Our Services

Our Privacy Service has been designed on the basis that organizations need tailored risk-based solutions to address their individual privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, guiding you through the complexity of privacy and complex global organizations.

1. Define
Articulate the strategic links between business goals, risks and personal information processing activities and set high-level financial and resource needs for privacy management across your organization.

2. Assess
Undertake assessments to identify legal, technical and managerial risks associated with privacy compliance and areas where the organizations may be misinterpreting privacy requirements or failing to leverage the value of personal information.

3. Design
With an understanding of the current state and applicable privacy requirements and priorities, help your organization design the right approach to addressing privacy compliance.

4. Implement
Establish legal and corporate policies objectives and implement pragmatic privacy structures and controls to manage privacy risks in the context of your organization’s overall business risks. Our modular and layered structure enables targeted and tailored solutions to be developed and delivered at any level – from individual process to entire global organization.

5. Monitor
Help your organization design, implement and maintain a privacy monitoring framework, enabling timely assessment of governance structures and controls, and adherence to processes and procedures.

Privacy Management Framework
Our framework elements are the distinct elements that organizations employ to manage privacy. They provide a practical and pragmatic structure for organizing the day-to-day management and oversight required to manage privacy.

Find out how we can help you to prepare for the new privacy regime.
Dear reader,

The EU has reached an agreement on the new General Data Protection Regulation (GDPR). Belgian organizations will have less than two years to become compliant by pushing through managerial, technological and legal reforms where necessary. GDPR shall apply from the 25th of May 2018 and will impact every organization in different ways, depending on the sector in which it is active.

This regulation will replace the Belgian Privacy Act of 1992 and the existing Data Protection Directive which didn’t receive any significant updates since it was introduced in 1995. These new rules will help to stimulate the Digital Single Market in the EU by creating trust and legal certainty in the online environment.

Non-compliance can result in fines of up to €10 million or 2% of the annual global turnover when organizations don’t meet the obligations as a data controller or data processor, and up to €20 million or 4% of the annual global turnover for non-compliance with the basic principles for processing or the data subject’s rights.

Furthermore, your organization must demonstrate compliance with this new regulation. It is therefore recommended to prepare a personalized proactive framework that reflects the key elements of the GDPR.

Wouter Lauwers
Partner, K law

Benny Bogaerts
Director, KPMG Advisory

GDPR Essentials

Territorial reach
The extra-territorial reach of the GDPR implies that data controllers and processors located outside the EU can also fall within its scope under certain conditions. The transfer of personal data outside the EU is subject to strict rules.

Consent & new rights
The consent of a data subject for the processing of its personal data must be freely given, specific, informed and unambiguous. Furthermore, data subjects will have the right to withdraw consent at any given time, the right to data portability and the right to erasure.

DPIA to Privacy by Design
A Data Protection Impact Assessment (DPIA) will be mandatory in most cases in order to apply the newly introduced concepts of “privacy by design” and “privacy by default.”

Mandatory DPO
Your organization may be obligated to appoint a Data Protection Officer (DPO).

Data Breach
Data breaches should be reported to the supervising authority within 72 hours after becoming aware of the breach. Your organization should have the necessary processes and procedures in place to swiftly respond.

Processors
The GDPR imposes significant direct obligations upon the processors, such as taking appropriate measures to protect the processing of personal data, etc.

Roadmap

1. Define the goal
   — Define a strategic privacy roadmap
   — Define legal objectives

2. Assess the current state
   — Determine the current state of privacy maturity via an assessment
   — Review the compliance of your existing privacy notices and consent practices with the GDPR
   — Catalogue the Subject Access Request Response requirements.
   — Privacy Compliance Reviews
   — Check privacy due diligences
   — Review the legal basis of your existing processing activities with the GDPR

3. Design
   — Create a Custom Privacy Governance model and Privacy RACI
   — Draft data processing agreements
   — Prepare vendor risk assessment and auditing processes
   — Outline policy privacy, processes and guidance, including Websites
   — Design data inventory solution, questionnaire and toolkit
   — Define data transfer compliance mechanisms

4. Implement the changes
   — Privacy Improvement Program
   — Draft the necessary agreements for transferring personal data outside the EU
   — Further DPO
   — Implement notice and consent delivery process
   — Guide the implementation of Information Lifecycle Management requirements
   — Establishing clear policies and procedures in case of any data breach
   — Establishing a framework to demonstrate compliance and accountability

5. Monitor the results
   — Development of privacy metrics, including templates and dashboards
   — IT audit schedule aligned with Privacy roadmap
   — Process to monitor for and manage incidents affecting personal data, including reporting processes and templates
   — Reporting on training completion
   — Continuous follow-up of the GDPR for any legal changes

Compliance

Now

25th May 2018