MSECB

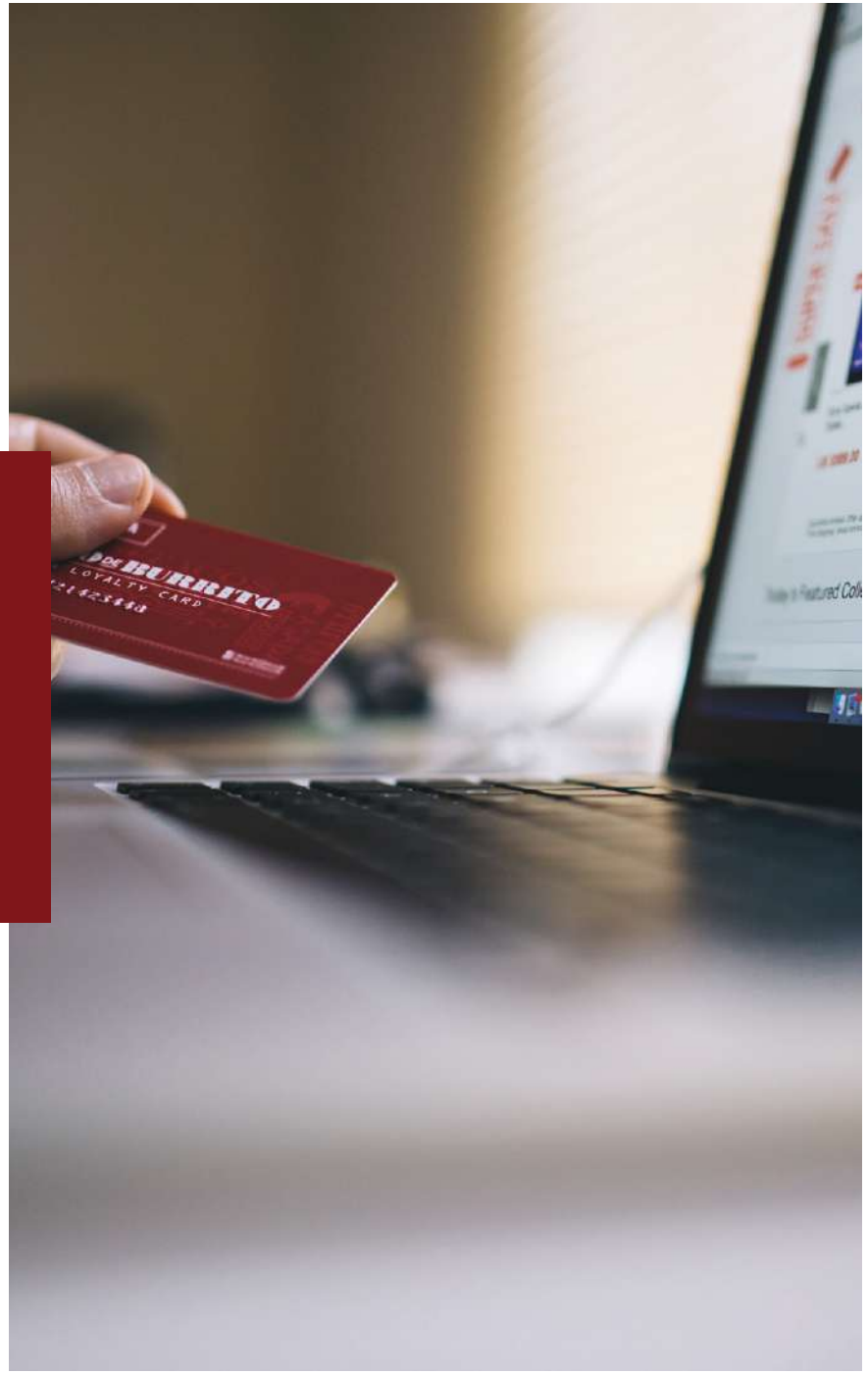
MSECB ISO 31700-1:2023 - PRIVACY BY DESIGN CERTIFICATION PROGRAM

www.msecb.com

Privacy

In the past, privacy and data protection have been perceived by many organizations as an issue mainly related to legal compliance, often confined to the mere formal process of issuing long privacy policies covering any potential eventuality and reacting to incidents in order to minimize the damage to their own interest.

Privacy has been a controversial topic for a long time; there were many attempts to define what privacy is. Commonly, privacy is defined as “the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information”.



What is personal data?

Personal data are any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data, for example, a name and surname; a home address; an e-mail address; an identification number; location data (for example the location data function on a mobile phone); and an Internet Protocol (IP) address. Personal data that has been de-identified, encrypted, or pseudonymized but can be used to re-identify a person remains personal data. Personal data that has been rendered anonymous in such a way that the individual cannot be identified is no longer considered personal data.

*Source: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What is Privacy by Design?

"Privacy by Design" has been frequently-discussed topic related to data protection. Privacy by Design states that any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or process.

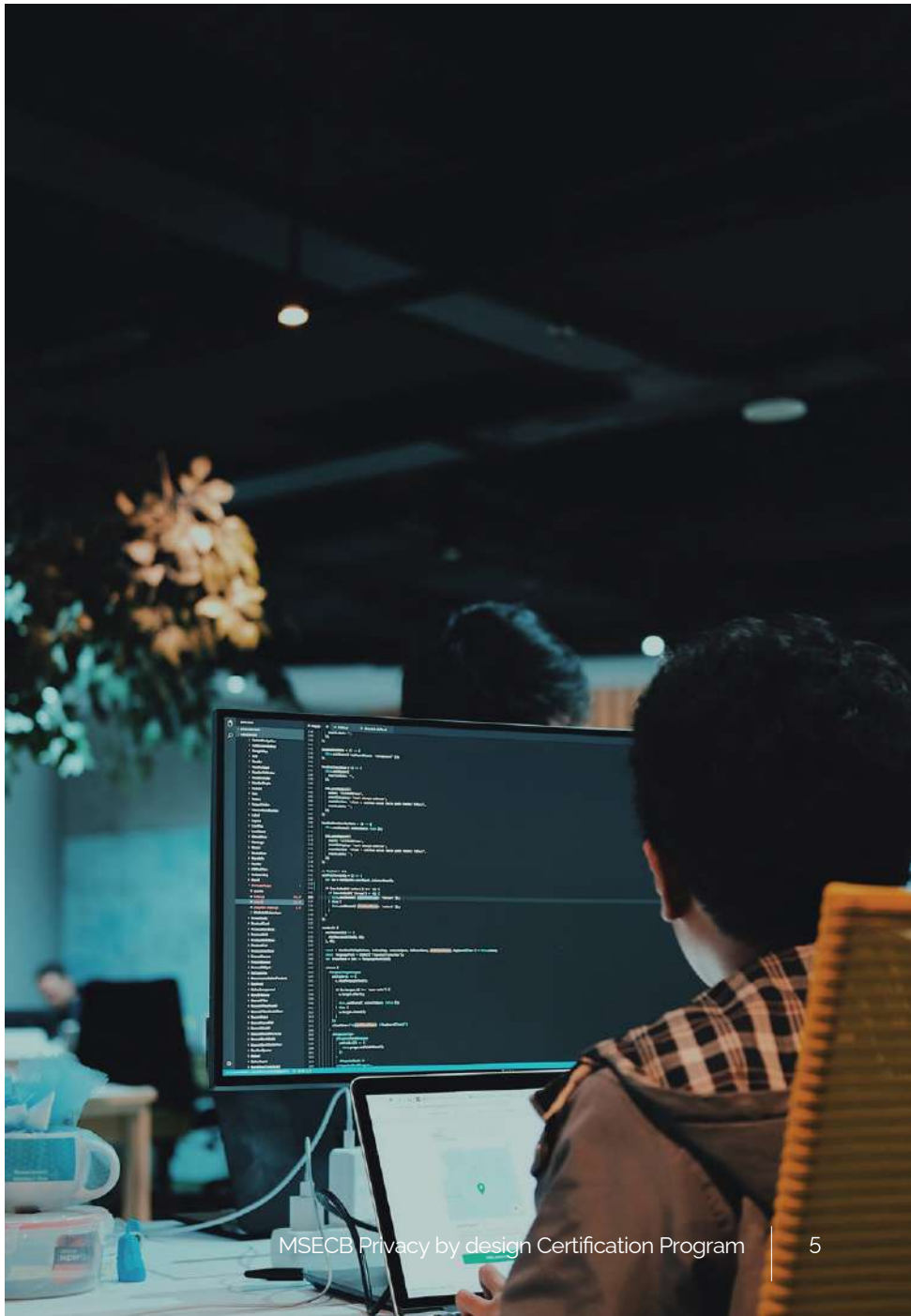
Privacy by design is about doing design (Principle 1), doing privacy (Principle 2), and doing privacy in design (Principle 3). The 7 Foundational Principles of Privacy by Design are presented below:

- Proactive not reactive; Preventative not remedial - Anticipate, identify, and prevent invasive events before they happen; this means taking action before the fact, not afterward;
- Privacy as the default - Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual;
- Privacy embedded into design - Privacy measures should not be add-ons, but fully integrated components of the system;
- Full functionality – Positive-sum, not zero-sum - Privacy by Design employs a "win-win" approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both;
- End-to-End Security – Lifecycle Protection - Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed;
- Visibility and transparency - Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification;
- Respect for user privacy - Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

The PbD concept assumes a holistic approach by transforming how an organization manages the privacy from policies and compliance to an organization-wide business issue and strategy.

This concept encompasses many elements in practice:

- Recognition that privacy interests and concerns must be addressed.
- Applications of basic principles expressing universal spheres of privacy protect.
- Early mitigation of privacy concerns when developing information technology and systems, across the entire information life cycle.
- Need for qualified privacy leadership and/or professional input.
- Adoption and integration of privacy-enhancing technologies.



Why PbD matters more than ever?

The notion of privacy by design as a voluntary concept is about to change. In Europe, GDPR makes PbD a legal requirement within the EU (note: European data protection and privacy laws are extraterritorial). This means that organizations will not only need to develop to Privacy by Design, but also document the Privacy by Design development processes.

Why certify?

By having Privacy by Deisgn Certification from a certification body as MSECB, your organization will be able to:

- Ensure compliance by getting ahead of the legislative curve and minimizing compliance risk.
- Reduce the likelihood of fines and penalties from authorities as results of privacy breaches.
- Maintain best practices with independent assessment of privacy and security controls.
- Gain competitive advantage and market access with relevant industry scheme certification.
- Customer confidence and trust.
- Reputation and respect.
- Continually improve processes and performance.
- Use Privacy by Design to enhance privacy awareness within your organization.

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 MSECB ISO 31700-1:2023 Privacy by Design Certification.

How to get certified?

Under the Privacy Certified Framework, MSECB is responsible to certify organizations that meet the necessary privacy criteria.

MSECB operationalized the ISO 31700-1:2023 - Privacy by Design framework by developing privacy criteria and illustrative pivacy controls that organizations will be assessed against from MSECB's privacy and security professionals. The MSECB's ISO 31700-1:2023 - Privacy by Design Framework is based on the General Data Protection Regulation, Bill C-27, Law 25, international law, regulatory expectations on facial recognition, artificial intelligence, and digital ID services, and ISO 31700-1:2023.

Below are described briefly the steps on how to get certified:

1. Apply - The ISO ISO 31700-1:2023 - Privacy by Design Certification begins when your organization submits application which can be found by request.
2. Assess - Assessment services will be carried out under a separate agreement where the product(s), service(s) and/or Process(es) being certified will be assessed. A report will be issued based on the assessment methodology developed exclusively for Certification.
3. Certify - After examining the assessment report, MSECB will issue a decision as to whether certification will be granted. Certified organization will be granted with the certificate and will be listed on our website.
4. Surveillance - Certifications are valid for a three-year period, but must be renewed annually. MSECB will remind you well in advance with all the details on how to keep your certification current.

Once you receive certification, you can display the ISO 31700-1:2023 - Privacy by Design Certification on your website and/or product offering, and share your assessment results and certification with you business partners.

Note: *ISO 31700-1:2023 Privacy by Design Certification is being offered by MSECB; it is not affiliated with the Information and Privacy Commissioner of Ontario nor does it signify compliance with Ontario's privacy laws.*

MSECB

www.msecb.com