GDPR for Canadian Organisations
What you need to know!
Brief history of the EU and Canadian data protection laws

- **Post WWII**, concerns about protection of human rights.
- **1950**, EU Convention on Human Rights (ECHR) introduces privacy.
- **1980**, OECD guidelines on transborder data flows.
- **1981**, EU Treaty 108 – eight principles for protecting personal data
- **1983** Canadian Privacy Act (federal / established the office of the Privacy Commissioner of Canada)
- **1995**, Canadian Freedom of Information Act
- **1998**, EU States transpose DPD to law (e.g. UK’s DPA1998, Germany’s Bundesdatenschutzgesetz)
- **2000**, Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
- **2014**, Canada’s Anti-Spam Law (CASL) comes into force (3 year transition period – July 1st 2017)
- **2016**, EU GDPR approved, becomes law two years from publication (May 25th 2018)
The **General Data Protection Regulation** (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents, no matter where they are located.

- **Enhanced** personal privacy rights
- **Increased** duty for protecting data
- **Mandatory** breach reporting
- **Significant** penalties for non-compliance

Microsoft believes the GDPR is an important step forward for clarifying and enabling individual privacy rights.
What are the key changes to address the GDPR?

**Personal privacy**
- Individuals have the right to:
  - Access their personal data
  - Correct errors in their personal data
  - Erase their personal data
  - Object to processing of their personal data
  - Export personal data

**Controls and notifications**
- Organizations will need to:
  - Protect personal data using appropriate security
  - Notify authorities of personal data breaches
  - Obtain appropriate consents for processing data
  - Keep records detailing data processing

**Transparent policies**
- Organizations are required to:
  - Provide clear notice of data collection
  - Outline processing purposes and use cases
  - Define data retention and deletion policies

**IT and training**
- Organizations will need to:
  - Train privacy personnel & employee
  - Audit and update data policies
  - Employ a Data Protection Officer (if required)
  - Create & manage compliant vendor contracts
The GDPR by the numbers: recitals + 11 chapters over 99 Articles = 204 pages

- Chapter I General Provisions: Articles 1 – 4
- Chapter II Principles: Articles 5 – 11
- Chapter III Rights of the Data Subject: Articles 12 – 23
- Chapter IV Controller and Processor: Articles 24 – 43
- Chapter V Transfer of Personal Data to Third Countries: Articles 44 – 50
- Chapter VI Independent Supervisory Authorities: Articles 51 – 59
- Chapter VII Cooperation and Consistency: Articles 60 – 76
- Chapter VIII Remedies, Liabilities and Penalties: Articles 77 – 84
- Chapters IX – XI Various specific provisions: Articles 85 – 99
Key definitions

‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Articles 51 – 52: Independent supervisory authorities

Member States must provide one or more independent supervisory authorities:

- Monitor the application of the GDPR.
- Supervisory authorities must act independently.
- Member States must provide adequate resources.

Lead supervisory authorities:

- Entities operating in more than one state can choose a lead supervisory authority for all their pan-EU activities.
- Monitor compliance in respect of cross-border processing by an organisation whose main establishment is in that Member State.
Remedies, liability and penalties

Article 83: General conditions for imposing administrative fines.

€20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher).

€10,000,000 or, in case of an undertaking, 2% total worldwide annual turnover in the preceding financial year (whichever is greater).

Articles

- e.g.
- 5: Principles relating to the processing of personal data
- 6: Lawfulness of processing
- 7: Conditions for consent
- 9: Processing special categories of personal data (i.e. sensitive personal data)
- 12 – 22: Data subject rights
- 44 – 49: Transfers to third countries
- 58: Supervisory Authorities

Articles

- e.g.
- 8: Child’s consent
- 25: Data protection by design and by default
- 26: Joint controllers
- 27: Representatives of controllers not established in EU
- 26 – 29 and 30: Processing
- 33 & 34: Notification of breaches
- 35 & 35: Data protection impact assessment & prior consultation
- 37 – 39: DPOs
How the EU GDPR defines personal data

**Personal data**

Any information related to an identified or identifiable natural person including direct and indirect identification. Examples include:

- Name
- Identification number (e.g., SSN)
- Location data (e.g., home address)
- Online identifier (e.g., e-mail address, screen names, IP addresses, device IDs)

**Sensitive personal data**

Personal data afforded enhanced protections:

- Genetic data (e.g., an individual’s gene sequence)
- Biometric Data (e.g., fingerprints, facial recognition, retinal scans)
- Sub categories of personal data including:
  - Racial or ethnic origin
  - Political opinions, religious or philosophical beliefs
  - Trade union membership
  - Data concerning health
  - Data concerning a person’s sex life or sexual orientation
Article 6: Lawfulness of processing

Processing will only be lawful if ONE of the following conditions is met:

Data subject gives consent for one or more specific purposes.
Processing is necessary to meet contractual obligations entered into by the data subject.
Processing is necessary to comply with legal obligations of the controller.
Processing is necessary to protect the vital interests of the data subject.
Processing is necessary for tasks in the public interest or exercise of authority vested in the controller.
Processing is for the purposes of legitimate interests pursued by the controller.
The following conditions apply for consent:

- Controllers must be able to demonstrate that consent was given.
- Written consent must be clear, intelligible and easily accessible, otherwise not binding.
- Consent can be withdrawn any time, and it must be as easy to withdraw consent as give it.
- Consent to processing data is not necessary for the performance of a contract.
- Ticking a box or choosing appropriate technical settings is still valid.
Article 8: Conditions applicable to child’s consent for information society services

The following conditions apply for child consent:

• If consent is given and the child is at least 16 years old.
• Below the age of 16 years, parental authorization is required.
• Member States may reduce the definition, but not below 13 years.
• Controller shall make reasonable efforts to verify authorization.
• Rules on the validity, formation or effect of a contract in relation to a child shall not be affected.
• Information Society Services – Google, eBay etc.
A legal contract must ensure that the processor:

• processes the personal data only on documented instructions from the controller;
• ensures that persons authorised to process the personal data observe confidentiality;
• takes appropriate security measures;
• respects the conditions for engaging another processor;
• assists the controller by implementing appropriate technical and organisational measures;
• assists the controller in ensuring compliance with the obligations in respect of security of processing;
• deletes or returns all the personal data to the controller after the end of the provision of services; and
• makes available to the controller all information necessary to demonstrate compliance with the Regulation.
Article 32: Security of processing

A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:

- Pseudonymisation and encryption of personal data.
- Ensuring the ongoing confidentiality, integrity and availability of systems.
- A process for regularly testing, assessing and evaluating the effectiveness of security measures.
- Taking security measures that comply with the concept of data protection by design.
- Taking steps to ensure that any natural person working for the controller or processor only processes data under explicit instruction unless required to do so by EU or Member State law.
Where there is a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Communication of the breach to the data subject shall be described in clear and unambiguous terms.

Breach notification to the data subject is not required if:

▪ the personal data has been rendered unintelligible to any person who is not authorised to access it, such as through encryption;
▪ the controller has measures that ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
▪ it would involve disproportionate effort. In such a case, there shall instead be a public communication, or similar measure, whereby the data subjects are informed in an equally effective manner.

Supervisory authority may direct controller to notify data subject if it considers personal data breach to be a high risk
Data protection officers (DPOs)

Article 39: Tasks of the data protection officer

- To inform and advise.
- To monitor compliance.
- To provide advice with regard to data protection impact assessments.
- To cooperate and liaise with the supervisory authority.
- To be a point of contact for data subjects.

The DPO must have due regard to risk associated with processing operations.
Article 35: Data protection impact assessment

DPIA must be performed where processing is likely to result in a high risk to the rights and freedoms of natural persons.

It shall contain at least:

A description of processing and operations.
An assessment of the necessity and proportionality of the processing.
An assessment of the risks to the rights and freedoms of data subjects.
The measures envisaged to address the risks.
Evidence of compliance with approved codes of conduct.
A statement as to whether data subjects have been consulted.
Transfer of personal data to third countries or international organisations

Article 45: Transfers on the basis of adequacy

A transfer may take place where there is an adequate level of protection. The adequacy criteria:
the rule of law;
respect for human rights and fundamental freedoms;
relevant legislation, both general and sectoral, including:
  - concerning public security;
  - defence;
  - national security; and
  - criminal law.

### Transfer of personal data to third countries or international organisations

No restrictions on transfers to EEA countries:

<table>
<thead>
<tr>
<th>Austria</th>
<th>Germany</th>
<th>Malta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Greece</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Hungary</td>
<td>Norway</td>
</tr>
<tr>
<td>Croatia</td>
<td>Iceland</td>
<td>Poland</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Ireland</td>
<td>Portugal</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Italy</td>
<td>Romania</td>
</tr>
<tr>
<td>Denmark</td>
<td>Latvia</td>
<td>Slovakia</td>
</tr>
<tr>
<td>Estonia</td>
<td>Liechtenstein</td>
<td>Slovenia</td>
</tr>
<tr>
<td>Finland</td>
<td>Lithuania</td>
<td>Spain</td>
</tr>
<tr>
<td>France</td>
<td>Luxembourg</td>
<td>Sweden</td>
</tr>
<tr>
<td></td>
<td></td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Transfer of personal data to third countries or international organisations

The following additional countries are considered by the EU as having adequate data protection laws:

- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay
Transfer of personal data to third countries or international organisations

Article 46: Transfers subject to appropriate safeguards

Personal data transferred only where there are appropriate safeguards, enforceable data subject rights and legal remedies.

The appropriate safeguards may be provided by:

• a legally binding and enforceable instrument between public authorities or bodies;
• binding corporate rules in accordance with the GDPR;
• standard data protection clauses adopted by the Commission;
• approved codes of conduct (privacy Shield).
Resources

- www.eugdpr.org
- Ico.org.uk: Getting ready for the GDPR
- Ico.org.uk: Overview of the General Data Protection Regulation (GDPR)
- www.microsoft.com/gdpr