MAYER·BROWN

Preparing Your Vendor Agreements for the General Data Protection Regulation

Oliver Yaros
Partner - London
+44 (0)203 130 3698
oyaros@mayerbrown.com

Lei Shen
Senior Associate - Chicago
+1 312 701 8852
lshen@mayerbrown.com

December 6, 2017

Speakers

Oliver Yaros is a partner in the Intellectual Property & IT Group, Cybersecurity & Data Privacy and Technology Transactions practices of the London office of Mayer Brown, and advises clients on data privacy, technology transactions, outsourcing, IT, e-commerce and IP issues. On data privacy matters, Oliver advises clients on how to conduct global privacy compliance projects, how to prepare for and respond to data breach events and data protection reform such as the GDPR and Privacy Shield, conflicts in laws that prevent international transfers, Brexit, and using data in the context of fintech, digital and "Big Data" analytics initiatives as well as in connection with IT outsourcings. Oliver also acts on global financial industry utility projects for banks relating to KYC, fintech and digital initiatives. Oliver is a Certified Information Privacy Professional in Europe (CIPP/E) with the International Association of Privacy Professionals (IAPP).

Lei Shen is a senior associate in the Cybersecurity & Data Privacy and Technology Transactions practices in Mayer Brown's Chicago office. Lei focuses her practice on data privacy and security, including compliance with U.S. and international privacy laws, and on technology transactions. Lei has passed the Certified Information Privacy Professional/United States (CIPP/US) certification exam offered by the International Association of Privacy Professionals (IAPP).

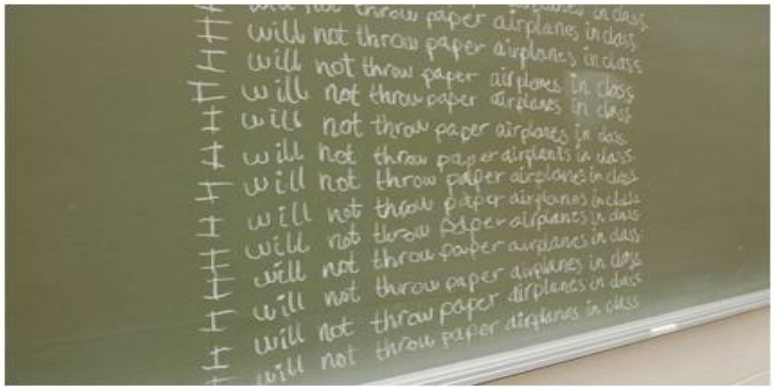
Topics We Will Cover Today

- What are the basics of data protection?
- What are the new requirements under the GDPR?
- Overview of recent guidance provided by the Article 29 Working Party and DPAs
- What should businesses expect and how should businesses prepare as they approach the implementation of the GDPR?
- How should organisations be reviewing and updating their vendor agreements to ensure compliance with the GDPR?
- Questions

DATA PROTECTION BASICS:
Overview of EU Directive

Data Protection Basics

- **Current Law:**
  - Currently governed by the European Data Protection Directive 1995, as implemented in EU Member States
- **Terms to Know:**
  - Personal data
  - Processing
  - Data controller
  - Data processor
  - Data subject
- **Enforcement:**
  - Regulated by national data protection authorities
  - Sanctions for non-compliance include criminal proceedings and civil fines



MAYER · BROWN

OVERVIEW OF GDPR:
Key Changes and Compliance Requirements

GDPR: The Key Changes

- **A Regulation, not a Directive:** The GDPR will be directly applicable in the same form in all EU Member States with the intention of reducing the burden on international organisations
- **Changes to territorial scope:** In addition to businesses that are established in the EU, non-EU businesses that process personal data in relation to the offering of goods or services to individuals within the EU, or as a result of monitoring individuals within the EU, will now have to comply
- **Significantly higher fines:** The maximum fine will be substantially increased to 4% of an enterprise's worldwide turnover or €20 million per infringement, whichever is higher
- **New data loss notification obligation:** The relevant European DPA must be notified without undue delay and where feasible within 72 hours. The individuals affected may also have to be notified

GDPR: The Key Changes (cont.)

- **New data privacy governance requirements:** A data protection officer may have to be appointed to be responsible for an organisation's compliance. Organisations will also be required to map their processing activities and undertake data protection impact assessments for higher risk processing
- **A requirement to implement "privacy by design":** Businesses must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken
- **Strengthening of individuals' rights to personal data:** Individuals will have the "right to be forgotten", the "right to data portability" and the right not to be subjected to automated data profiling
- **Obligations on both data controllers and data processors:** Service providers will be held accountable for their own level of appropriate security, must document their processing to the same extent under the GDPR and must obtain prior consent to use sub-processors

Territorial Scope: Directive vs. GDPR

European Data Protection Directive 95/46 applies to	General Data Protection Regulation 2016/679 applies to
A data controller where it is established in an EU Member State and the data that is processed in the context of that establishment	The processing of personal data in the context of the activities of a data controller or data processor established in the European Union, irrespective of where the processing takes place
A data controller where it is not established in an EU Member State but is using equipment in an EU Member State for processing data otherwise than for the purposes of transit through that Member State	The processing of personal data of data subjects who are in the European Union by a data controller or data processor not established in the EU, where the processing activities are related to: • The offering of goods or services to those data subjects; or • The monitoring of their behaviour in the EU

GDPR Compliance Requirements:
Requirement to Appoint a Data Protection Officer (DPO)

- **Controllers and processors that carry out the following types of processing must appoint a DPO:**
  - 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

- **General industry good practice may require the appointment of DPOs by certain businesses**

- **Data Protection Officers 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; and
  - Inform the organisation of its responsibilities under the GDPR and monitor compliance, including assigning responsibilities, raising awareness, organising training and conducting audits

GDPR Compliance Requirements:
Data Mapping and Data Privacy Impact Assessments

- **Data Mapping and Data Privacy Impact Assessments: A focus on risk management and record keeping**
  - Controllers and processors will be subject to increased recordkeeping duties. Controllers and processors must create and maintain a record of processing activities for which they are responsible
  - 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

GDPR Compliance Requirements:
Grounds for Processing

- **"Consent":**
  - Consent must be an informed, unambiguous and freely given indication by a statement or clear affirmative action of the data subject's consent to processing for specified purposes, and it must be capable of being withdrawn at any time. Whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance will be taken into account when assessing if consent has been "freely given"
  - The data controller must be able to demonstrate that consent has been given
  - Where consent is given in a written document, the request for consent must be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language
- **"Legitimate interests":**
  - The processing must be necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
  - Requirement to notify the individuals concerned of the details of the legitimate interests being pursued

GDPR Compliance Requirements:
Notice Requirements

- **The notification must contain:**
  - The identity and the contact details of the data controller and, where applicable, of the data controller's representative and the data protection officer
  - In the case of personal data provided by a third party, the categories of personal data being processed
  - The purposes of the processing as well as the legal basis for the processing (consent, legitimate interests, etc). If "legitimate interests", these must be identified
  - The recipients or categories of recipients of the personal data, if any
  - Where the personal data is to be transferred outside of the EEA, that fact and the existence or absence of an adequacy decision by the Commission, or a reference to the appropriate or suitable safeguards being adopted and the means by which the data subject can obtain a copy of them

GDPR Compliance Requirements:
Notice Requirements (cont.)

- **The notification must contain:**
  - The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
  - A description of the data subject's rights under the GDPR and their right to complain to a DPA
  - Where consent is being relied upon, the right to withdraw it at any time
  - Whether the personal data is required to perform a contract / is required by law, whether the data subject is required to provide that personal data and the consequences if they do not (not required where personal data received from a third party)
  - The existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

GDPR Compliance Requirements:
Enhanced Rights of Data Subjects

- **Current Position (Under the Directive)**
  - Limited rights – subject access requests

- **Under the GDPR**
  - 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
  - Right to object to profiling / automated decision-making

Get Ready to Comply:
Ten Steps for Preparing for GDPR

1. **Inform your leadership, formulate a plan**
2. **Decide whether a data protection officer should be appointed and a data protection framework created**
3. **Map the personal data that your organisation is processing**
4. **Examine the results to determine which of your data processing activities and business units must comply with the GDPR**
5. **Address the risks identified in any data processing activities**
6. **Evaluate the grounds under which personal data is being processed**
7. **Update your data governance policies and procedures**
8. **Design and implement new compliance systems to comply with the GDPR**
9. **Review your supply chain contracts to ensure that your service providers will comply**
10. **Assess any international transfers of personal data being conducted by your business**

REVIEWING YOUR VENDOR CONTRACTS FOR THE GDPR

Key Changes for Processors under GDPR

	EU Directive (current requirements)	EU GDPR
Obligation to Comply	• Controller has the primary obligation to comply	• Processors will have direct obligations and liabilities under the GDPR: › Cooperating with supervisory authority › Implementing appropriate technical and organizational security measures › Maintaining records of processing activities › Notifying controller in the event of a data breach › Complying with cross-border data transfer requirements
Liability	• Controller liable for breaches by the data processor	• 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

Key Changes for Using Processors / Vendors

- Controllers should only select processors who provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures that will meet the requirements of the GDPR
  - Adherence to codes of conduct or approved certification mechanisms may be used as an element to demonstrate compliance
- Parties must ensure that an adequate transfer mechanism is in place if transferring data out of the EU
- Contracts with processors must meet the requirements of the GDPR, which contain certain provisions not required by the EU Data Protection Directive

Key Changes for Processor / Vendor Agreements

EU Directive (current requirements)	EU GDPR
• Two contractual requirements: › Only act on controller's instructions › Implement appropriate technical and organisational security measures	• Retains and strengthens Directive's contractual requirements: › Only act on controller's documented instructions › Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk • Also adds several new contractual requirements, including but not limited to: › Recordkeeping and audits › Subcontracting

Updating Your Vendor Agreements:
Required Provisions

- **Contract must set out:**
  - Subject matter and duration of processing
  - Nature and purpose of processing
  - Type of personal data and categories of data subjects
  - Obligations and rights of controller

- **Contract must include the following terms:**
  - Process only on documented instructions from controller
  - Duty of confidentiality
  - Implementation of appropriate technical and organisational security measures
  - Sub-processing restrictions

Updating Your Vendor Agreements:
Required Provisions (cont.)

- **Contract must include the following terms (cont.):**
  - Assistance to enable controller to comply with data subject requests (e.g., right to data portability, right to erasure, etc.)
  - Assistance to enable controller to comply with its obligations in Articles 32 to 36 (i.e., security, notification of data breaches, DPIAs, consultation)
  - Deletion or return of data at end of contract
  - Information to demonstrate compliance
  - Audits and inspections
  - Notification of infringing instructions

Updating Your Vendor Agreements:
Other Provisions to Consider

- Definitions
- Recordkeeping
  - Maintain record of categories of processing activities carried out on controller's behalf
- Comply with cross-border data transfer requirements
- DPO requirement
- Data protection by design
- If applicable, Privacy Shield onward transfer requirements
- Consider indemnities, limits of liability and other similar clauses to address new risks

Updating Your Vendor Agreements:
Recent Guidance from DPAs

- **Recent Guidance from DPAs**:
  - UK's ICO: guidance takes point of view of controller
  - France's CNIL: guidance takes point of view of processor
- Still a number of unanswered questions
  - For example, how far down the subprocessor chain must a processor flow down obligations?

Data Breach Notification

- **Data breach notification (for data controllers):**
  - Report to the competent Supervisory Authority "without undue delay and where feasible not later than 72 hours" unless the breach is *unlikely to result in a risk* to data subjects
    - Describe nature of breach (e.g., categories and number of data subjects, categories of personal data)
    - Name and contact information of the DPO or other contact point
    - Describe consequences of the breach
    - Describe mitigating measures taken or proposed
  - Report to data subjects without undue delay if breach is *likely to result in high risk* to data subjects
    - May be able to avoid notice to individuals if the controller satisfies the SA that, for example, data are unintelligible (through acceptable encryption) or risks have otherwise been mitigated

Data Breach Notification (cont.)

- **Data breach notification (for data processors):**
  - Report to data controller without undue delay after becoming aware of a breach
    - Very broad obligation
    - No risk analysis is given, unlike for data controllers' notification obligations
- **Recent guidance from Article 29 Working Party:**
  - Awareness of breach
    - Controller
    - Processor
  - Notification of availability breaches

Comparison of U.S. vs EU Data Breach Obligations

	U.S. State Data Breach Laws	EU GDPR
Scope	• Mostly limited to personal information that could put person at risk for identity theft	• Covers all personal data, subject to risk analysis
Definition of Breach	• Typically requires "unauthorized access or acquisition" of covered information	• "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"
Notification Timeframes	• Controller: fastest is 30 days • Processor: fastest is 24 hours	• Controller: 72 hours to supervisory authority; without undue delay to individuals • Processor: without undue delay

Comparison of U.S. vs EU Data Breach Obligations

	U.S. State Data Breach Laws	EU GDPR
Whom to Notify	• Notify affected individuals • Notify a variety of state and other agencies (e.g., law enforcement, state attorneys general, credit reporting agencies, etc.)	• Notify affected individuals • Notify supervisory authority
Liability and Fines	• Mostly class action lawsuits • Some government enforcement actions	• Fines for not notifying of a data breach can reach 2% of global turnover or €10 million, whichever is higher

Assess Your International Transfers

- Data transfer restrictions apply to controllers and processors
- Current legal instruments to ensure legality of transferring data outside the EU are generally maintained under GDPR
- Transfer to country with Adequate Protection (same as Directive) OR use of approved means:
  - EU Model Clauses (but with caution – Schrems challenge)
  - Binding Corporate Rules (BCRs) (intracompany only, available for controller group or processor group)
  - Privacy Shield – NOT Safe Harbor
  - Derogations (EU Directive derogations continue to apply)
    - Data Subject Consent
  - Approval from Data Protection Authority (DPA)
  - Data Protection Seals

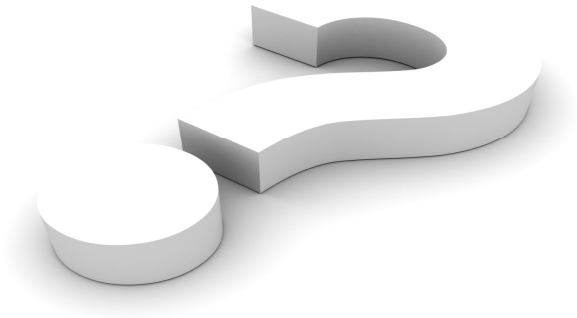
Assess Your International Transfers:
Privacy Shield

- Replacement mechanism to Safe Harbor that permits transfers of EU personal information to the US
- Must be subject to jurisdiction of FTC or DOT to self-certify
- Privacy Shield Principles: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability (plus 16 Supplemental Principles)
- The "Onward Transfer" principle addresses how Privacy Shield-certified companies must protect personal information that they transfer onto other data controllers or to third-party agents
  - Will need to modify agreements of third parties that receive such data
- Not easy – compliance often requires certain operational, policy and contractual changes

Amending Your Contracts:
Next Steps

- Create a project plan for the assessment and renegotiation of the relevant agreements
  - Assemble a team to manage and execute the project
- Identify contracts to be remediated and prioritize by underlying risk
- Determine how to execute the renegotiation of the relevant agreements. For example, consider:
  - Can the agreements be amended using a template GDPR amendment or must each agreement have bespoke amendments prepared?
  - What is the negotiating power with each vendor?
  - Do other revisions need to be made (e.g., non-GDPR-related privacy and security provisions)?
- Consider creating a playbook to assist in negotiations of amendment or agreement

Questions?



Oliver Yaros
Partner - London
+44 (0)203 130 3698
oyaros@mayerbrown.com

Lei Shen
Senior Associate - Chicago
+1 312 701 8852
lshen@mayerbrown.com

MAYER·BROWN

Reminders and Upcoming Webinars

- A recording and link to the materials from this program will be distributed by email to you in the next day or two.
- For those applying for CLE credit, please note that certificates of attendance will be distributed within 30 days of the program date.
- To submit topic ideas for future programs, please email us at TechTransactions@mayerbrown.com.

MAYER·BROWN