GDPR Preparation

IT Risk Advisory Services

Have you heard about the EU's General Data Protection Regulation, also known as GDPR? Are you familiar with new data protection requirements to which all enterprises and public organisations need to adapt their business, procurement and personnel administration processes? Did you know that the maximum fine for non-compliance is set to drastically increase and could reach 4% of an organisation's revenue?

Who is affected?

The EU's GDPR applies to all public and private organisations that manage the personal data of clients or employees. According to the regulation, "personal data" comprises not only information conventionally regarded as personal data (e.g. name and address) but also any information that enables the identification of a person, such as photos, financial data, fingerprints, medical data, browsing history, etc. GDPR goes into effect in all EU member states starting 25 May 2018. Moreover, it also applies to non-EU enterprises as long as they offer goods and services to customers within the EU. Taking all of that into consideration, there is hardly any organisation not affected by the GDPR rules.

Preparation tasks

There is not much time left to carry out the necessary organisational, operational, information security and privacy-related changes towards compliance. To accomplish this, one first needs to assess which of their enterprise's departments handles personal data and which workflows are affected. On the one hand, you need to know the nature of the data in question and how the organisation acquires it. On the other hand, you need to be aware of where the data is stored and monitor its protection, considering technical and administrative aspects as well. Furthermore, you need to assess which elements of the enterprise's current practice differ from GDPR requirements. Then, based on those considerations, it can be determined what steps need to be taken in order to comply with GDPR requirements. When setting improvement goals, important aspects, besides legal compliance, include cost efficiency and choosing a solution that fits the organisation's existing processes and systems.

Do the following issues sound familiar to you?

Many firms and public organisations face difficulties when it comes to interpretation of the GDPR due to its new perspective and complex rules. Often there arises the need for an assessment framework that helps evaluate an organisation's existing data protection capabilities and promote the planning and monitoring of improvement measures needed for GDPR compliance. Some examples:

- Do client and employee contracts need to be modified due to the GDPR? Do privacy information sheets and declarations need to be revised?
- What kind of organisational and technical solutions ensure classification and continuous registration of personal data managed by the organisation? Can the necessary changes be implemented in the existing systems or are new investments needed?

Important dates

GDPR finalised
In December 2015, the European Parliament and the Council agreed on the final text of the GDPR.

Formal adoption of GDPR
The regulation was published in the Official Journal of the European Union on 5 May 2016.

Entering into force
GDPR will enter into force in all EU member states after a 2-year transition period on 25 May 2018.

2015 — 2016 — 2017 — 2018 — 2019

– Which organisations are required to appoint a dedicated data protection officer? What kind of changes are needed in the organisational structure and in data protection processes?
– How can the level of data protection-related risks be determined based on the GDPR? What kind of IT security enhancement measures are needed and how can they help lower incident management costs?
– How do supplier contracts need to be modified? How do firms that store client or employee data at remote sites or in the cloud need to prepare themselves for GDPR?

How can we help?

Relying on the KPMG Privacy Management Framework, which covers all crucial areas of data protection, our professionals lead you through the steps of preparation for compliance with GDPR and help you meet the tight deadline. The main elements of our framework are outlined below.

Assessment

First, we assess which of your organisation's processes include managing personal information. Then we evaluate which risks are associated with the management of the personal data in question. For example, it does matter whether you are handling general personal data or sensitive personal information (e.g. medical or biometric data). We review whether your enterprise's existing privacy solutions are suitable for the management of the identified risks.

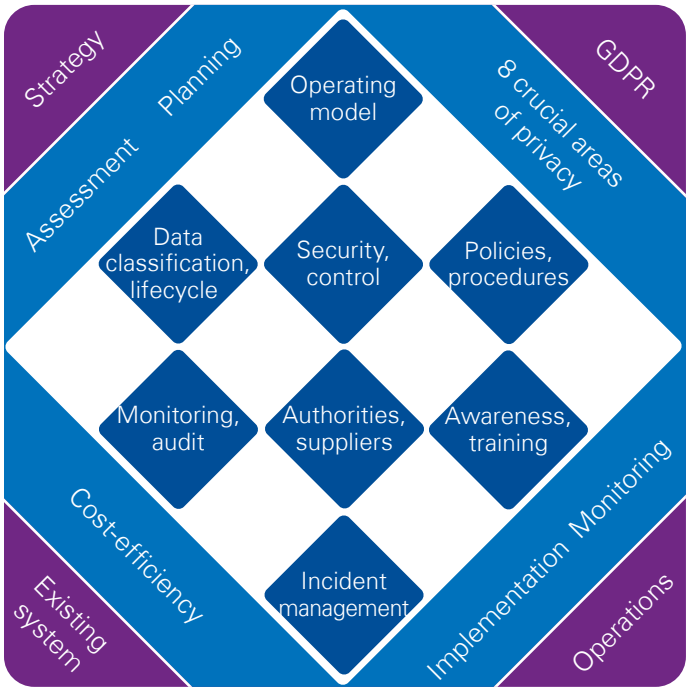
Planning

Our assessment helps in identifying key areas of GDPR compliance. Based on the assessment's results our experts help you plan enhancement measures which enable you to cost-effectively bridge the gap between your existing operating model and GDPR requirements. We help you implement a solution that best fits your enterprise's existing systems.

Implementation

Our professional competencies encompass the fields of information security, data protection, legal issues, ERP systems and organisational development and can support you in the implementation of improvement plans in all areas covered by GDPR.

KPMG Privacy Management Framework



Monitoring

We can take on quality assurance of the implementation of improvement plans, as well as the monitoring of its results, and data protection and data management audit for later retest. We help your organisation prepare itself for privacy audits carried out by authorities and in its reporting obligations to authorities.

What advantages do we bring?

KPMG's IT Risk Advisory Services practice has broad experience in the review and evaluation of information security and privacy maturity and in the planning and implementation of assessment-based, cost-efficient development. We support you with our expertise in all areas affected by GDPR: information security, privacy, legal issues, risk management, organisational development, and technical issues. Our objective is to help you to comply with the EU's new General Data Protection Regulation without draining your budget and seeking to gain the most advantages.

If our service offerings have aroused your interest, please contact us via the following contact information.

Contact:

György Sallai
Director
T.: +(36) 1 887 6620
E.: gyorgy.sallai@kpmg.hu

KPMG.hu