Deloitte.

RYERSON UNIVERSITY

# Privacy by Design

## Setting a new standard for privacy certification

Privacy by Design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices.

# Privacy by Design Framework

Organizations understand the need to both innovate and safeguard the personal and confidential data of their customers, employees, and business partners. This has become increasingly challenging in the era of "big data" for several reasons:

- Globalization has fostered an environment where knowledge workers feel the need to share information more readily, exposing organizations to a higher likelihood of information security breaches
- Organizational boundaries are no longer static, making it difficult to track how, where, and by whom information is being stored, managed, and accessed
- Collaboration and social networking tools promise new possibilities, but also come with potentially serious vulnerabilities if not proactively managed

> "Protecting privacy while meeting the regulatory requirements for data protection around the world is becoming an increasingly challenging task. Taking a comprehensive, properly implemented risk-based approach—where globally defined risks are anticipated and countermeasures are built into systems and operations, by design—can be far more effective, and more likely to respond to the broad range of requirements in multiple jurisdictions." – *Dr. Ann Cavoukian, Executive Director of the Privacy and Big Data Institute at Ryerson University, Three-term Information and Privacy Commissioner of Ontario, Creator of Privacy by Design*

In this complex electronic business environment, a "check the box" compliance model leads to a false sense of security. That's why a risk-based approach to identifying digital vulnerabilities and closing privacy gaps becomes a necessity. Once you've done the work to proactively ensure that your controls are implemented and your information is secure, having your privacy practices certified against a global privacy standard can take your privacy and security posture to the next level. And when you put privacy risk prevention and certification together, you have **Privacy by Design Certification**.

A demonstrated ability to secure and protect digital data—both your own and your customers'—is increasingly being recognized as a business imperative that yields a competitive advantage.

# 7 Foundational Principles

**Privacy by Design means building privacy into the design, operation, and management of a given system, business process, or design specification; it is based on adherence with the 7 Foundational Principles of Privacy by Design:**

Any organization launching new services, products, or innovative technologies, or expanding into new geographies through mergers or acquisitions, can benefit immensely from privacy certification.

# Benefits of Certification: Reap the rewards

Ensuring privacy and security—through every phase of the data lifecycle (e.g. collection, use, retention, storage, disposal or destruction)—has become crucial to avoiding legal liability, maintaining regulatory compliance, protecting your brand, and preserving customer confidence. That's especially true for organizations that are increasingly subject to heightened scrutiny both internally by their boards and externally by their regulators and business partners. By taking a dynamic, proactive approach to privacy protection, Privacy by Design certification will give your organization the ability to:

- Ensure compliance by getting ahead of the legislative curve and minimizing compliance risk
- Reduce the likelihood of fines and penalties, including financial losses and/or liability associated with privacy breaches
- Build your brand by fostering greater consumer confidence and trust thereby gaining a sustainable competitive advantage
- Better manage post-breach incidents to regain consumer trust and confidence
- Maintain best practices by seeking independent testing of privacy and security controls rather than more self-reporting or testing

**Cost of taking the reactive approach to privacy breaches:**

Privacy by Design goes well beyond accepted fair information practices and privacy standards, virtually assuring regulatory compliance—no matter where you operate.

# Steps to Certification
## Implementing Privacy by Design: It starts with three steps

Under our Privacy by Design framework, Ryerson University is responsible for certifying organizations that meet the necessary privacy criteria. To achieve certification, organizations must first undergo an initial assessment conducted by Deloitte.

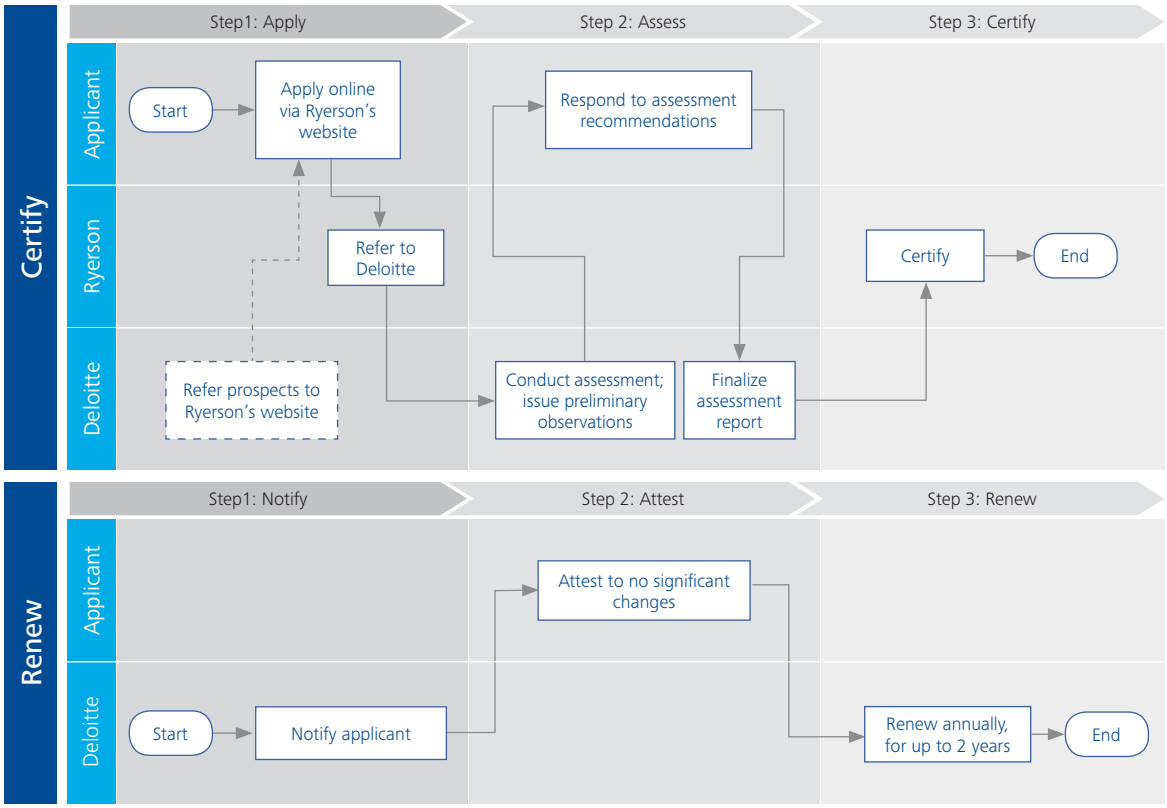
Using a set of well-defined assessment criteria, Deloitte's privacy and security professionals will test your product, service, or offering against the 7 Foundational Principles of Privacy by Design. We also assess the strength of your privacy practices relative to internationally recognized privacy principles, including privacy regulations, industry self-regulatory requirements, and industry best practices (e.g. FIPs, OECD, GAPP, CBR, and APEC Privacy Framework) using an assessment methodology based on harmonized privacy and security legal requirements.

To this end, Deloitte operationalized the Privacy by Design framework by developing 30 measurable privacy criteria and 107 illustrative privacy controls that organizations will be assessed against, using a unique scorecard approach that maps back to each of the 7 Foundational Principles.

---

Putting privacy front and centre:
Deloitte relies on our global team of privacy and security experts who are Privacy by Design accredited, including a former privacy regulator, privacy lawyers, and IT and security specialists. Taking a holistic, risk-based approach, Deloitte will test your controls using a quantifiable scorecard technique to help provide the privacy certification your organization needs.

The upshot is a simple three-step process for certification: apply, assess, and certify:




Organizations may pursue certification once the assessment is complete; any assessment rating below "satisfactory" will need to be addressed before receiving full certification.

# Deloitte Assessment Approach

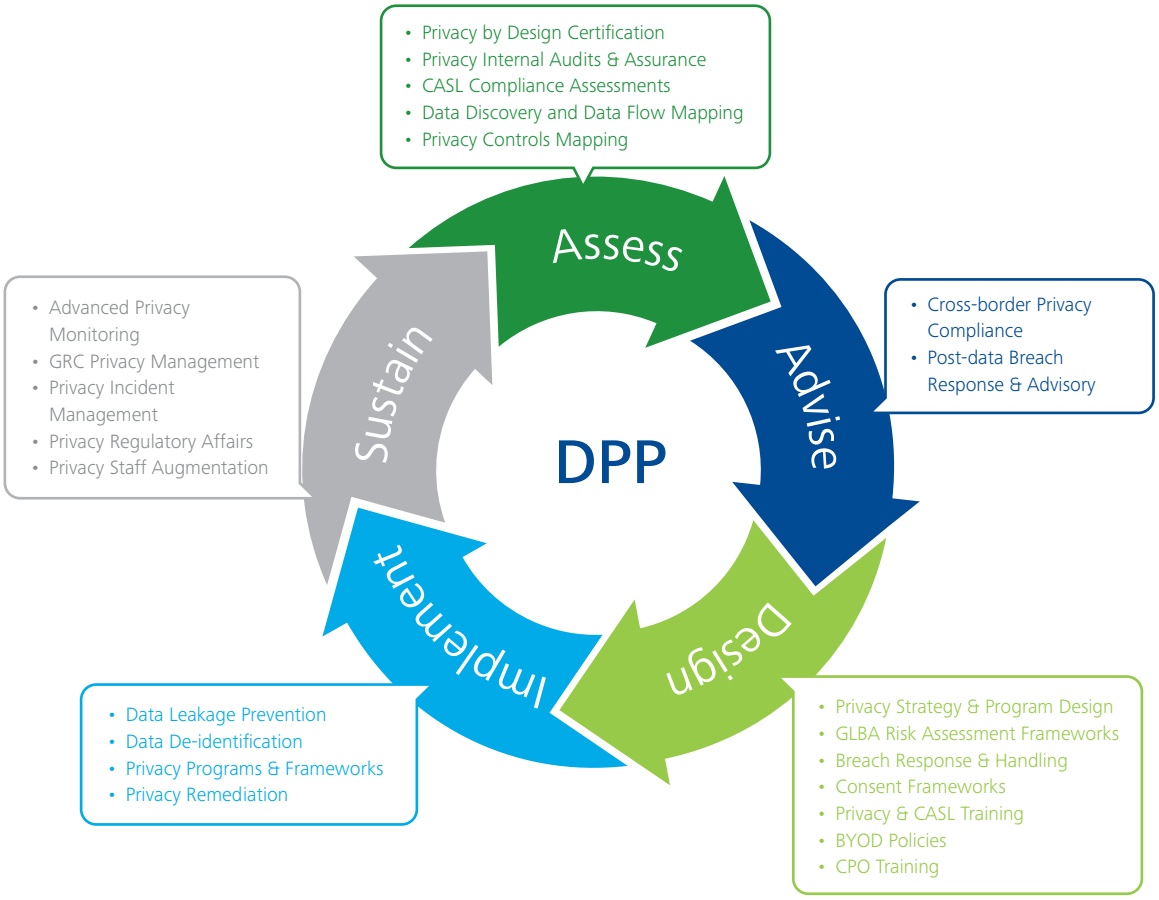
**Before you can be certified, you will be assessed according to this process:**

| | |
|---|---|
| **Scope** | We begin by working with you to identify the scope of your privacy review.<br><br>**The scope of your assessment can include:**<br>☑ All types of personal information holdings and related business processes, including medical and employee information<br>☑ A defined part of the organization, line of business, function, system, or initiative |
| **Assess & Test** | **Our privacy and security professionals:**<br>☑ Use a combination of manual reviews, sampling, and scorecard metrics to assess your current design controls and related information-handling practices<br>☑ Conduct company interviews, on-site visits (where required), and data discovery (where requested) to identify data collection and residency issues<br>☑ Evaluate whether a privacy or security control exists, and whether the privacy activities or controls have been properly designed<br>☑ Compare your solution architecture, related information-handling practices, and operational processes against control activities |
| **Report** | **We deliver results in a restricted use, detailed Privacy Scorecard report that:**<br>☑ Identifies any deficiencies or gaps in information system design, policies, and practices<br>☑ Includes an analysis of personal information and related privacy gaps across the data lifecycle<br>☑ Contains an analysis of your compliance requirements with all relevant policies, practices, laws, codes, and contracts<br>☑ Analyzes each element of your organization's privacy program, policies, and procedures<br>☑ Includes a gap analysis that highlights the gap between your desired state of risk management and the current "as-is" state<br>☑ Provides detailed observations and recommendations to management for closing identified privacy gaps |
| **Certify** | **As part of the certification process, Ryerson:**<br>☑ Verifies that any gaps identified in your Privacy Scorecard have been addressed and closed<br>☑ Displays your company's name on its validation page to provide real-time verification that your certification is current and valid |

Once you receive certification, you can display your Privacy by Design certification on your website and/or product or offering, and share your assessment results and certification with your business partners.

# Deloitte Data Protection and Privacy service catalogue

**Privacy by Design Certification is part of a full suite of Data Protection and Privacy (DPP) services offered by Deloitte:**



## Contacts

**Sylvia Kingsmill, BA, LLB**
National Partner, Data Protection and Privacy Leader, Enterprise Risk
skingsmill@deloitte.ca

**Dr. Ann Cavoukian, Ph.D.**
Executive Director, Privacy and Big Data Institute
ann.cavoukian@ryerson.ca

### About Sylvia Kingsmill

Sylvia Kingsmill, BA, LLB, leads the Data Protection and Privacy practice for Deloitte Canada. She has 15 years' experience in providing strategic, risk-based compliance and privacy advisory services, serving a diverse global client base. Her specialty is in advising executive teams on the development and implementation of data-driven digital strategies to support major IT and business transformation and alignment with regulatory requirements. She often deals with regulators, including Privacy Commissioners, on behalf of her clients in remediating regulatory findings and optimizing data management and governance practices. Sylvia recently developed the Privacy by Design Certification Program with Ryerson's Big Data and Privacy Institute to help clients launch new, privacy-enhancing technologies. She advises on innovative and ethical uses of big data while protecting privacy to help her clients manage not only their regulatory risks but also their branding and marketing strategy as they expand their digital footprint.

### About Dr. Ann Cavoukian

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She is presently the Executive Director of the Privacy and Big Data Institute at Ryerson University. Appointed as the Information and Privacy Commissioner of Ontario, Canada, in 1997, Dr. Cavoukian served an unprecedented three terms as Commissioner. There she created Privacy by Design, a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure, and business practices, thereby achieving the strongest protection possible. In October 2010, regulators at the International Conference of Data Protection Authorities and Privacy Commissioners unanimously passed a Resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. Since then, Privacy by Design has been translated into 37 languages.

### About Deloitte's National Data Protection and Privacy Practice

Deloitte's national Data Protection and Privacy practice is comprised of multi-disciplinary professionals specializing in technology, policy, security, law, information governance and management, project management, communications, and privacy regulatory affairs. The practice has helped clients in both the public and private sectors, many of whom must manage sensitive financial, personal, and medical information in accordance with a myriad of regional and international standards and regulations.

### About Ryerson University and the Privacy and Big Data Institute

Ryerson is Canada's leader in innovative, career-focused education. It is a distinctly urban university with a focus on innovation and entrepreneurship. Ryerson has a mission to serve societal need and a long-standing commitment to engaging its community. The Privacy and Big Data Institute at Ryerson was created to serve as a hub for Ryerson faculty, staff, and students engaged in data-driven research, innovation, and education. The Institute's mission is to pursue and promote collaborations with industry to address privacy, security, and/or data analytics challenges.

*Privacy by Design Certification is being offered by the Privacy and Big Data Institute at Ryerson University; it is not affiliated with the Information and Privacy Commissioner of Ontario nor does it signify compliance with Ontario's privacy laws.*

**www.deloitte.ca**

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© Deloitte LLP and affiliated entities.
Designed and produced by the Deloitte Design Studio, Canada. 15-2971H