



## **Neolegal Inc. Privacy Policy**

This policy is designed to comply with the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. As part of the services provided by Neolegal Inc. we are required to collect personal information from our Clients and we are committed to protecting that information.

Neolegal Inc. agrees to act on behalf of the Customer exclusively for the purpose of providing Services previously limited by the specific program (package) purchased.

Neolegal Inc. declares that it is bound on behalf of itself and its lawyers by the *Code of Professional Conduct of Lawyers*, the rules of the Barreau du Québec, and by all other laws or regulations that apply to the present contractual relationship.

Neolegal Inc., on behalf of itself and its representatives, undertakes to act loyally and transparently, in the interest of its Clients and in accordance with the customs and practices of the legal profession.

In case of subscription to a Service, Neolegal Inc. will keep the Client's file according to its internal rules and in accordance with the laws in place, as well as all the information transmitted, on its servers as used internally throughout the contractual relationship between the Parties.

Neolegal Inc. is committed to seeking express consent for the collection of all personal information from Customers. All information thus obtained will not be used or communicated without said express consent of the Customers.

Neolegal Inc. will not hold or request any original documents from the Customer. The Client is responsible for all original documents that make up his/her legal file.

Neolegal Inc. is committed to respecting the privacy and confidentiality of all Client information. All conversations between the Client and a Neolegal Inc. representative may be recorded for quality control purposes and to comply with the Code of Ethics for Lawyers. The conversations are kept in a highly secure manner and only authorized Neolegal Inc. personnel can access them.

Neolegal Inc. does not keep any information related to the payment of its customers, nor the data necessary for the purchase. This data is encrypted and destroyed after use according to the standards set forth in this regard.

Neolegal Inc. also ensures that its payment providers meet the highest industry standards.

Neolegal Inc. is required to collect personal information for client identification purposes pursuant to section 14 of the Regulation respecting the accounting and professional practice standards for lawyers. The information collected also allows Neolegal Inc. to ensure, among other things, that there is no conflict of interest or appearance of conflict of interest.

### **General processes and data anonymization**

The person responsible for the protection of personal information within Neolegal is the current VP, Legal. Me Catherine Fugère-Lamarre assumes this role and holds, supported by the cybersecurity committee, including Mr. Sid Benachenhou, as CTO, the responsibilities related to it.

Her contact information is as follows:

Email: confidentialite@neolegal.ca  
Address: 420 Notre-Dame Street West, Suite 601  
H2Y 1V3  
Telephone: 514-390-0367

The data concerning the personal information of the Clients is secured by logins and a two-factor authentication. This data is stored in Canada.

Backups are done daily, and a simulation exercise schedule is established.

Cybersecurity training is offered to all Neolegal Inc. employees on a regular basis.

An internal audit schedule is also established to regularly analyze the processes and procedures in place.

In accordance with sections 9 and 18 in fine of the *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*, Neolegal is required to keep client files for a period of 7 years after the closing of the client's account.

After this period, the data is encrypted and anonymized in accordance with the standards set out in the Act.

After the closure of a file and for the duration of 7 years, personal information is accessible only by authorized persons. The same applies to open files.

### **Formation of a Cyber Security Committee**

To ensure that this policy is maintained and respected, a committee made up of the CTO, CLO, and the person responsible for finances was set up as soon as this policy was adopted.

This committee has the task of analyzing requests for information, complaints, and analyzing all cybersecurity processes and data retention.

The committee will meet on a quarterly basis.

This committee will also be responsible for the overall risk assessment of each IT project.

## **Process for inquiries or complaints**

If the Client wishes to obtain information related to this policy, he/she may do so at the following address: [confidentialite@neolegal.ca](mailto:confidentialite@neolegal.ca) or [privacy@neolegal.ca](mailto:privacy@neolegal.ca)

If the Client wishes to report a privacy incident or complaint, he/she should take the following steps:

- a. Write to: [confidentialite@neolegal.ca](mailto:confidentialite@neolegal.ca) or [privacy@neolegal.ca](mailto:privacy@neolegal.ca)
- b. Write the reason and nature of the complaint;
- c. The committee will conduct an analysis of the complaint or incident;
- d. Upon receipt of the complaint, time limits will be stipulated to properly process the information;
- e. The complainant will be notified of the progress of the case and if additional information is required, a request will be made;
- f. Upon decision of the committee, a response will be sent to the complainant;
- g. If the complaint is justified, clear and specific actions shall be taken as soon as possible, and the complainant shall be notified of such actions;
- h. If the complaint is not justified, a response will also be sent to the complainant and the file will be closed;
- i. If a privacy/security incident has occurred, the disclosure process to the appropriate authorities and stakeholders will be implemented and followed.

## **Employee Access to Personal Information of Neolegal Inc.**

Only authorized employees at each stage of the mandate have access to the Client's file.

All employees of Neolegal Inc. are bound by solicitor-client privilege and may not divulge in any way whatsoever the information they receive.

No personal information may be handwritten and if so, the employee shall ensure that the information so written is properly destroyed.

The process established during a security incident.

In the event of a security incident involving personal information, the following steps will be followed:

- a. The Committee will meet to understand the situation;
- b. The CTO will implement technological actions to quickly rectify the situation according to the nature of the incident;
- c. An assessment will be done to know who has been affected, as well as the risks to the company and the risks of recurrence;
- d. CLO will advise the *commission d'accès à l'information*;
- e. A plan will be made to notify affected customers, partners, employees, Board of Directors, shareholders, and all officers as required;
- f. An audit will be conducted afterwards to ensure that customer data is properly protected from the aftermath of the incident.

Information that the incident log must contain:

- a. Date of the incident;
- b. Name of all the persons affected and their relationship with Neolegal inc.;
- c. Nature of the incident;
- d. Impact of the incident (i.e., risk assessment);
- e. Communication strategy to those involved (see list in previous point);
- f. Actions to be taken and taken to resolve the incident;
- g. Actions to be taken to prevent this type of incident in the future and the implementation of adequate and sustainable solutions.

The *Commission d'accès à l'information* will also need to be made aware of any risks as well as incidents that have occurred and if the potential for an incident creates serious risks.

### **Security of personal information with our partners**

Neolegal Inc. during its business deals with various partners, including, but not limited to, service providers, legal service contractors and business partners in general, who may be involved in various sectors, such as, but not limited to, the legal, insurance and other sectors.

Neolegal Inc. ensures that each Partner complies with the highest industry standards, as well as all standards and policies set forth in the *Privacy Act*.

All transfers of personal information to business partners shall be done in a secure manner, in consultation with the Technology Department and the CTO.

All personal information of customers will not be transferred to a business partner without the express consent of the customer and will only be transferred under the terms and conditions previously established.

Neolegal Inc. ensures that transfers of personal information are done in a secure manner using information technology.