Glossary of Definitions and Terms

Access control –Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users must present credentials before they can be granted access. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

Confidential information – This is information that often holds tremendous value and importance for organizations. The disclosure or loss of such confidential information can be of grave concern for organizations but it does not constitute a privacy breach because it does not involve the handling of personal information.

Consent - In PIPEDA, consent functions as a way for individuals to protect their privacy by exercising control over their personal information—what personal information organizations can collect, how they can use it, and to whom they can disclose it.

Data sharing agreement - A data-sharing agreement is a formal contract that clearly documents what data are being shared and how the data can be used. Such an agreement serves two purposes. First, it protects the business providing the data, ensuring that the data will not be misused. Second, it prevents miscommunication on the part of the provider of the data and the SME receiving the data by making certain that any questions about data use are discussed. Before any data are shared, both the provider and receiver should talk in person or on the phone to discuss data-sharing and data-use issues and come to a collaborative understanding that will then be documented in a data-sharing agreement.

Personal information - Although there may be jurisdictional differences, personal information (also known as personally identifiable information or “PII”) may be defined as any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature.

Privacy – Information privacy refers to the ability of individuals to exercise personal control over the collection, use and disclosure by other parties of their personal information.

Privacy breach - A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly shared. A privacy breach may also be a consequence of faulty business procedures or operational breakdowns.

Privacy Impact Assessment (PIA) – A privacy impact assessment (PIA) is a process used to determine how a program, service, system or technology could affect the privacy of an individual. It can also help to avoid or lessen possible negative effects on privacy that might result from the introduction of a program, service, system or technology. Also, a PIA is a way for the SME to state its commitment to protect the privacy of individuals. PIAs promote transparency and accountability, and contribute to continued consumer confidence in the way the SME manages personal information.

Purpose limitation – Protects individuals by setting limits on how those collecting the data are able to use the individual’s data. The concept of purpose limitation has two main building blocks: personal data must be collected for 'specified, explicit and legitimate' purposes (purpose specification) and not be 'further processed in a way incompatible' with those purposes (compatible use). [Source: WP 29 paper on purpose limitation]

Secondary use - This is the use of information collected for one purpose for a different purpose without a person’s consent. Secondary creates a harm, as it involves using information in ways a person does not consent to and might not find desirable.

Security/Safeguards – The physical, technological and administrative protective measures and security techniques that are designed to ensure that personal information remains confidential, available and uncompromised. This includes measures such as encryption, passwords, and firewalls designed to prevent unauthorized access to information, to protect the integrity of computing resources, and to limit the potential damage that can be caused by unauthorized access.

Threat Risk Assessment (TRA) – This is the component of risk management that identifies and quantifies the risks to the organization’s information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization’s mission.