KPMG

EU General Data Protection Regulation ratified

Is your organization ready for the EU General Data Protection Regulation?

Changes in data protection regulation

GDPR ratified

The European Commission officially ratified the final version of the General Data Protection Regulation (GDPR) on the 14th of April. It is fair to say that this new legislation is the biggest and most impactful change in privacy and data protection regulation in history. This regulation came about after more than four years of deliberations and discussion and will impact organizations worldwide.

The regulation will be enforced after a two year period. This means that from January 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!

What's the big deal?

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.

HUGE 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.

REAL REPUTATIONAL RISK

Enforcement activities by data protection regulators will increase. Data protection breaches will hence be brought to light sooner. 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 citizens' and 'organizations that monitor (online) behaviour of EU citizens'. This means that more organizations are in scope of EU data protection regulation.

WHAT ARE THE MAIN NEW REQUIREMENTS?

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

Privacy by Design and Default

- *Under the old privacy 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.*

Privacy Impact Assessment (PIA)

- *Under the GDPR, organizations should carry out a PIA on the envisaged processing operations, where processing is likely to lead to high privacy risks.*
- *If the result of the PIA illustrates a high inherent risk, the data protection supervisory authority need be consulted prior to processing.*

Mandatory Data Privacy 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 from the organization.*
- *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 timely notify the supervisory authority in case of a data breach involving personal data.*
- *In case of a data breach with high privacy risks, also the data subjects should be informed.*

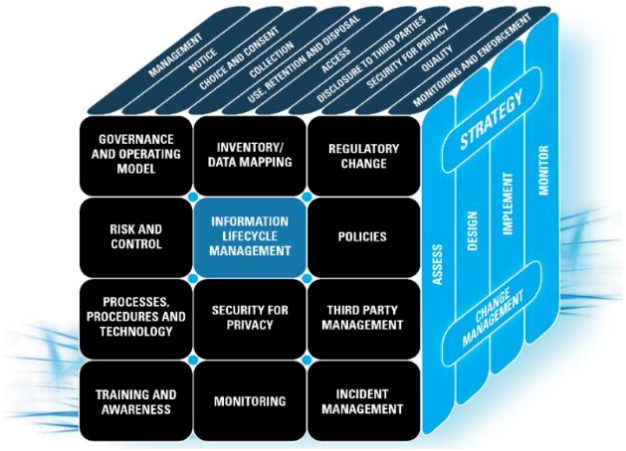
Other new requirements are Privacy Accountability, Right to be forgotten & data portability, Privacy protection for minors as well as Requirements for profiling, user tracking/monitoring & (Big) Data Analytics. In addition to the new requirements, many data protection requirements that existed under the old regime stay in effect (e.g. limitations on cross border data transfer, requirements on consent, requirements related to access rights of data subjects, etc.). Failure to implement one or more data protection requirements adequately, will lead to very significant fines. Hence, adequate implementation of data protection requirements within your organization, is now more important than ever.

KPMG

The new GDPR requirements that are mentioned on the front of this factsheet, show how the GDPR requires organizations to implement adequate and tailored privacy control frameworks and risk management. Mere policy updates for privacy compliance, will not suffice. The GDPR demands auditable privacy governance implementation and maintenance. We help you in implementing the right measures and managing those adequately.

WHAT TO DO NOW?

KPMG's privacy governance framework is based on the approach to: (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 privacy in your organization.



To determine how the GDPR affects your organization, we firstly assess the data protection readiness of your organization. We distinguish **four different assessment options**. Depending on your organization's privacy governance history, management and overall maturity, there is a readiness assessment available that would suit your needs best.

A. GDPR quick scan	Assessment which takes the additional requirements of the GDPR as the basis. The outcome of this assessment is the readiness status per new GDPR requirement, including related recommendations.
B. Privacy quick scan	Assessment which takes all relevant data protection and privacy principles as the basis, thereby highlighting the new requirements of the GDPR. The outcome is an overall privacy readiness status for your organization, including recommendations. This could serve as the basis for setting up or improving a privacy governance model for your organization.
C. Privacy maturity assessment	Maturity assessment which gives an overall indication of the privacy 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 privacy governance framework in accordance with the GDPR and other international privacy requirements.
D. Privacy attestation	Policy makers, business partners and customers increasingly demand you to demonstrate your commitment to data protection and privacy. This option 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?

- A Privacy / Data protection assessment will show your (internal) stakeholders your organization's **privacy readiness status** and will present clear and **workable recommendations for improving** your overall privacy and data protection governance.
- Benefit from a proven approach to privacy management that is **pragmatic, flexible, scalable** and allows you to focus on the privacy challenges and opportunities of your organization.
- Acquire a view of industry privacy 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** who have the skills, competencies and experience to support you with the most challenging issues. Our specialists cover all aspects of privacy, 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 over 2,000 security practitioners globally, giving us the ability to orchestrate and deliver to consistently high standards worldwide.

Contact us

For more information on our Privacy offerings or KPMG's Cyber Security Services, please contact us or visit us at **www.kpmg.com/nl/cybersecurity**

Koos Wolters
Partner
Tel. +31 20 656 40 48
E: wolters.koos@kpmg.nl

Ronald Koorn
Partner
Tel. +31 30 658 21 59
E: koorn.ronald@kpmg.nl

Maurice Koetsier
Senior Consultant
T: +31 30 658 21 68
E: koetsier.maurice@kpmg.nl