KPMG

Towards effective Data Protection

Mastering the rules of the General Data Protection Regulation (GDPR).

kpmg.ch/gdpr

The European Commission has adopted the General Data Protection Regulation (GDPR). This new legislation is the most impactful change in privacy and Data Protection regulation of the last decades. This regulation came about after more than four years of deliberations and negotiations and will impact organizations worldwide. The GDPR requires fundamental changes to how organizations approach Data Protection.

The regulation was formally adopted by the European Parliament and Council in May 2016. The new rules will become applicable two years thereafter. This means that from May 2018 onwards, your organization needs to be in full compliance with the new rules of the GDPR. Since certain provisions of the GDPR will require substantial changes in your organization: **The time to act is now!**

How does it impact organizations?

Until recently, Data Protection regulation in the EU received only limited attention. Fines for breach of regulations were limited and enforcement actions infrequent. With the GDPR, this will change. Three factors attribute to this.

Real reputational risk

Enforcement activities by Data Protection regulators will increase. Data Protection breaches will hence be brought to light sooner. The risk of reputational consequences will therefore become all the more real.

Large geographic reach

With the GDPR, the geographic reach of the legislation is increased to 'all organizations offering goods or services to EU residents' and 'organizations that monitor the (online) behavior of EU residents'. This means that your organization might now be in scope of the EU Data Protection regulation, where it was not the case before.

Huge fines

Failure to implement one or more Data Protection requirements adequately, will lead to very significant fines. The GDPR introduces fines that can amount to 20 million EUR or 4% of global annual turnover, whichever is higher. This is a big and serious change compared to the limited sanctioning possibility under the old regime. Hence, adequate implementation of Data Protection requirements within your organization is now more important than ever.

What are the fundamental changes

The GDPR introduces a number of new legislative requirements. A few of the most important ones are briefly described below:

Data Protection by Design and Default

- Under the old Data Protection regime, organizations were already required to have 'appropriate technical and organizational measures' to protect personal data. Under the GDPR, organizations must now demonstrate that measures are continuously reviewed and updated.
- Additionally, organizations must now demonstrate that the appropriate measures are included in the design of processing operations and that by default, personal data are only processed where necessary.

Data Protection Impact Assessment (DPIA)

- Under the GDPR, organizations should carry out a DPIA on the envisaged processing operations, where processing is likely to lead to high privacy risks.
- If the result of the DPIA shows a high inherent risk, the Data Protection supervisory authority needs to be consulted prior to processing.

Mandatory Data Protection Officer (DPO)

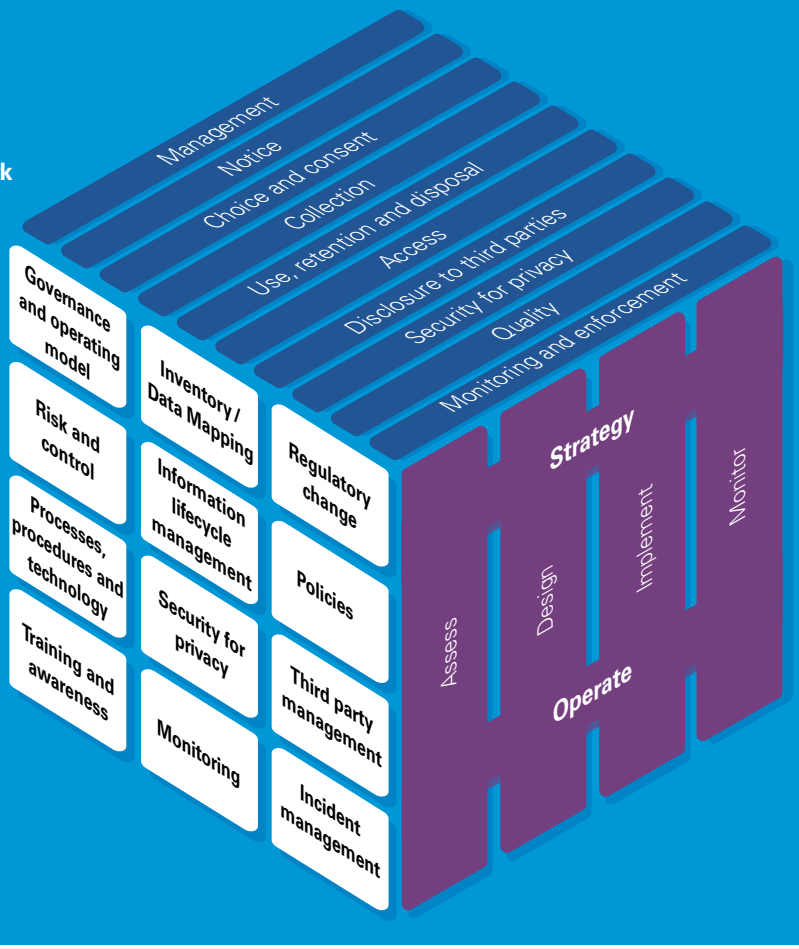
- Under the GDPR the appointment of a DPO is mandatory in a number of situations.
- The DPO must possess expert knowledge of Data Protection law and practices and should be sufficiently independent in the performance of its role.
- The DPO role may be carried out by a service organization.

Data Breach Notification obligation

- The GDPR introduces the obligation for data breach notifications for every organization.
- Organizations should notify the supervisory authority within 72 hours in case of a data breach requiring notification.
- Personal data breaches need not be reported if the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals.
- In case of a data breach with high privacy risks, the data subjects should also be informed.

In addition to the new requirements that are described above, many Data Protection requirements that existed under the old regime stay in effect in a similar or amended form (e.g. limitations on cross-border data transfer, requirements on consent, requirements related to access rights of data subjects, etc.). The GDPR demands from organizations to implement adequate and tailored Data Protection control frameworks and risk management. Mere policy updates for Data Protection compliance will not suffice. Data protection processes and controls need to be in place. The GDPR demands auditable Data Protection

KPMG Data Protection Governance Framework



governance implementation and maintenance. We help you in implementing the right measures and managing them adequately.

What to do now?

To determine how the GDPR affects your organization, **a first step is assessing the Data Protection readiness of your organization**. For this purpose we use our Data Protection governance framework.

KPMG's Data Protection governance framework is based on the following approach: (I) assess, (II) design, (III) implement and (IV) monitor. On the basis of known business and IT governance building blocks, the 12 framework components provide a pragmatic structure for dealing with Data Protection in your organization.

We can help you in each stage of your Data Protection improvement journey. Below we present only a few of our possible services:

	GDPR Services	Description
Assess	**GDPR quick scan**	Assessment which takes as the basis the additional key requirements of the GDPR compared to the EU Data Protection directive. The outcome of this assessment is the readiness status per new GDPR requirement, including related recommendations. This assessment is ideal if your organization has recently completed a Data Protection assessment based on the requirements of the EU Data Protection directive.
Design	**Data Protection maturity assessment**	Maturity assessment which gives an overall indication of the Data Protection maturity of your organization. The results are grouped on the 12 framework components. The outcome of this assessment serves as the perfect basis for setting up and tailoring your Data Protection governance framework in accordance with the GDPR and other international Data Protection requirements.
	Design GDPR governance strategy	The GDPR governance strategy contains the project plan and roadmap that shows for your organization which measures will be undertaken to improve Data Protection. In addition, it details how the activities will need to be performed and what the corresponding timelines are. A GDPR governance strategy is essential for structurally improving your organizations Data Protection in order to become.
Implement	**Implement GDPR governance measure**	It is recommended to follow a structured approach when implementing GDPR compliance measures. Benefit from industry best practices and proven project management methods.
Monitor	**Data protection certification / attestation**	Policy makers, business partners and customers increasingly demand that you demonstrate your commitment to Data Protection and privacy. Data protection certification is recommended if you trust that your organization has implemented adequate privacy governance already. Obtaining a privacy certificate will certify your accountability for privacy.

What are your benefits?

In working with KPMG, your benefits are as follows:

- A Data Protection assessment will show your (internal) stakeholders your organization's **readiness status including Data Protection gaps** and will present clear and **workable recommendations for improving** your overall Data Protection governance.
- Benefit from a proven approach to Data Protection management that is **pragmatic, flexible, scalable** and allows you to focus on the Data Protection challenges and opportunities of your organization.
- Acquire a view of industry Data Protection practices based on real-time **benchmarking**.
- Leverage Governance, Risk Management and Compliance (**GRC**) tooling for the delivery of assessments and for (continuous) monitoring.
- Achieve cost efficiency by **combining** this activity **with other certification and assurance activities**.
- Benefit from a multidisciplinary privacy advisory team of **highly qualified professionals** with hands on experience with Data Protection assessments and transformations. Our specialists cover all aspects of privacy and Data Protection, including: legal, information governance, business processes, security technology and GRC tooling.
- KPMG's **global presence** allows for cost-effective **local delivery**. KPMG is a global network of over 152,000 professionals in 56 countries, with strong EU presence and EU Data Protection expertise.
- KPMG's advice goes beyond legal compliance and also puts the focus on assessing, implementing and monitoring adequate Data Protection controls and processes.

Credentials

KPMG has a proven track record in Data Protection. KPMG has successfully helped clients worldwide in various industries in becoming Data Protection compliant and maintaining their control status. Below only a select few are shown.

Major International Swiss Bank	Major international technology company	Pharmaceutical company	Public Bodies
KPMG drives the execution of the client data confidentiality program and other privacy and Data Protection initiatives in the bank.	KPMG assesses the policies and procedures to protect privacy and freedom of expression principles.	KPMG advised and supported on improving the governance framework for cross-border data transfers as a result of changes in the regulatory landscape.	KPMG performs Data Protection audits on behalf of regional governments' Data Protection Authorities
2013 – 2016	**ongoing**	**2015 – 2016**	**ongoing**

Contact us

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

Matthias Bossardt
Partner, Consulting
+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner, Consulting
+41 58 249 28 13
tbolliger@kpmg.com

kpmg.ch/gdpr

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

© 2018 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.