

GENERAL DATA PROTECTION REGULATION (GDPR)

MORRISON
FOERSTER

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

What is the GDPR?

- The GDPR is the EU's reform of its privacy framework.
- The GDPR introduced 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 is more difficult to obtain valid consent.

Enforcement

- Data Protection Authorities (DPAs) now 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)

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.

New compliance obligations

- Direct obligations also 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 you to be able to demonstrate your compliance with the GDPR
- The duty to carry out **Data Privacy Impact Assessments (DPIAs)** in case of high risk processing activities and potentially to consult your 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

How Can We Help You?

- 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.

CONTACTS



Annabel Gillham
Partner, London
(44) 207 9204147
agillham@mofo.com



Lokke Moerel
Senior Of Counsel, Berlin
44 (20) 79204054
lmoerel@mofo.com



Hanno Timmer
Partner, Berlin
49 (0) 3072622-1235
htimmer@mofo.com



Alex van der Wolk
Partner, Brussels
Berlin, 49 (0)3072622-1279
London, 44 (20) 79204074
avanderwolk@mofo.com



Alja Poler de Zwart
Partner, Brussels
(32) 23407360
apolerdezwart@mofo.com

A PRACTICAL GUIDE TO YOUR OBLIGATIONS

Key elements of GDPR readiness programs

Privacy Compliance Program

AWARENESS

- Start by making sure that decision makers and other key people in your organisation are aware that the GDPR is coming and what this means for the company.
- Form your GDPR readiness core team to start developing and executing your readiness plan

DUE DILIGENCE & GAP-ANALYSIS

- Assess which data processings by establishments inside and outside the EU are subject to the GDPR
- Create inventory of systems, databases and dataflows in preparation of compliance obligations
- Inventorise 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 still 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 organisation
- 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 **pseudonymised** 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