Regulators, business leaders, and technologists all agree – an organization’s privacy efforts cannot be solely assured by compliance with regulations; privacy must become the default mode of an operation.

**Privacy by Design: a risk management solution**

Privacy by Design builds on the premise that privacy should be embedded into the design, operation, and management of IT systems, networks, and business practices in order to prevent privacy vulnerabilities and the potential for irreparable financial and reputational harm.

Originally developed by Dr. Ann Cavoukian, Privacy by Design is now law under the EU’s General Data Protection Regulation (GDPR) and a globally recognized ISO standard (ISO 31700, Consumer Protection: Privacy by Design for Consumer Goods and Services).

Privacy by Design is structured around 7 Foundational Principles, which exist as a baseline for robust data protection.

1) **Proactive not Reactive**: Privacy by Design anticipates risks and prevents privacy invasive events before they happen to build customer trust.
2) **Privacy as the Default Setting**: Personal data should be automatically protected – no action is needed by the user to protect their privacy – it is built into the system.
3) **Privacy Embedded into Design**: Privacy is embedded into the design and architecture of IT systems, and becomes part of the product, service or processes’ core functionality.
4) **Positive Sum, Not Zero Sum**: Privacy by Design avoids the false idea of trade-offs between privacy and security, showcasing that it is possible to have both.
5) **End-to End Security**: Privacy by Design embeds security into the system from the start, which works to ensure a secure lifestyle management of information.
6) **Visibility and Transparency**: Privacy by Design ensures operational execution aligns with policies. The end-user should know which data is collected, and for what purpose.
7) **Respect for User Privacy**: Privacy by Design develops trust by choosing user-centric measures - strong privacy defaults, appropriate notice, and empowering user-friendly options.

Compliance with Privacy by Design allows an organization to achieve a “defensible” position. A Privacy by Design Certification demonstrates an organization’s proactive, risk-based approach to achieving compliance, as well as earning customers’ trust while building a true due-diligence defence in the event of a privacy breach, investigation and/or complaint.

**Two-step process to achieving best-in-class privacy standard**

Obtaining a Privacy by Design Certification is a two-step process:

**Step One: Assessment**. Taking a holistic, risk-based approach, KPMG assesses an organization’s product, service, process or system using an assessment methodology structured around the 7 Foundational Principles of Privacy by Design that maps to international privacy legal requirements (e.g. GDPR), ISO privacy and security standards, regulatory expectations and industry best practices.
The assessment is conducted through a set of interviews with key stakeholders and a review of documentation. An organization’s current privacy controls and information handling practices are also reviewed to assess how well privacy is operationalized on the ground.

KPMG will issue a Privacy by Design Assessment Report that provides a current state ‘snapshot’ of an organization’s privacy posture along with a roadmap that identifies any gaps for remediation. Once the organization achieves a ‘clean report’, (e.g. without any gaps or deficiencies), it can proceed to Step Two, which is the certification process.

**Step Two: Certification.** An organization can apply to for an assessment by the Professional Evaluation and Certification Board (PECB), an ISO accredited third party certification body, which reviews KPMG’s Privacy by Design Assessment Report. If satisfied on its own criteria, PECB will issue a Privacy by Design Certification Seal for the organization’s product, service, process or system. The Certification Seal can be displayed on the company product offering for three years, subject to renewal.

**Contact us**

KPMG’s Privacy, Regulatory and Information Management (PRIM) practice is comprised of professionals from KPMG in Canada and from other KPMG member firms in privacy, data governance, cyber security, including former privacy lawyers, Chief Privacy Officers and privacy regulators.

For more information or to discuss how we can help you, please contact us:

Sylvia Kingsmill, BA, LLB  
PRIM, Forensic Risk Consulting  
Partner  
T: (416) 777-8190  
E: skingsmill@kpmg.ca

Karen Burke, JD  
PRIM, Forensic Risk Consulting  
Executive Director  
T: (647) 777-5251  
E: karenburke@kpmg.ca

Howard Wong, BAS, MLIS, CIPP/C  
PRIM, Forensic Risk Consulting  
Senior Manager  
T: (416) 777-3262  
E: howardwong@kpmg.ca

François Senécal, LLB, LLM  
PRIM, Forensic Risk Consulting  
Manager  
T: (514) 840-2342  
E: fsenecal@kpmg.ca

Eugen Miscoi, LLB, MA  
PRIM, Forensic Risk Consulting  
Senior Consultant  
T: (514) 940-4372  
E: emiscoi@kpmg.ca

Ana Crisan, BAH, MI  
PRIM, Forensic Risk Consulting  
Senior Consultant  
T: (416) 777-8610  
E: acrisan@kpmg.ca

Implement the solution; obtain the results

A Privacy by Design Certification Seal can serve as a valuable tool to demonstrating a proactive risk-based approach to privacy risk management. It also serves as a competitive advantage to earning consumer trust and loyalty with new technologies, services, or processes.