GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR introduces far reaching obligations for companies that collect, use or otherwise process personal information.

MORRISON FOERSTER

What is the GDPR?

- The GDPR is the EU's reform of its privacy framework.
- Currently, the EU's privacy framework consists of a bundle of national data privacy laws.
- The GDPR will introduce a single framework that is directly applicable in all EU Member States; however, a large number of national customizations remain possible.
- The GDPR contains the same six core data protection principles, but there are significant changes and additional requirements. For example, it will be more difficult to obtain valid consent.

To whom does the GDPR apply?

- Companies established **in the EU** that process personal information;
- Companies based **outside the EU** that:
  - **offer goods or services directly to individuals** in the EU (regardless of whether payment is required), or
  - **monitor behavior of individuals** in the EU, for instance through customer profiling.

Enforcement

- Data Protection Authorities (DPAs) will have the power to levy fines of increasing levels of severity, up to **EUR 20 million or 4% of a company's group global annual turnover** of the past financial year.
- DPAs have a wide range of other powers, such as on-site audit rights and imposing temporary or definite limitations including a ban on processing.
- Broad rights for individuals, including the ability to:
  - Lodge complaints with DPA in the Member State of his/her residency.
  - Engage in group litigation.
- Individuals can sue for compensation for both material and non-material damages (e.g. distress).

New compliance obligations

- Direct obligations for **processors** who process data on the instructions of a controller.
- The duty to appoint a **Data Protection Officer (DPO)** in certain cases.
- A general **accountability requirement**, requiring a company to be able to demonstrate compliance with the GDPR.
- The duty to carry out **Data Privacy Impact Assessments (DPIAs)** in cases of high-risk processing activities, and potentially to consult a data protection authority (DPA).
- The requirement to keep **records** of all data processings.
- Responding to broadened rights of individuals such as the **right to be forgotten** and the **right to data portability.**
- Complying with specific restrictions and limitations on **profiling.**
- The notification of **data security breaches** to individuals and DPAs within 72 hours.

Timeline to Prepare for GDPR

25 May 2016 → **2016** → **2016/2017** → **25 May 2018**

GDPR formally adopted. Companies not yet required to comply.

Establish GDPR readiness plan.

Execute GDPR readiness plan.

GDPR directly applicable to companies.

How Can We Help You?

- Getting ready for the GDPR will be different for every company and will be dependent on many factors.
- MoFo has extensive experience helping companies across industries, including B2B or B2C organizations, as well as service providers (i.e. data processors).
- We can help you with every phase of GDPR preparedness, such as performing a GDPR gap-analysis, formulating and/or implementing your compliance plan, or helping you with your overall privacy compliance program.
- We would be delighted to further discuss how we can assist with your organization's specific needs.

We're here to help. We're MoFo, in Europe.

CONTACTS

Lokke Moerel
Senior Of Counsel
Berlin
49 (30) 726221278
lmoerel@mofo.com

Alex van der Wolk
Partner
Brussels / London
32 (2) 3407369 / 44 (20) 79204074
avanderwolk@mofo.com

Miriam Wugmeister
Partner
New York
(212) 506-7213
mwugmeister@mofo.com

Hanno Timner
Partner
Berlin
49 (0) 3072622-1235
htimner@mofo.com

A PRACTICAL GUIDE TO YOUR OBLIGATIONS

Key elements of GDPR readiness programs

MORRISON FOERSTER

Privacy Compliance Program

AWARENESS

- Start by ensuring that decision makers and key people in your organization are aware of the GDPR and what this means for the company.
- Form a GDPR core team to develop and execute your readiness plan.

DUE DILIGENCE & GAP-ANALYSIS

- Assess which data processings are subject to the GDPR.
- Create system, database, and dataflow inventories in preparation for compliance obligations.
- Inventory global data transfers.
- Assess which data processing activities warrant appointment of DPO and require a DPIA to be carried out.
- Assess which authority will be your Lead-DPA.

NOTICES & AGREEMENTS

- Update your customer- and employee-facing privacy notices.
- Verify whether you can rely on consent and update your consent statements to comply with new consent requirements.
- Update agreements and templates with third-party service providers.
- Verify your data transfer agreements or other transfer mechanisms.

COMPLIANCE OBLIGATIONS

- Set up or revise your DPIA checklists and procedures.
- Address your record keeping obligations (including the legal basis for processing personal information).
- Review and update your data retention policy, including to account for data minimization.
- Implement privacy-by-design and privacy-by-default into your working principles.
- If applicable: appoint your DPO.

INTERNAL PROCEDURES

- Implement a procedure to address data security breaches, including the ability to make notifications where required.
- Update your internal processes to address and be able to respond to individuals' new rights.

TRAINING

- Provide general training and awareness on GDPR compliance throughout the organization.
- Educate and train specific key stakeholders, such as IT, HR, Marketing, Audit, Procurement, Risk & Compliance, and Privacy Officers.

Specific Areas of Attention

- ✓ The GDPR also applies when data are **pseudonymized** or when online identifiers are used, such as **cookies** and **IP-addresses.**
- ✓ When you monitor the **behaviour** of individuals for commercial purposes, engage in **profiling**, or (re-)use information for **analytics** purposes, specific restrictions and limitations apply.
- ✓ When you process personal information of **minors** (< 16 years), specific requirements apply.
- ✓ When you are a **supplier** that qualifies as a data processor, there will be new obligations that are directly applicable to you and you may have to renegotiate your customer agreements.
- ✓ When you hold data provided to you by individuals (such as personal information stored in the cloud or posted to social media), you should specifically prepare for this **information to be portable** in a machine-readable format at the end of the contract or when consent is withdrawn.