JANUARY 2018

Privacy by Design

Privacy by Design is a methodology for proactively embedding privacy into information technology, business practices, and networked infrastructures. The Privacy by Design measures are designed to anticipate and prevent privacy invasive events before they occur.

SEVEN FOUNDATIONAL PRINCIPLES

The Privacy by Design framework is based on seven foundational principles:

1. Proactive not Reactive; Preventative not Remedial

Anticipate, identify and prevent privacy invasive events before they occur.

2. Privacy as the Default Setting

Build in the maximum degree of privacy into the default settings for any system or business practice. Doing so will keep a user's privacy intact, even if they choose to do nothing.

3. Privacy Embedded into Design

Embed privacy settings into the design and architecture of information technology systems and business practices instead of implementing them after the fact as an add-on.

4. Full Functionality — Positive-Sum, not Zero-Sum

Accommodate all legitimate interests and objectives in a positive-sum manner to create a balance between privacy and security because it is possible to have both.

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

5. End-to-End Security — Full Lifecycle Protection

Embed strong security measures to the complete lifecycle of data to ensure secure management of the information from beginning to end.

6. Visibility and Transparency — Keep it Open

Assure stakeholders that privacy standards are open, transparent and subject to independent verification.

7. Respect for User Privacy — Keep it User-Centric

Protect the interests of users by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario