


Appendix – Third Party Management

What to do when transferring personal information to a service provider / third party?

Simply mentioning a service provider's commitment to comply with legal obligations regarding the protection of personal information in a contract is not sufficient to comply with the requirements of Bill 25.


As of September 22, 2023,  it will be necessary to sign a written agreement that includes:

- a description of the measures taken by the service provider to protect the confidentiality of personal information;
- an obligation on the part of the service provider to use personal information only for the purposes of providing the services, and not to retain such personal information after the contract has expired;
- the obligation of the service provider to promptly inform the person responsible for the protection of personal information of any breach or attempted breach of an obligation relating to the confidentiality of personal information;
- the obligation to allow your organization's Privacy Officer to carry out any audit relating to confidentiality requirements.

Appendix – Third Party Management

Key Actions



- Draw up a list of service providers to whom the organization communicates or gives access to personal information. 
- Review existing contracts to identify whether the required elements are present or whether adjustments need to be made.
- Prepare a privacy checklist when using a new service provider.
- Draw up a privacy schedule setting out the elements required by law to be signed by all your service providers who will be handling personal information.

Appendix – Third Party Management

Reminder



Transfers outside Quebec

If personal information is transferred outside Quebec on or after 22 September 2023, a privacy impact assessment (PIA) must be carried out prior to the transfer to determine whether the personal information will be adequately protected in accordance with generally accepted privacy principles.

The PIA will need to take into account:

- the sensitivity of the personal information
- the purposes for which it is to be used
- safeguards (including contractual safeguards);
- the legal regime applicable in the receiving State, in particular the applicable principles for the protection of personal information.

The disclosure of personal information, which also includes simple access granted to personal information, will be subject to a written agreement that considers the results of the PIA and the terms and conditions agreed to in order to mitigate the risks identified by the PIA (if applicable).



cyber eco