INFO·TECH
MONTRÉAL

THE NON-PROFIT EXECUTIVE DIRECTOR'S GUIDE TO NAVIGATING LAW 25

WHY COMPLIANCE MATTERS

ASSESSING YOUR CURRENT COMPLIANCE STATUS

HANDLING DATA BREACHES

OVERVIEW OF LAW 25

As a non-profit, Law 25 means **reviewing and updating your data handling practices.** It involves ensuring that you meet the law's requirements while continuing to serve your mission effectively. **Organizations that do not comply with Law 25 are subject to potential fines and penalties.**

WHAT DOES LAW 25 REQUIRE?

Enhanced Consent

Organizations must obtain clear and **explicit consent** from individuals before collecting their personal data.

Transparency Obligations

Non-profits need to provide detailed information about **how personal data is used and processed.**

Data Protection Measures

The law requires organizations to implement **robust security measures** to protect personal data.

Rights of Individuals

Individuals have rights to **access, correct, and erase** their personal data.

ENHANCED CONSENT

All details about the data being collected and how it will be used should be summarized clearly and using simple language in your privacy policy. **Adding a checkbox at the bottom of all form submissions requiring having read your privacy policy can help in acquiring enhanced consent.**

HOW DO I OBTAIN ENHANCED CONSENT?

Informed Consent

Individuals should be fully informed about **what they are consenting to**, including the specific purposes for which their data will be used.

Clear and Simple Language

Avoid legal jargon and ensure that the **information is easily understandable by the average person** in consent forms.

Regular Review and Updates

Regularly review and update consent preferences to ensure they remain valid. If there are any changes to how personal information will be used, obtain new consent with the updated details.

☑ **I have read and agree to the terms and conditions outlined in the privacy policy.**

Link to your privacy policy

SUBMIT

TRANSPARENCY OBLIGATIONS

In your privacy policy, you should include details about what information is collected, for what purpose(s) that information will be used and how it will be stored. **This ensures that users filling out your forms are fully aware of what they are consenting to.**

WHAT SHOULD I INCLUDE IN MY PRIVACY POLICY?

Information Collected

Try to keep this to the bare minimum required to perform your job function. It might be tempting to ask for full name, phone number, email address, home address, date of birth. etc, but make it a point to evaluate and include only necessary details. **This minimizes risk of data theft in the event of a breach.**

Purpose of Collection

Relate this back to how this information will be used to perform your job. If you'll be communicating exclusively via email, it may not be necessary to collect phone numbers, and vice versa.

Data Protection Officer (DPO) Contact Details

Each organization must appoint a data protection officer to oversee data protection practices and ensure that personal information is handled in accordance with the law. **If a DPO is not explicitly appointed, the responsibility defaults to the highest-ranking individual, such as the executive director.**

User Rights

These include the right to access, correct and erase their personal information from an organization's database upon request. **Instructions for making such requests should be outlined in your privacy policy in clear language.**

DATA PROTECTION MEASURES

Evaluate your current security practices. A compliance audit helps identify areas where your data handling practices may fall short of Law 25 requirements. Look at how you collect, store, and process personal data and assess whether your current procedures meet the legal standards.

WHERE SHOULD I LOOK?

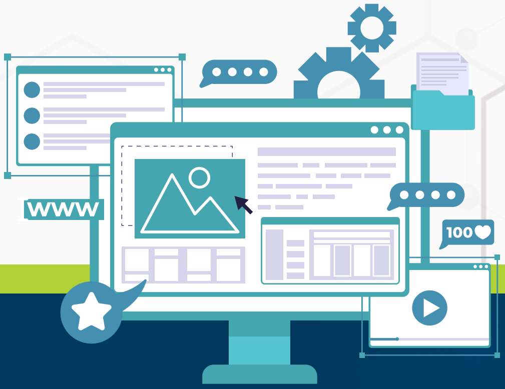
Your web sites(s)

Audit the areas of your website where you're actively collecting personal data such as forms. **Keep your privacy policy up-to-date** with information about how data is collected, used and stored.

Where is that information stored?

When someone fills out the forms on your site, where is that information sent?

- Is it sent directly to your / another employee's **inbox**?
- Is it stored in a customer relationship management **(CRM) software**?
- Is it integrated with an existing **spreadsheet** that fills upon submission?



INFO·TECH
MONTRÉAL

DATA PROTECTION MEASURES

Once you know where data is stored, **make sure those databases are locked down to prevent unauthorized access.**

HOW DO I SECURE IT?

Zero-trust access

Access to these databases of information **should only be shared with employees on a need-to-know basis**. In other words, if the employee doesn't need it to perform their job function, they shouldn't have it.

Multi-factor authentication (MFA / 2FA)

When someone who is authorized to access that information, **they should be required to provide additional forms of identification** to verify that they are who they say they are. Additional forms of verification can take on different forms.

Something you **know** (ex. passwords)

Something you **have** (ex. code sent to your phone)

Something you **are** (ex. fingerprint, retina scans)

RANKING TYPES OF MFA

Like tying your bike to a rack with chains and padlocks is probably more secure than using a cable lock, **some types of MFA are more secure than others**. Here's a rundown of the most common types of MFA and their security levels.

No MFA, password-only

The lowest level of security, this can easily be breached by anyone staring over an authorized user's shoulder, or with a simple keylogger that can track your keystrokes. **Should never be used to access sensitive information.**

Email codes

Provides an extra layer of security, but relies on the security of the email account. **If the email account is compromised and not also secured via MFA, then this method is no longer a reliable security measure.**

Text / Call one-time passwords (OTPs)

Better than email codes but **can still be rendered useless if a bad actor has your phone number reassigned to another SIM card** (read about SIM swap fraud).

Authenticator apps / Hardware tokens

Generate OTPs using an app on your phone or external hardware that are **only valid for for a short timeframe** (ex. a new code is generated every 30 seconds.)

Biometric authentication

Uses physical characteristics unique to you like **fingerprints, retina scans or facial recognition**. Very secure but can be expensive to implement.

RIGHTS OF INDIVIDUALS

Under Quebec's Law 25, end-users have several important rights regarding their personal information including **how they can access, modify or erase it upon request.**

WHAT ARE THE KEY USER RIGHTS?

Right to be Informed

This ties back into transparency obligations **requiring organizations to explicitly state how information is being collected, used, and shared.**

Right to Access / Rectification / Erasure

Users may request a copy of their data and information about how it is being used at any time. They also reserve the right to **request corrections and delete it** if the data is no longer needed for its original purpose.

Right to Withdraw Consent

Individuals can withdraw their consent for the processing of their personal information at any time. This means **organizations must stop using the data** for the purposes for which consent was originally given.

INFO·TECH
MONTRÉAL

HANDLING DATA BREACHES

If you suspect that a data breach has occurred, often through infection via malware, **take the following steps to minimize the risk of data theft.**

1

Quarantine

Any computers that you suspect have been compromised in a data breach **should be disconnected from the network immediately** to prevent spread and additional damage.

2

Scan for Infection

Ensure that any active malware infections have been removed from the compromised device before reconnecting it to the network. Reach out to your IT provider to confirm removal of any infections.

3

Determine the Cause

While security breaches can happen for various reasons, it's often the case that they occur due to unintentional mistakes or oversights.

4

Prevention

Once the cause has been identified, shift your focus toward end-user education by ensuring that everyone has the knowledge and tools they need to prevent such incidents in the future.

Once a security breach occurs, there's a significant chance that some data may have been compromised. While we can't change what has happened, we can take strong measures to prevent future incidents and protect our data moving forward.

ANY QUESTIONS?

As the executive director of a non-profit organization, staying compliant with Law 25 can be a lot to juggle, including **protection of personal information, implementing robust privacy policies, and regularly updating security measures to meet the stringent requirements.**

Navigating these regulations can be complex and time-consuming, but it's crucial for maintaining trust and transparency with donors and stakeholders.

If you ever need assistance with remaining compliant with Law 25, we're just a phone call away, ready to support you in every way we can.

INFO·TECH
MONTRÉAL

REACH OUT FOR ADDITIONAL SUPPORT

☎ (514) 634-4636 x108 ✉ alessandro@infotechmontreal.com 🌐 www.infotechmontreal.com