PRIVACY
FACT SHEET

General Data Protection Regulation

OVERVIEW

The European Union's (EU) General Data Protection Regulation (GDPR) is a privacy law that came into force on May 25, 2018. It is designed to give individuals in the EU control over how their data are processed and used.

Although it is an EU law, the GDPR may apply to public institutions and health information custodians in Ontario in certain limited circumstances. The Information and Privacy Commissioner of Ontario (IPC) does not oversee or enforce the GDPR.

This fact sheet provides institutions and custodians in Ontario with general information about the potential application of this law, and some of its key requirements. Some GDPR requirements may go beyond the privacy rules set out in the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), and the *Personal Health Information Protection Act* (*PHIPA*).

This fact sheet is not a legal interpretation of any provision of the GDPR and does not provide legal advice about its application in Ontario. Organizations should consult their legal counsel for advice. The scope of the law's application and the interpretation of its requirements depend on future decisions and guidance issued by the EU data protection authorities and courts.

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

TERMINOLOGY

The GDPR applies to the processing of personal data. The regulation defines **personal data** as "any information relating to an identified or identifiable natural person," who is called a **data subject**. Personal data includes IP addresses, email addresses and telephone numbers.

Processing refers to any operation performed on personal data, including its collection, use, storage and disclosure. **Controllers** are organizations responsible for determining the purposes and means of processing personal data—why and how they intend to collect and use the personal data. Organizations that process personal data on behalf of a controller are called **processors**. If these terms were used in Ontario, institutions or custodians would be the controllers. If an institution or custodian outsourced activities, such as data storage, to a third party, the third party would be a processor.

The EU regulatory bodies that oversee the GDPR in member states are called **supervisory authorities** in the regulation, and are more commonly known as **data protection authorities**.

APPLICATION OF THE GDPR

The GDPR applies to the processing of personal data by a controller or processor that is established in the EU, even if the data processing occurs outside of the EU. It also applies to the processing of personal data by a controller or processor who is not established in the EU, if the data processing activities relate to:

- offering goods and services to individuals in the EU, or
- monitoring the behavior of individuals in the EU.

Simply having a public website that individuals in the EU can access is not enough to bring an organization under the GDPR. However, the presence of additional factors, such as using a language or currency used in the EU, or specifically mentioning customers in the EU, may demonstrate an intent to offer goods or services to individuals in the EU.

Although it does not apply to most activities conducted by Ontario's institutions and custodians, certain activities may be subject to the GDPR. For example, Ontario colleges and universities that actively recruit foreign students from the EU **may** be subject to the GDPR with respect to their processing of the personal data of those students in the EU.

Organizations that are subject to the GDPR and fail to comply may face significant fines.

KEY PROVISIONS OF THE GDPR

The following is a brief description of a few key provisions of the GDPR. This is not a comprehensive guide but instead highlights some of the significant provisions of the GDPR, which may differ from or go beyond the requirements in *FIPPA, MFIPPA* and *PHIPA*. Note that there may be exceptions to these rules that are not addressed in this guidance document.

Lawful Grounds for Processing Personal Data

The regulation sets out the circumstances in which personal data may be lawfully processed. Some examples of these circumstances follow.

Personal data may be processed if the data subject has provided consent. The consent must be specific, freely given, informed and unambiguous. Consent must be express and not implied, and must be set out separately from other matters. That means consent cannot be bundled into general terms of use for a service. The data subject or individual must also have the right to withdraw consent at any time.

Personal data may be processed where it is necessary for the controller's legitimate interests, and if it does not override the individual's fundamental rights and freedoms. This applies to situations where the individual would reasonably expect the processing to occur. For instance, an EU applicant to an Ontario university or college would reasonably expect that the institution would require their personal data to process their application.

Personal data may also be processed if it is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority.

Special Categories of Personal Data

Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric or health data, or data concerning a person's sex life or sexual orientation are subject to heightened restrictions on when and how it may be processed.

Notice of Collection

The GDPR requires that individuals receive notice prior to the collection of their personal data. The controller must provide the individual with information such as:

- the identity and contact details of the controller
- the intended purposes of processing the data
- the legal basis for processing the data
- who will receive the data
- how long the data will be retained

Individuals must also be notified of their rights under the GDPR, which are discussed in more detail below. Similar notice requirements apply where the controller receives personal data from a source that is not the individual, unless an exception applies.

Data Protection Impact Assessments

A data protection impact assessment, commonly known in Ontario as a privacy impact assessment, is required where processing is likely to result in a high risk to the rights and freedoms of the individual. The GDPR includes examples of high-risk activities that require an assessment. The controller must conduct the data protection impact assessment before processing begins.

Mandatory Breach Notification

Controllers are required to notify the **data protection authority** of a personal data breach without delay, or not later than 72 hours after having become aware of it. Notification is required unless the breach is unlikely to result in a risk to the rights and freedoms of the individual.

Controllers are required to notify the **individual**, without undue delay, when a breach is likely to result in a high risk to an individual's rights and freedoms.

Rights of the Individual

Right to be informed: As noted above, individuals have the right to be informed about how a controller will be processing their personal data.

Right to access and correction: Generally, individuals have the right to request a copy of the personal data they provided to a data controller and to correction of their personal data.

Right to data portability: Individuals have the right to receive the data in a structured, commonly used, machine-readable format.

Right to object to processing: In certain circumstances, individuals have the right to object to the processing of their personal data, such as processing for direct marketing.

Right to restrict processing: Individuals have the right to restrict the processing of personal data in specific situations, such as where the individual contests the accuracy of the data, or where the individual has objected to the processing of their data and is awaiting a decision.

Right to complain: Individuals also have the right to complain to their data protection authority if they believe the processing of their personal data violates the GDPR.

Right to erasure: Under the GDPR, individuals have the right to request that their personal data be erased, which is sometimes called **the right to be forgotten**. This right only applies in certain circumstances, such as where the data are no longer necessary for the purpose for which they were collected or processed. Individuals also have the right to request that their personal data be delisted or deindexed from a search engine.

There are exceptions to this right. These include where the processing of the personal data is necessary to exercise the right of freedom of expression; for compliance with a legal obligation; to exercise or defend a legal claim; or where it is in the interests of public health.

ADDITIONAL RESOURCES

- **EU General Data Protection Regulation**
- Article 29 Data Protection Working Party, **EU General Data Protection Regulation: General Information Document**
- European Commission, **2018 Reform of EU Data Protection Rules**
- Information Commissioner's Office of the United Kingdom, **Guide to the General Data Protection Regulation**
- Office of the Information and Privacy Commissioner of British Columbia, **Competitive Advantage: Compliance with PIPA and the GDPR**
- Information and Privacy Commissioner of New South Wales, **NSW Public Sector Agencies and the GDPR**

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