Privacy Horizon

General Data Protection Regulation (GDPR) Overview

EUROPEAN CANADIAN CENTRE FOR INNOVATION AND RESEARCH

enterprise europe network

Business Support on Your Doorstep

Disclaimer

I am not a lawyer. Nothing I say today should be construed as legal advice.

I am a privacy and security specialist who works with organizations on compliance solutions to ensure that they are on the right side of the law.

Agenda

- GDPR Overview
- Who does GDPR Apply To?

Privacy Horizon

Overview of GDPR

- The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that came into effect on May 25, 2018, in the EU. It aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- Key aspects include data protection rights for individuals, obligations for data processors and controllers, and stringent data breach notification requirements.

Key Principles

The regulation is built around several key principles concerning the processing of personal data:

- Lawfulness, Fairness, and Transparency: Processing must be lawful, fair, and transparent to the data subject.
- Purpose Limitation: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data Minimization: Data collection must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- Accuracy: Personal data must be accurate and, where necessary, kept up to date.
- Storage Limitation: Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security.
- Accountability: The controller is responsible for, and must be able to demonstrate compliance with, the above principles.

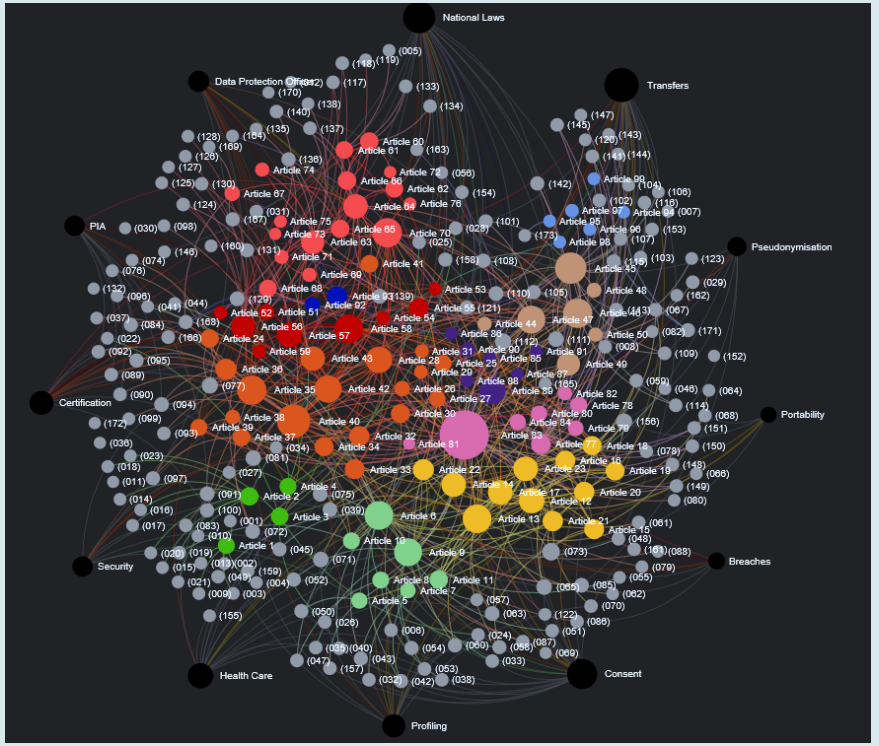
Right of the Individuals

The GDPR provides several rights to individuals regarding their personal data, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten)
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

Who does GDPR Apply To?

- The GDPR applies to organizations located within the EU AND will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.
- It covers a wide range of information that can be used alone or in combination with other data to identify a person. This includes names, photos, email addresses, bank details, social networking posts, medical information, genetic information, biometric information or a computer IP address.
- GDPR distinguishes between anonymized and pseudonymized information



Roles Under the GDPR

- Data Subject - a natural person whose personal data is processed by a controller or processor
- Data Controller - a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- Data Processor - any person who processes the data on behalf of the data controller.

Penalties Under GDPR

- Organizations that breach GDPR can be fined up to 4% of their annual global turnover or € 20 million.
- This is the maximum fine that can be imposed for the most serious infringements, e.g., insufficient customer consent to process data or contravening the core of Privacy by Design concepts.
- There is a tiered approach to fines. For example, a company can be fined 2% for not having its records in order (Article 28), not informing the supervising authority and data subject (individual) about a breach, or not conducting an impact assessment.

Horizon Europe Program

Universities in Canada participating in initiatives within the EU, such as the Horizon Europe Program, may need to comply with the General Data Protection Regulation (GDPR) under certain conditions. GDPR applies to organizations outside the EU if they offer goods or services to or monitor the behavior of EU data subjects. Here are the key considerations for Canadian universities in this context:

1. Data Processing Activities: If the personal data of individuals in the EU are processed as part of the Horizon Europe Program, it will likely need to comply with GDPR. This could include data processing related to research activities, collaboration with EU entities, or any other actions involving EU residents' personal data.
2. Data Transfer and Storage: GDPR compliance is also necessary when personal data collected in the EU is transferred to Canada or stored on Canadian servers.
3. Collaborative Nature of the Program: The Horizon Europe Program's focus on collaboration across borders means Canadian universities may act as data controllers or processors in partnership with EU-based institutions. This requires GDPR adherence regarding data protection agreements, data subject rights, and other related responsibilities.
4. Technology and Data Use: Given the program's emphasis on innovation and technology, Canadian universities should be particularly mindful of GDPR's requirements regarding the use of new technologies and data science. This includes obligations around data protection by design and by default and conducting Data Protection Impact Assessments (DPIAs) when necessary.

Questions

Contact
Patrick Lo
Patrick.lo@privacyhorizon.com