KPMG

EU General Data Protection Regulation (GDPR)

Well positioned for the current challenges of European data protection

The GDPR represents a range of extensive revised requirements and modified time periods together with a significant increase in administrative fines for companies in all sectors. Until today the need for action is still pressing although the GDPR has already entered into force on 25 May 2018. KPMG can help companies implement the extensive requirements on time.

The challenge

The EU General Data Protection Regulation entails a completely revised data protection regime. It specifies the implementation of a data protection management system. Previous responsibilities, processes and measures have to be re-evaluated. Risk analysis, documentation and transparency are at the forefront. The record of processing activities represents the central element of documentation and control.

The GDPR includes the following new requirements in particular:

- A massive increase in administrative fines (up to EUR 20 million or up to four per cent of total worldwide annual turnover of the preceding financial year)
- Additional liability risks (accountability; reversing the burden of proof)
- New time periods and transparency requirements
- More stringent notification requirements in case of data breaches (72-hour time period)
- Requirement for a data protection impact assessment based on risk analysis
- 'Privacy by Design' and 'Privacy by Default'
- New requirements for records of processing activities
- Additional information and reporting obligations
- Extended rights for data subjects (especially the right to data portability and right to erasure)
- New requirements for consent
- New requirements for data processing on behalf

Furthermore, flexibility clauses grant national legislators the power to design regulations in specific areas. The German legislator has implemented parts of these flexibility clauses in the new German Federal Data Protection Act (BDSG).

Note: companies established outside the EU must also observe the GDPR if they process the data of persons residing in the EU for the purpose of offering goods/services or for monitoring their behaviour.

Based on the diversity of the processes and measures which still have to be implemented, increased expenditure is associated with the ability to meet compliance with the GDPR. Companies that process large volumes of data or highly sensitive data or that utilise new and complex technologies will need to undertake greater effort compared to other companies.

With respect to the GDPR requirements, companies should examine the following:

- ✓ Does the company have an extensive data protection concept in terms of a data protection management system?
- ✓ Does the company have a record of processing activities at its command?
- ✓ Has the company, beyond any doubt, clarified the circumstances in which a data protection impact assessment, including consultation with the supervisory authority, needs to be undertaken?
- ✓ Do processes and responsibilities exist to achieve compliance with information and transparency obligations and adherence to time periods?
- ✓ In case of a data breach, is the company able to react adequately and to meet the 72-hour deadline?
- ✓ Are the principles of 'Privacy by Design' and 'Privacy by Default' taken into account when implementing technical and organisational measures?
- ✓ Have adequate processes and measures been established to aid data portability?
- ✓ Does the company have an adequate erasure concept in place to deal with erasure requests, particularly in relation to processes to provide information on third parties to whom data has been disclosed?
- ✓ Do existing processes to obtain the consent of data subjects satisfy the more stringent requirements of the GDPR?
- ✓ How are international data transfers handled? What measures are used and do these comply with the new requirements?
- ✓ Do contracts with processors satisfy the requirements of the GDPR?
- ✓ Are national requirements issued on the basis of flexibility clauses taken into account?

Our service

With extensive experience stemming from numerous projects and broad knowledge, KPMG is at your disposal with regard to all questions centring on the topic of the General Data Protection Regulation and its implementation. Based on a gap analysis, we support you with the conception and the implementation of a data protection management system, focusing on its core data protection processes, risk assessments and the establishment of the record of processing activities. We are also at your disposal for the realisation of individual measures, such as the conception of a company-wide concept of erasure, the guarantee of the transparency requirements or the management of service providers in the course of commissioned data processing and third country transfer. Furthermore, we conduct performance tests of the data protection management system in accordance with recognised standards. Our experts are also there to support you in case of an emergency. In case of infringements against data protection and data security, we assist you with the investigation and clearance and make recommendations with regard to make recommendations with regard to the realignment of processes and systems.

Well equipped to meet your needs

KPMG's Compliance & Forensic division cooperates closely with IT and industry experts. It has extensive experience and a practical approach to data protection consulting and is very familiar with all regulatory requirements and standards.

Our specialists are at your service across Germany. Thanks to our involvement in the global KPMG network, we are also able to draw upon the expertise of further experts for competent support with international issues and matters. In this way, you benefit globally from our in-depth understanding of markets, sectors and companies. Please do not hesitate to contact us with your queries or to set up an initial meeting.

Contact

KPMG AG Wirtschaftsprüfungsgesellschaft

Barbara Scheben
Partner, Compliance & Forensic
T +49 69 9587-3737
bscheben@kpmg.com

Christopher Martens
Manager, Compliance & Forensic
T +49 69 9587-6444
christophermartens@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia