EU General Data Protection Regulation (GDPR) - Key Compliance Issues for US Companies

Steptoe
STEPTOE & JOHNSON LLP

- **Jurisdiction**
  GDPR applies directly to processing of personal data outside the EU:
  - to offer goods or services to individuals in the EU (and possibly to EU businesses); or
  - to monitor behavior of individuals in the EU.

  This is a major change from the Data Protection Directive (**Directive**), which applies only to EU-established companies and data processing within the EU. US companies with business in the EU should assess whether they are directly subject to GDPR (which affects applicability of other requirements below).

- **Privacy Policy / Customer Notices / Consent**
  GDPR provides new detail on what information must be provided to individuals when their data is processed, and how they may validly consent to such processing. This requires companies subject to GDPR to reassess current notice and consent processes for data processing such as:
  - collection of data, including via websites/apps (and associated use of cookies);
  - ongoing retention of data for an appropriate period; and
  - transfers of data to third parties.

- **Transfers to US (and other foreign jurisdictions)**
  Foreign transfer rules under the GDPR are largely the same as those under the Directive, but it is advisable to assess transfers of personal data from the EU to US (or elsewhere) as part of an overall GDPR compliance plan. Compliance approaches can include joining the Privacy Shield, adopting EU standard contract clauses, relying on customer consent and/or other approaches.

- **Interactions with Data Subjects and Data Protection Authorities**
  Companies subject to GDPR should expect (and prepare for) interactions with data subjects (i.e. individuals whose data they process) and data protection authorities (**DPAs**) in the EU countries where they do business. Data subject rights under GDPR include (in appropriate circumstances):
  - access to and deletion of data held about them (including “right to be forgotten”);
  - objection to automatic decision-making (i.e. without human intervention); and
  - data “portability”.

- **Data Processors**
  GDPR applies directly to “data processors”, who operate at the direction of a “data controller” that is responsible for processing personal data (unlike the Directive, which applies only to data controllers). Companies that currently operate as data processors may face increased obligations.

- **Data Protection Officer**
  GDPR requires some companies to appoint a data protection officer (**DPO**) – i.e. those that engage at large scale in (i) regular and systematic monitoring or (ii) processing of sensitive data or data on criminal convictions – and requires other companies to assess whether to appoint a DPO.

- **Data Breach Notification**
  GDPR requires data controllers to notify many breaches of personal data security to DPAs and (where there is a likelihood of harm) to data subjects.

- **Fines / Risk Management**
  There has been much attention to the substantially increased maximum fines under GDPR – for some violations, up to the greater of €20 million or 4% of global revenue. We believe that very large fines are unlikely for responsible companies; however, the magnitude of possible fines indicates increased attention to data protection risk management.

- **Privacy by Design**
  GDPR takes and overall approach of “data protection by design and by default”, requiring companies to assess the data protection requirements for their business – and significantly increasing compliance risks for those that fail to do so.

- **Other Issues**
  The business model and data processing approach of each company are likely to raise specific issues in addition to those above.