GDPR

for Canadian small businesses: What does this mean for you?

What is the GDPR?

The General Data Protection Regulation (GDPR) is the European Union's (EU) new privacy law. Its aim is to give greater protection and rights to individuals in the EU in regards to the collection and use of their personal data.

Does it apply to your business?

If your business has clients, customers, or website visitors in the EU, you must be in compliance with the GDPR.

Also, if you collect personal data from European citizens (e.g. through a subscription form on your website) and/or, send commercial emails, the GDPR applies to you and it is your duty to comply.

What do we mean by personal data?

By personal data, we mean anything that can identify an individual.

- Age
- Ethnicity
- Gender
- Postal Address
- Job Position
- Biometric data such as fingerprints and facial recognition
- Medical information
- Unique identifiers such as IP address, location data, email address, etc.

The 3 actors of the GDPR

The GDPR makes the distinction between 3 actors.

Data Subject

The person whose personal data is being collected, which could be users, website visitors, or customers.

Data Controller

The business who is asking users, website visitors, or customers for their personal information. Your business would be considered the data controller.

Data Processor

A third party that processes and stores the data on behalf of the data controller. For example, Cyberimpact is a data processor.

What could you face if don't comply?

You could face a fine of **up to 20 million Euros** or **4% of your revenue from the previous year**, whichever is greater, as well as bad press and a potential loss of confidence from customers.

Recommendations for

GDPR COMPLIANCE

1 Understand and document all personal data your business is handling

You need to identify how your business collects and processes personal data. This means your business is responsible for tracking:

- The personal data that you currently hold, as well as the personal data that you intend to collect (e.g. names, emails, addresses, etc.).
- How you got this information (e.g. a customer form, subscription forms on website, membership form, quote enquiry, etc.).
- Reason for collecting and handling personal data.
- How long have you had the data, and is it still relevant and required for the purposes you collected it.
- If you share this information with other organizations.

2 Data privacy rights and data access requests

Clearly state how and why your business intends to use the data being collected. You must also state how your customers can modify and view their personal data. For example, having a good data privacy policy will help make sure you're protecting this right. As well, customers have the right to request that you delete their personal data. You must also make sure that you have the technology and processes in place to complete these requests within one month.

3 Appoint a data protection officer

Designate someone from your business to be responsible for data protection matters (Data Protection Officer)*. The appointed individual would be responsible for raising awareness of data protection regulations, training employees, and monitoring compliance.

4 Review and update your security measures

Only use reliable processors who are familiar with privacy laws (GDPR, CASL). If you store this data on an IT system, limit the access to the files containing the data (e.g., by a password or by regularly updating the security settings of your system).

5 Obtaining consent

Segment your EU contacts in different groups or lists (e.g. within your email marketing provider). You should only add or email customers who have given you "expressed consent", and only keep the personal data for as long as necessary. Your business must keep a record of how and when an individual gave consent. Opting for a mailing list does not give the business owner ability to use a customer's data for something else unless this is clearly outlined.

6 Data breach process

If personal data is accidentally lost, hacked, altered, or destroyed, your business is responsible for managing any data breaches. This must be reported to the relevant EU data protection authority within 72h of becoming aware of the data breach occurrence. You must also notify all affected individuals.

7 Consult with an expert

Consider conducting a compliance assessment with the help of professionals.

* You don't need to designate a Data Protection Officer if processing of personal data isn't a core part of your business, and your activity isn't at a large scale.