. Oliver acts on global financial industry utility projects, IT and business process outsourcing projects and IT systems procurement transactions as well as advising a range of clients (financial institutions, manufacturers and retailers of consumer products, publishers and providers of digital media and online content) on many e-commerce and data protection issues. From May 2013 to October 2014, Oliver spent 18 months on secondment to the GBM Legal team of HSBC in London during which he advised the Global Banking and Markets (investment bank) division and worked with other divisions of HSBC on the creation of various global know your client / client onboarding and other types of banking industry utility joint ventures with other banks, on a number of multilateral and bilateral outsourcing projects, on investment banking IT system procurement projects and on various worldwide IP portfolio management and data protection issues.

# Introduction: Topics we will cover today on the GDPR

- Timetable for implementation
- Territorial impact and scope of the new GDPR
- Sanctions and fines
- Data breach notification
- Compliance requirements: Privacy impact assessments, data protection officers and obligations on data processors
- Enhanced rights of data subjects, right to be forgotten, data portability
- International data transfers
- Questions

# Timetable for implementation of the Regulation

- Proposals for wholesale updating of Data Privacy Directive of 1995 published in January 2012
- "Trilogue" between EU Commission, EU Council and EU Parliament and text of Regulation substantially agreed December 2015
- Political agreement/formal adoption early 2016
- Implementation 2 years following publication of the Regulation in the Official Journal

"Citizens and businesses will benefit from clear rules that are fit for the digital age, that give strong protections and at the same time create opportunities and encourage innovations in a European Digital Single Market"

- Vera Jourova

# Scope and territorial impact

- One continent – one law
  - Regulation as legislative instrument of EU
  - Territorial scope
  - Harmonization jeopardized by exemptions and references to Member States' law
    - National security activities and law enforcement
    - Employee personal data, etc
- Who is covered?
  - GDPR to apply whenever personal data about EU residents is processed in connection with (i) offer of goods and services or (ii) monitoring of behavior with EU
    - EU based organisations
    - Organisations outside EU
    - Data controllers
    - Data processors

# Scope and territorial impact

- What is covered?
  - Personal Data
  - Sensitive Data
  - Pseudonymous Data
- One-stop-Shop
  - Lead supervisory authority where organization has its single or “main” establishment
    - Identification of “main” establishment will be key
    - Problem: leeway under GDPR for “other” DPAs to declare themselves competent
  - Co-operation between national DPAs
  - European Data Protection Board

# Sanctions & Disclosure

- Sanctions
  - Various sets of corrective powers (Art. 53.1b) and sanctions (Art. 79) attributed to DPAs:
    - Warning to controller or processor
    - Order controller or processor to bring processing into compliance or controller to communicate data breaches to data subjects
    - Suspend data flows to a recipient in third country / international organization
    - Impose administrative fines **in addition to, or instead of** measures referred above
  - Role for the EDPB in drawing up guidelines (Art. 66.1.(ba))
  - Member State's discretion in setting penalties (Art. 79.b)

# Sanctions & Disclosure

- Sanctions
  - Effective, proportionate and dissuasive and take into account the nature, gravity and duration of infringement, the intentional or negligent character, repetition of infringements, adherence to a code of conduct or approved certification mechanisms, etc
  - Range of administrative fines:
    - Up to the higher of 20 mio and 4% of the total worldwide turnover of the preceding financial year in 6 cases:
      - Basic principles for processing
      - Data subject's rights
      - Data transfers
      - Certain sensitive processing (Chapter IX)
      - Non compliance with DPA (i) limitation and suspension or (ii) order

# Sanctions & Disclosure

- Sanctions
  - Range of administrative fines:
    - In other cases, up to the higher of 10 mio EUR or 2% of the total worldwide turnover of the preceding financial year in most instance

# Sanctions & Disclosure: Data breach notification

- Disclosure
  - In case of a personal data breach, requirement for the data controller to notify the competent DPA without undue delay and, where feasible, not later that 72 hours after having become aware of it (with carve out)
  - No deadline for data processor to notify data controller but a requirement to do so without undue delay
  - Specific requirements on information to be provided and documentary evidence to be compiled in order for the DPA to assess the response
  - Personal data breach = breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed

# Sanctions & Disclosure: Data breach notification

- Disclosure
  - Communication to the data subjects by the data controller (only) is required only if “the personal data breach is likely to result in a high risk the rights and freedoms of individuals”
  - No communication required in cases in which (art. 32.3):
    - He has taken the appropriate technical and organizational measures
    - There is no likely high risk due to the measures taken by the data controller
    - It would involve a disproportionate effort (although in such case, public communication or similar measure shall be pursued)

# Compliance requirements

- **Data privacy impact assessments: A focus on compliance and risk management**

- Controllers and processors will be subject to increased record keeping duties. Controllers and processors must maintain a record of processing activities under its responsibility

- Where a type of processing is likely to be "high risk" in relation to the rights and freedoms of the individuals concerned, the controller must conduct an assessment of the impact of the envisaged processing

- A data protection impact assessment must be carried out in respect of:

  - Systematic, extensive evaluation of personal aspects of persons based on automated processing – i.e. profiling;
  - The processing of sensitive personal data, criminal convictions and offences; or
  - Systematic monitoring of publicly accessible areas on a large scale

- These assessments must include at least:

  - A systematic description of the processing operations and the purposes of the processing;
  - An assessment of the necessity and proportionality of the processing operations;
  - An assessment of the risks to the rights and freedoms of the individuals concerned; and
  - The measures to address the risks, including safeguards, security measures, mechanisms to protect the personal data and demonstrate compliance with the GDPR taking into account the rights of the individuals concerned

- Where a DPIA indicates processing is high risk in absence of any measures to be taken, the controller must consult with the data protection authority

# Compliance requirements

- **Requirement to appoint a data protection officer (DPO)**

- Controllers and processors that carry out the following types of processing must appoint a data protection officer:

  - Those that conduct processing of sensitive personal data on a large scale;
  - Those that conduct processing that entails regular and systematic monitoring of individuals on a large scale; or
  - Those that process personal data as a public authority or body

- A DPO must:

  - Cooperate with and be the contact point with the data protection authority and have his or her contact details published so that individuals can contact him or her to exercise their rights under the GDPR;
  - Have expert knowledge of data protection law and practices;
  - Must report directly to the highest management level of the organisation;
  - Must act independently, must not receive any instructions regarding the exercise of his or her tasks, shall not be dismissed or penalised for performing them;
  - Inform the organisation of its responsibilities under the GDPR and monitor compliance, including assigning responsibilities, raising awareness, organising training and conducting audits; and
  - Advise on and monitor the carrying out of any data protection impact assessments

# Compliance requirements

- **Requirements with respect to data processors**
  - Processors' liabilities will no longer be regulated solely by the contract with the controller. Data processors will have direct obligations and liabilities under the GDPR and data protection authorities may take action against a data processor for breaching its obligations or acting outside or contrary to the instructions of the data controller
  - Processors will be held accountable for ensuring their own level of appropriate security and must document their processing of personal data
  - Processors must obtain the prior consent of the controller to engage sub-processors
  - Controllers must only use processors that provide sufficient guarantees on implementing appropriate technical and organisational measures to protect personal data. Controllers must ensure that processors agree to certain contractual requirements set out in the GDPR concerning confidentiality of personal data, international transfers of personal data, audits, return of personal data and other requirements
  - Controllers and processors may be jointly responsible to the authorities for certain aspects of data protection compliance
  - These changes will affect contractual relationships at every stage of a supply chain and will alter the negotiating positions of suppliers and customers alike

# Enhanced rights of data subjects

- Consent
  - must be “unambiguous”
    - no implied consent
- Disclosure of information by Data Controllers
  - likely emergence of “laundry instructions” icons disclosing processing activities
  - time limit for disclosure to the data subject of details of personal data obtained from another data controller
- Data Portability
  - right to require data to be transferred to a new data controller
  - where processing is based on consent and where it is by automated means
- Right to be forgotten/Erasure right
  - new obligation to inform other Controllers of an erasure request from a data subject taking account of cost and available technology

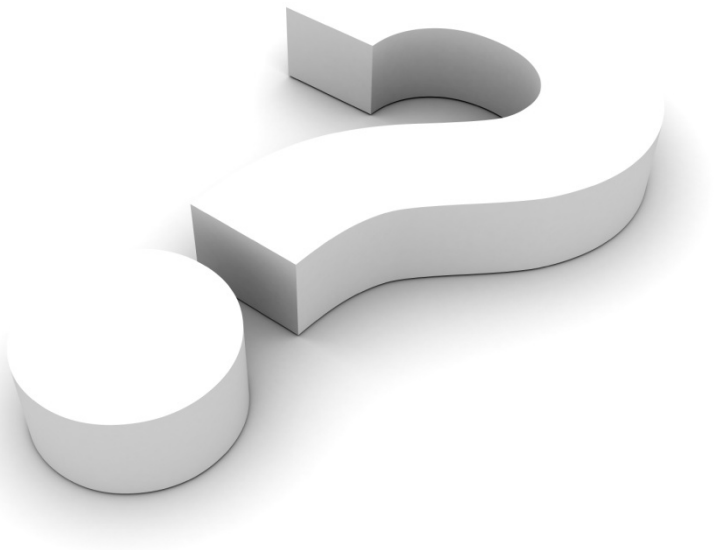
# Enhanced rights of data subjects

- Updated controls on Automated Decision making technologies
  - Public sector/security services balancing test
  - Direct marketing
    - Right to object
  - Automated individual decision making
  - Right to object subject to exclusions
- Privacy seals
  - Quality assurance schemes to be supported. More potential traps for data controllers?

# Data Transfers

- Current legal instruments to ensure legality of transferring data outside the EU are generally maintained under GDPR
  - Adequacy decisions of EU Commission
  - Standard contract clauses
  - Binding corporate rules
  - Explicit recognition of privacy seals, certifications and code of conduct
  - Consent
- But: GDPR does not address the current issues in connection with the invalidation of safe harbor
  - What is to be expected here?

# Questions




**Charles-Albert Helleputte**
Partner - Brussels
+32 2 551 5982
chelleputte@mayerbrown.com

**Guido Zeppenfeld**
Partner - Düsseldorf and Frankfurt
+49 69 7941 1701
gzeppenfeld@mayerbrown.com

**Mark Prinsley**
Partner - London
+44 203 130 3900
mprinsley@mayerbrown.com

**Oliver Yaros**
Senior Associate - London
+44 203 130 3698
oyaros@mayerbrown.com