

PROGRAMME PRIORITÉ PRP* PRIVACY NOW PROGRAM

BONNES PRATIQUES PRP
PRIVACY GOOD PRACTICES

Septembre 2023 September

Avis de non-responsabilité

Rien dans le présent document ne doit être considéré comme étant des conseils juridiques.

Tout conseiller est invité à obtenir de tels conseils auprès de ses propres conseillers juridiques.

Disclaimer of liability

Nothing in this document should be construed as legal advice.

All advisors are invited to obtain such advice from their own legal representatives.

Table des matières

- La protection des renseignements personnels (PRP)
- La PRP au Canada
- Requis québécois depuis septembre 2022
- Requis québécois pour septembre 2023
- Bonnes pratiques de protection des RP
- Liens utiles

Table of contents

- Privacy
- Privacy in Canada
- Requirements in Quebec since September 2022
- Requirements in Quebec for September 2023
- Privacy good practices
- Useful links

****Click [here](#) for English version***

La protection des renseignements personnels

Tout individu a le droit au respect de sa vie privée.

À cette fin, il doit pouvoir compter sur la protection de ses renseignements personnels, lorsqu'il les confie à son conseiller

Quel que soit son support ou la forme sous laquelle il est accessible, un renseignement personnel est un renseignement :

- relatif à un individu;
- et qui peut permettre d'identifier cet individu (directement ou indirectement).

Exemples de renseignement personnel :

- adresse personnelle
- courriel
- numéro de téléphone
- date de naissance
- revenu
- détention d'actifs
- informations relatives à la tolérance au risque d'un investisseur individuel
- informations relatives aux investissements et transactions que fait un individu

Les informations relatives à une compagnie ne sont pas des renseignements personnels, sauf celles concernant les individus qui y sont liés.

Niveau de sensibilité

d'un renseignement personnel

Certains renseignements personnels ont une plus grande valeur pour un individu dans le cadre de sa vie privée.

S'il confie des renseignements personnels sensibles à une entreprise, la personne concernée s'attend à ce que celle-ci les traite avec encore plus de précaution que ses autres renseignements.

Exemples de renseignement personnel avec un plus **haut niveau de sensibilité** :

- informations médicales
- numéro d'assurance sociale
- coordonnées bancaires
- cote de crédit

La PRP au Canada

Le traitement de renseignements personnels des Canadiens effectué par une **entreprise privée** dans le cadre de ses **activités commerciales** est encadré par une législation fédérale qui s'applique partout au pays, sauf dans trois provinces, qui disposent de leur propre législation : le Québec, l'Alberta et la Colombie-Britannique

Chaque législation instaure sa propre autorité réglementaire

Fédérale

Commissariat à la protection de la vie privée du Canada

Québec

Commission d'accès à l'information (« CAI »)

Alberta

Commissariat à l'information et à la protection de la vie privée de l'Alberta

Colombie-Britannique

Commissariat à l'information et à la protection de la vie privée pour la Colombie-Britannique

Leur rôle est, dans leur juridiction respective :

- d'enquêter sur les plaintes pour violation de la vie privée qui leur sont adressées,
- de procéder à des inspections chez les entreprises,
- d'imposer aux entreprises contrevenantes de changer leurs pratiques,
- d'imposer des sanctions pécuniaires en cas de contravention à la loi

La protection des renseignements personnels

Une affaire sérieuse

En réponse aux préoccupations grandissantes des Canadiens relativement à leur vie privée, les gouvernements souhaitent instaurer des législations plus strictes à ce sujet.

Ils envisagent ainsi des **sanctions** beaucoup plus sévères envers les entreprises qui manqueraient à leurs obligations en matière de protection des renseignements personnels.

Notamment, **au Québec**, les sanctions prévues peuvent aller jusqu'à un montant maximum de :

- **100 000 \$** à l'encontre des personnes physiques,
- **25 000 000 \$** (ou 4% du chiffre d'affaires mondial annuel) à l'encontre des personnes morales.

Nouveaux requis en PRP au Québec

Depuis septembre 2022

Dans le cadre de vos activités commerciales, vous devriez déjà, entre autres, avoir mis en place les principaux éléments ci-dessous:

1. Nomination d'un responsable de la protection des renseignements personnels

La responsabilité d'assurer la protection des renseignements personnels revient d'office à la personne ayant la plus haute autorité dans l'entreprise, mais elle peut déléguer cette fonction. Cette personne est responsable de veiller à assurer le respect et la mise en œuvre des lois en matière de protection des renseignements personnels au sein de l'entreprise. Elle est aussi le point de contact principal vers qui les individus peuvent se tourner s'ils souhaitent de l'information sur les renseignements personnels que l'entreprise détient sur eux. Ses coordonnées doivent donc être publiées sur le site web de l'entreprise.

2. Signalement d'un incident de confidentialité

Tout accès, transfert ou utilisation non autorisé à des renseignements personnels ou leur perte constitue un incident de confidentialité et doit être inscrit dans un registre de l'entreprise et lorsqu'il représente un risque de préjudice sérieux pour l'individu affecté, l'individu et la Commission d'accès à l'information (CAI) doivent être informés. Lorsque l'individu affecté est un client d'[nom de l'entité d'iAGF concernée], vous devez en aviser [nom de l'entité d'iAGF concernée] sans délai en toute circonstance.

3. Déclaration des banques de données biométriques

La collecte de données biométriques (ex: données sur la voix, les empreintes digitales, le visage) nécessite l'obtention du consentement exprès des individus concernés. Si vous souhaitez utiliser des données biométriques d'individus dans le cadre de vos activités, vous devez en aviser préalablement la CAI.

Nouveaux requis en PRP au Québec

Pour septembre 2023

Voici les principaux éléments à **mettre en œuvre**

Adoption de politiques et de pratiques de protection des renseignements personnels

Des politiques et pratiques claires en matière de gouvernance et de PRP impliquant notamment la conservation et destruction de ces données ainsi qu'un processus de traitement des plaintes sont requises. Ces politiques doivent être publiées sur le site internet de l'entreprise de manière claire et adaptées en fonction des activités de celle-ci. Pour en savoir sur les politiques et pratiques de l'IA Groupe financier, consulter son Avis relatif à la protection des renseignements personnels à [ia.ca](#) Section Protection des renseignements personnels.

Évaluation des facteurs relatifs à la vie privée (EFVP)

Les organisations au Québec doivent réaliser une EFVP lors d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels ou avant de communiquer de telles information à l'extérieur de la province. Cette mesure a pour but de s'assurer que les concepts en matière de PRP sont tenus en compte avant d'entreprendre toute activité pouvant affectant la vie privée d'un individu.

Obligation d'information et de transparence

Obligation de fournir des informations claires et simples lors de la collecte de renseignements personnels, en particulier sur les finalités, les moyens de la collecte, la possibilité de toute communication de renseignements personnels à l'extérieur de la province et les droits d'accès et de rectification.

Nouveaux droits individuels

Les individus peuvent demander la destruction des renseignements personnels qu'une entreprise détient sur eux et si l'entreprise n'est plus justifiée de les conserver, elle doit y donner droit et surtout fournir aux individus une attestation que la destruction a bel et bien eu lieu.

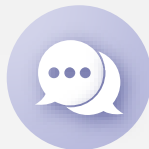
Toute entreprise prenant des décisions fondées exclusivement sur le traitement automatisé de renseignements personnels doit en informer les individus concernés et leur donner le droit d'en savoir plus.

À venir en septembre 2024 – Droit à la portabilité

The background is a solid blue color. Overlaid on this are numerous small, stylized human figures in various poses and colors (white, yellow, grey, etc.), scattered across the frame. In the lower right quadrant, there is a large, faint, concentric circular pattern resembling a fingerprint or a ripple in water.

Bonnes pratiques en PRP à adopter en tout temps

Informez vos clients



- Vos clients potentiels ou existants doivent **comprendre ce que vous souhaitez faire** avec leurs renseignements personnels (RP), pourquoi vous les recueillez et comptez les utiliser et à qui vous pourriez les partager
- **Soyez prêt à expliquer** les fins pour lesquelles ils sont recueillis, à qui ils seront communiqués et pourquoi
- **Comprenez les droits** que vos clients ont à l'égard de leurs renseignements personnels (droit d'y accéder, de les rectifier, d'en demander la destruction, d'avoir plus d'informations à leur sujet) afin de pouvoir les informer sur ceux-ci et répondre à leurs demandes, le cas échéant

Avoir sous la main un **document de référence** comme l'Avis relatif de la protection des renseignements personnels de iA Groupe financier ([lien](#)) vous permettra d'avoir des réponses aux questions de vos clients

Obtenir un consentement



- Assurez-vous d'obtenir **tous les consentements nécessaires** pour l'utilisation et la communication des renseignements personnels de vos clients que vous avez prévu faire.
- **Investia/iAGPP** inclut dans le processus d'ouverture de compte un consentement et vous devez vous assurer que tous les clients en aient connaissance. Cependant, vous pourriez avoir besoin d'un **consentement additionnel**, selon les services que vous offrez à vos clients, pour d'autres activités non liées à Investia/iAGPP, comme la planification successorale ou des activités d'assurance.
- Un client peut toujours **retirer son consentement**. Toutefois, si jamais le client retire son consentement pour des fins nécessaires pour lui offrir votre prestation de service, cela peut signifier que vous ne serez plus en mesure de maintenir votre relation avec lui.

Limitier la collecte, l'utilisation et la communication de RP



- Avant de recueillir des renseignements personnels, prenez le temps de **valider si vous en avez réellement besoin** dans le cadre de votre prestation de service
- **Restreignez l'utilisation** des renseignements personnels de vos clients à ce qui est nécessaire ou encore à des activités pour lesquelles vos clients ont spécifiquement consenti
 - Ils peuvent avoir retiré leur consentement, donc toujours valider le statut de leur consentement au moment de l'utilisation
- Ne communiquez des renseignements personnels à des tiers (ex: partenaires, fournisseurs de services) que lorsque c'est **vraiment nécessaire à vos activités** et que vous avez le consentement de votre client, lorsque requis
 - N'oubliez pas qu'il est souvent nécessaire d'établir un **contrat écrit avec ce tiers** incluant des clauses spécifiques avant de lui communiquer de telles informations

Conserver les RP juste le temps nécessaire



- Déterminez à l'avance combien de temps vous conserverez les renseignements personnels de vos clients
 - Un calendrier définissant les durées de conservation applicables selon la nature des renseignements personnels et le contexte d'utilisation est un outil essentiel
- Identifiez où vous conserverez ces RP, dans quel(s) système(s) et limitez le plus possible les copies non nécessaires (ex: courriels)
- Ces pratiques aident à limiter la probabilité d'une fuite de données et les conséquences qu'elle pourrait avoir sur vos clients et sur vous

Protéger les RP



Mettez en place des contrôles et des mesures de sécurité afin d'assurer en tout temps la protection des renseignements personnels qui vous sont confiés

- Pour ce faire, assurez-vous de bien gérer l'accès que vos collaborateurs pourraient avoir aux renseignements personnels de vos clients et de le limiter au strict nécessaire
- Bien former vos collaborateurs sur les bonnes pratiques en matière de PRP est également essentiel pour qu'ils les adoptent
- Référez-vous au Guide des bonnes pratiques en cybersécurité sur d'autres pratiques à adopter pour protéger, entre autres, les renseignements personnels sous votre responsabilité

The background is a solid blue color. It features a pattern of stylized, semi-transparent human figures in various poses, scattered across the frame. Additionally, there are concentric, wavy white lines that resemble a fingerprint or a ripple effect, primarily located on the right side of the image.

Liens utiles pour tous les types d'entreprises

1. Gouvernement du Québec

[Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, Entreprises \(quebec.ca\)](#)

2. Commission de l'accès à l'information

https://www.cai.gouv.qc.ca/documents/CAI_Guide_obligations_entreprises_vf.pdf

3. Gouvernement du Canada:

aperçu des lois relatives à la PRP

https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/02_05_d_15/

4. Guide de conformité

[Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé, BLG.](#)

5. Conformez votre entreprise à la Loi 25 sans vous ruiner

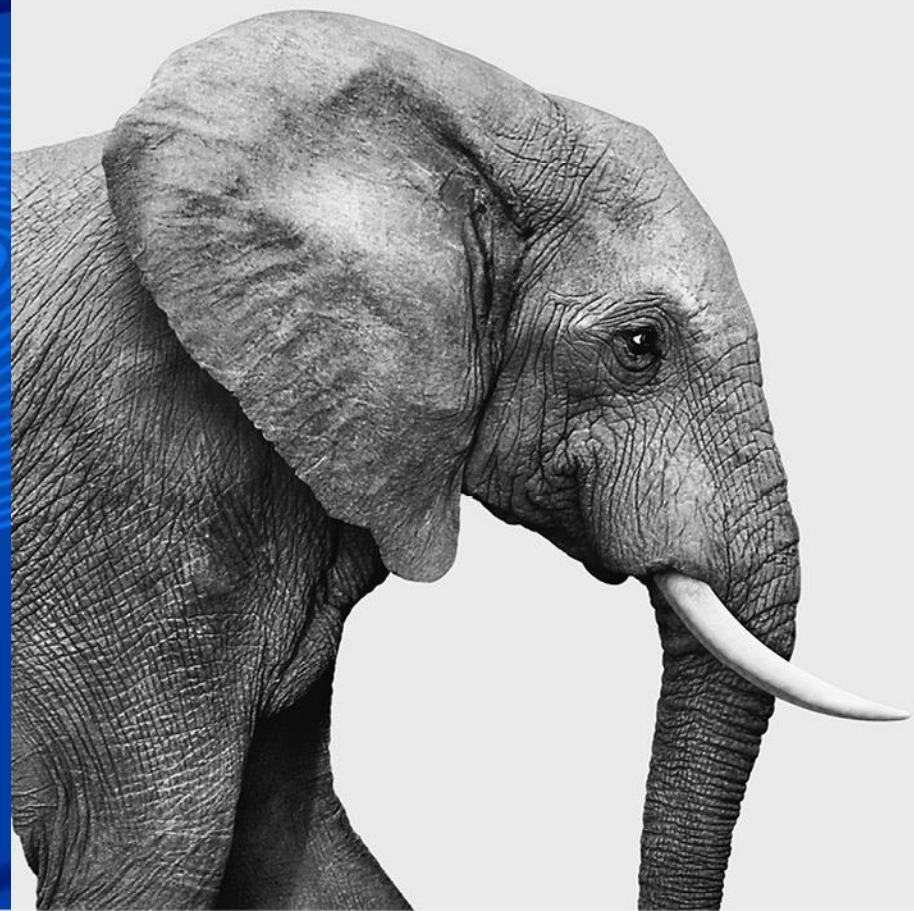
www.devenirresponsable.com

6. CyberEco

[Protection des données – Cybereco](#)

7. Fournisseurs de formations

- [Pensez cybersécurité \(pensezcybersecurite.gc.ca\)](http://pensezcybersecurite.gc.ca)
- [Sensibilisation à la cybersécurité | Terranova Security](#)
- Serene risc : [cybersec 101](#)



ON S'INVESTIT, POUR VOUS.
INVESTED IN YOU.

Privacy

Every individual has the right to privacy.

To this end, they must be able to count on the protection of their personal information when they entrust it to their advisor.

Regardless of the medium on which it is stored or the form in which it is made available, personal information is information:

- that relates to an individual ;
- and that can be used to identify that individual (directly or indirectly).

Examples of personal information:

- personal address
- email address
- telephone number
- date of birth
- income
- holding assets
- information relating to the investment's risk tolerance of an individual
- information on investments and transactions made by an individual

Information about a company is not personal information, except for information related to individuals associated with the company.

Sensitivity level

of personal information

Some personal information is of greater value to an individual as part of his or her private life.

If he entrusts sensitive personal information to a company, the concerned individual expects the company to treat it with even greater care than his/her other information.

Examples of personal information with a **higher level of sensitivity**:

- medical information
- social insurance number
- bank account details
- credit score

Privacy in Canada

The handling of Canadians' personal information by a **corporation** in the course of its **commercial activities** is governed by federal legislation that applies across the country, except in three provinces, which have their own legislation: Quebec, Alberta and British Columbia.

Each legislation sets up its own regulatory authority

Federal

Office of the Privacy
Commissioner of Canada

Quebec

Commission d'accès à
l'information (« CAI »)

Alberta

Office of the Information and Privacy
Commissioner of Alberta

British Columbia

Office of the Information and Privacy
Commissioner for British Columbia

Their role, within their respective jurisdiction, is to:

- investigate privacy complaints addressed to them,
- carry out company inspections,
- require offending companies to change their practices,
- impose financial penalties for violations of the law.

Privacy

Is a serious matter

In response to Canadians' growing concerns about their privacy, governments are looking to introduce stricter privacy legislation.

As a result, they plan to impose much stricter **penalties** on organizations that fail to meet their obligations to protect personal information.

In **Quebec**, for example, penalties can range up to a maximum of:

- **100 000 \$** against an individual,
- **25 000 000 \$** (or 4% of annual worldwide sales) against a company.

Requirements in Quebec since September 2022

As part of your business activities, you should already have the following key elements in place:

1. Designation of a person in charge of the protection of personal information

The person with the highest authority within the organization acts as the “Privacy Officer” and is responsible for ensuring compliance, but this function may be delegated. This person is responsible for ensuring compliance with and implementation of privacy legislation within the company. This person is also the main point of contact to whom individuals can turn if they wish to obtain information about the personal information the company holds on them. His or her contact details should therefore be published on the company's website.

2. Reporting a privacy incident

Unauthorized access, use, disclosure, loss of personal information is considered a privacy incident and must be recorded in a company register. When the incident poses a risk of serious harm, it will be required to notify the CAI and any individual affected by the incident. When the affected individual is a client of [name of the concerned iAFG entity], you must notify [name of the concerned iAFG entity] without delay in any circumstances.

3. Disclosure of biometric databases

The collection of biometric data (e.g. voice, fingerprint, facial) requires the express consent of the individuals concerned. If you wish to use individuals' biometric data in your activities, you must notify CAI in advance.

Requirements in Quebec for September 2023

Here are the key elements **to implement**

Adoption of policies and practices regarding personal information

Clear governance and privacy policies and practices, including data retention and destruction, and a complaints handling process are required. These policies must be clearly published on the organization's website, and adapted to its activities. To learn more about iA Financial Group's policies and practices, consult our Privacy Notice at ia.ca Privacy section.

Privacy Impact Assessment (PIA)

Organizations will be required to conduct a PIA prior to the acquisition, development or redesign of an information system or electronic service delivery project involving the collection, use, disclosure, retention or destruction of personal information or before communicating such information outside the province. The purpose of this measure is to ensure that privacy concepts are taken into account before undertaking any activity that may affect an individual's privacy.

Transparency and obligation to inform prior to consent

Obligation to provide clear and simple information at the time of collection of personal information, in particular on the purposes, means of collection, the possibility of any disclosure of personal information outside the province and the rights of access and rectification.

New individual rights

Individuals can request the destruction of personal information held on them by a company, and if the company is no longer justified in retaining it, it must grant this right and, above all, provide individuals with proof that the destruction has indeed taken place.

Any company making decisions based exclusively on the automated processing of personal information must inform the concerned individuals and give them the right to know more.

To come in September 2024 – Right to data portability

The background is a solid blue color. Overlaid on this are numerous small, white, stylized human figures in various poses, scattered across the frame. In the lower right quadrant, there is a large, white, concentric circular pattern resembling a fingerprint or a ripple in water.

Privacy good practices to adopt at all times

Inform your clients



- Your potential or existing clients need to understand **what you want to do** with their personal information (PI), why you collect it and intend to use it, and with whom you may share it.
- **Be prepared to explain** the purposes for which it is collected, to whom it will be disclosed and why.
- **Understand the rights** your clients have towards their personal information (right to access it, to rectify it, to ask for it to be destroyed, to have more information about its management) so that you can inform them about those and respond to their requests, if necessary.

Have a **reference document** on hand, such as iA Financial Group's Privacy Notice ([link](#)) will allow you to provide answers to your clients' questions.

Obtain consent



- Make sure you obtain **all the necessary consents** for the use and disclosure of your clients' personal information that you intend to make.
- **Investia/iAPW** includes consent as part of the account opening process, and you must ensure that all clients are aware of this. However, you may need **additional consent**, depending on the services you offer your clients, for other activities not related to **Investia/iAPW**, such as estate planning or insurance activities.
- Clients can always **withdraw their consent**. However, if the client ever withdraws his/her consent for purposes necessary to provide your service, this may mean that you will no longer be able to maintain your relationship with him/her.

Limiting the collection, use and communication of PI



- Before collecting personal information, take the time to **validate whether you really need it** to provide your service.
- **Limit the use** of your clients' personal information to what is necessary or to activities for which your clients have specifically consented.
 - They may have withdrawn their consent, so always validate the status of their consent at the time of use.
- Disclose personal information to third parties (e.g. partners, service providers) only when it is **truly necessary for your activities** and when required, only if you have your client's consent.
 - Don't forget that it is often necessary to draw up a **written contract with this third party**, including specific clauses, before disclosing such information.

Keeping PI only as long as necessary



- Determine in advance how long you will keep your clients' personal information.
 - A schedule defining the applicable retention periods according to the nature of the personal information and the context in which it is used is an essential tool.
- Identify where you will keep this PI, in which system(s), and keep unnecessary copies to a minimum (e.g. e-mails).
- These practices help limit the likelihood of a data breach and the consequences it could have on you and your clients.

Protecting PI



Implement controls and security measures to ensure that the personal information entrusted to you is protected at all times.

- To do this, make sure you manage the access your employees may have to your clients' personal information, and limit it to what is strictly necessary.
- It is also essential to provide your employees with training on good privacy practices, so that they adopt them.
- Refer to the Cybersecurity Best Practices Guide for other practices you can adopt to protect, among other things, the personal information under your responsibility.



Useful links for all types of businesses

Useful links for all types of businesses

1. **Government of Quebec (french only)**

[Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, Entreprises \(quebec.ca\)](#)

2. **Commission de l'accès à l'information (CAI)**

https://www.cai.gouv.qc.ca/documents/CAI_FI_New_Obligations_Businesses.pdf

3. **Gouvernement of Canada: Summary of privacy laws**

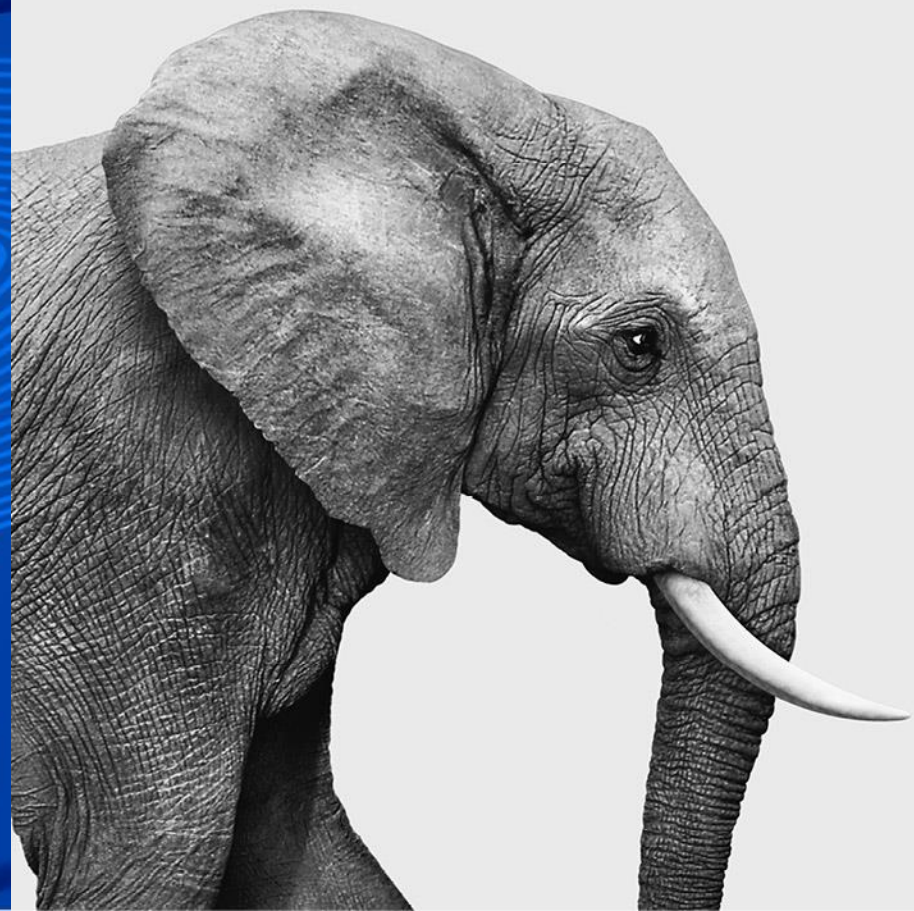
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

4. **[Québec Privacy Law Reform: A Compliance Guide for Organizations](#), BLG**

5. **CyberEco** : [Data protection - Cybereco](#)

6. **Training providers:**

- o [Get Cyber Safe \(getcybersafe.gc.ca\)](#)
- o [Security Awareness | Terranova Security](#)
- o Serene risc : [cybersec 101](#)



ON S'INVESTIT, POUR VOUS.
INVESTED IN YOU.