



TECHNI 1
CONTACT



Privacy Policy



Table of Contents

Table of Contents.....	1
Foreward.....	2
1. Objectives.....	2
2. Personal Information.....	2
3. Collection.....	3
4. Usage.....	3
5. Communication.....	3
6. Conservation.....	3
7. Destruction.....	4
8. Privacy Impact Assessment.....	4
9. Request For Access Or Modification.....	5
10. Confidentiality Incidents.....	5
11. Privacy Complaint Handling Process.....	6
12. Privacy Officer Contact Details.....	6
13. Effective Date Of The Policy.....	6
Appendix 1 – Privacy Policy For The Collection Of Personal Information By Technological Means.....	6
Appendix 2 – Digitization Procedure.....	8
Appendix 3 – Confidentiality Incident Registry.....	9
Appendix 4 – Procedure For Handling Complaints Related To The Protection Of Personal Information.....	10

Foreward

The Privacy Policy (hereinafter referred to as the "Policy") is adopted pursuant to the Act respecting the protection of personal information in the private sector, c. P-39.1 (hereinafter referred to as the "Private Sector Act").

Techni-Contact Canada Ltd. and AMX Canada Ltd. (hereinafter referred to as "the Companies") are for-profit legal entities that process personal information in the course of their activities. They are therefore subject to the Privacy Act.

In the course of its activities, the Companies must collect, use and retain personal information.

This Policy applies to the companies, which includes, in particular, the members of its personnel, its officers, as well as any person who otherwise provides services on behalf of the companies.

It applies to all personal information collected, used and retained by the companies, regardless of its form. The Policy covers personal information contained in all types of physical or digital documents, in the broadest sense, whether in written, graphic, sound, visual, computerized or other form. Personal information is defined as any information concerning a natural person that allows that person to be identified directly or indirectly.

The APPENDICES form an integral part of the Policy. It is given to current and new employees to read when they are hired.

1. Objectives

This Policy describes the standards for the collection, use, communication, retention and destruction of personal information in order to ensure its protection. It also explains the roles and responsibilities of company personnel throughout the information life cycle, and a process for handling complaints about the protection of personal information.

2. Personal Information

In the course of its activities, the companies may collect and process various types of personal information, including:

For personnel :

- identity information, such as first or last name, age, date of birth, social insurance number; bank account information for pre-authorized debits, etc;
- Contact information, including address, e-mail address and telephone number, as well as emergency contact information;
- information relating to the staffing and hiring process, resumes, personnel files, training certificates, proof of qualifications, interview notes,
- information contained in documents from related authorities such as CNESST, credit files, criminal records, etc.
- any other personal information required for its activities.

3. Collection

Companies collect personal information primarily from current and future employees through its hiring process.

Companies collect personal information directly from the individual concerned and with his or her consent, unless an exception is provided for by law.

Consent may be implied in certain situations, such as when an individual voluntarily provides his or her personal information as part of a hiring process.

In all cases, companies only collect personal information if they have a valid reason to do so. Moreover, collection is limited to the information needed to fulfill the intended purpose.

Unless an exception is provided for by law, companies seek the consent of the person concerned before collecting personal information about him or her from a third party.

Considering that the companies collect personal information by technological means, they have adopted a Privacy Policy for the collection of personal information by technological means, available in APPENDIX 1.

4. Usage

The company undertakes to use personal information in its possession only for the purposes for which it was collected and for which it is authorized by law to use it. It may, however, collect, use or disclose such information without the consent of the individual concerned, where permitted or required by law.

In certain circumstances, companies may collect, use or disclose personal information without the knowledge or consent of the individual concerned. Such circumstances include where, for legal, medical or security reasons, it is impossible or unlikely to obtain consent, where such use is clearly for the benefit of the individual concerned, where it is necessary to prevent or detect fraud, or for any other serious reason.

Companies restrict access by employees and officers to personal information and knowledge of a personal nature that is necessary for the performance of their duties.

5. Communication

In general, companies may not disclose personal information about an individual without that individual's consent.

However, companies may disclose personal information to a third party without the consent of the individual concerned when required to do so by law or regulation, or when permitted by the Privacy Act or any other law.

6. Conservation

Conservation

In the course of their activities, corporations must keep numerous documents containing personal information.

Certain documents must be kept for a period prescribed by the Taxation Act or any other authority governing the corporation.

Quality Of Personal Information

The companies ensure the quality of the personal information they hold. In this sense, the personal information kept is up-to-date, accurate and complete, and serves the purposes for which it was collected or used.

Constant updating of personal information is not required, unless justified by the purposes for which the information is collected. However, if the information is to be used to make a decision, it must be up to date at that time.

Physical And Digital Documents

Depending on the nature of the personal information, it may be held at the offices of the Companies, in various computer systems of the Companies or its service providers, or in storage facilities of the Companies or its service providers.

Safety Measures

The security and protection of personal information is important to us, and we implement security measures to ensure that personal information remains strictly confidential and is protected against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

These security measures may include organizational measures such as the use of locked filing cabinets, access to which is restricted to the personnel concerned and to what is necessary, access to locked offices, reminders of procedures relating to confidentiality and the protection of personal information at team meetings, the use of security procedures and various registers (hiring procedures, register of staff awareness of the Policy, register of confidentiality incidents, etc.), the use of a shredder or any other practices deemed necessary to protect personal data. For practices concerning the protection of computerized information, see Appendix 1 - Privacy policy for the collection of personal information by technological means.

7. Destruction

Original documents containing personal or confidential information are securely destroyed.

Companies use document destruction techniques adapted to the level of confidentiality of the document to be destroyed.

8. Privacy Impact Assessment

Companies must conduct a Privacy Impact Assessment (PIA) for all new projects involving the collection and/or use of personal information, the development and redesign of information systems, or the electronic delivery of services involving personal information.

The Privacy Impact Assessment carried out must be proportionate to the sensitivity of the information concerned, the purpose of its use, its quantity, distribution and medium.

Companies can use the guide developed by the Commission d'accès à l'information ["Act respecting the protection of personal information in the private sector"](#) to carry out a privacy impact assessment, where appropriate..

9. Request For Access Or Modification

Any person may request access to or correction of personal information held by the companies. Subject to certain legal restrictions, individuals may request access to and correction of their personal information held by the companies if it is inaccurate, incomplete or ambiguous.

For corrections, please contact the companies' Privacy Officer, who will respond in writing to such requests within 30 days of receipt.

10. Confidentiality Incidents

Confidentiality Incidents

A confidentiality incident is any unauthorized access, use or disclosure of personal information, as well as its loss or any other form of breach of its protection.

When we have reason to believe that a confidentiality incident involving personal information in our possession has occurred, we take reasonable steps to minimize the risk of harm and to prevent similar incidents in the future.

In the event of a confidentiality incident, the companies assess the damage caused. This assessment takes into account: the sensitivity of the personal information concerned; the possible malicious uses of the information and the apprehended consequences of the use of the information; and the likelihood of the information being used for harmful purposes.

When the incident poses a risk of serious harm to the persons whose information is involved, the companies notify in writing:

- The 'Commission d'accès à l'information' via the [formulaire d'avis](#) (available in French only) ;
- The person(s) concerned. The notice must provide adequate information on the scope and consequences of the incident.
- The notice must contain:
 - A description of the personal information involved in the incident. If this information is not known, the organization must provide the reason why this description cannot be provided.
 - A brief description of the circumstances of the incident;
 - The date or period when the incident took place, or an approximation of this period if not known;
 - A brief description of the measures taken or proposed to reduce the risk of harm being caused as a result of the incident;
 - Measures proposed to the person concerned to reduce the risk of harm being caused or to mitigate it;
 - The contact details of a person or department that the person concerned can contact to obtain further information about the incident.

Confidentiality Incidents Registry

Companies shall keep a registry of confidentiality incidents as provided for in APPENDIX 3.

The registry records all confidentiality incidents involving personal information, both those presenting a risk of serious harm and those not presenting a risk of serious harm.

The information contained in the registry of confidentiality incidents is kept up to date and retained for a minimum period of five (5) years after the date or period during which the companies became aware of the incident.

11. Privacy Complaint Handling Process

Any person concerned by the application of this Policy may lodge a complaint concerning its application or, more generally, concerning the protection of his or her personal information by the companies.

The procedure for handling complaints relating to the protection of personal information is set out in APPENDIX 4.

12. Privacy Officer Contact Details

Julien Surprenant, Corporate Privacy Officer, can be reached by telephone at 514-695-4883 ext. 232. He may be contacted for any questions relating to the application of this Policy.

13. Effective Date Of The Policy

The Policy takes effect on September 23, 2023.

The Policy has been approved by the Privacy Officer.

In the event of any change to this Policy, the Companies will make the Policy available as amended.

Appendix 1 – Privacy Policy For The Collection Of Personal Information By Technological Means

The companies are committed to ensuring the protection and confidentiality of the personal information you provide or that we collect when you interact with us by technological means. In this respect, this privacy policy (hereinafter the "Policy") is intended to inform you of the personal information collected, the purposes for which it is collected, the communications that may be made and, in general, the safeguards in place.

The Privacy Policy is adopted pursuant to section 8.2 of the [Act respecting the protection of personal information in the private sector](#), c. P-39.1 (hereinafter the "Private Sector Act").


Consent

With the exception of personal information required by law, the decision whether or not to provide us with your personal information rests solely with you. As a general rule, you can communicate with us without having to provide it.

If you use our services or submit your personal information to the companies, you will be deemed to have given your consent for the following purposes, for which the companies collect and use your personal information.

Information Sharing and Communication

Generally, companies cannot share your personal information with other organizations without your consent. We may disclose your personal information without your consent if we are



required or permitted to do so by law, but in such cases we will provide only the information that is required.

Storage and Security

All personal information you provide to the companies is stored and archived on secure servers with restricted access. Furthermore, in partnership with external consultant Exosource, the companies take various technical means to ensure a secure environment and to protect your personal information, including using firewalls and anti-virus software, managing access, using multi-factor authentication (MFA) processes, using automatic locking, making regular back-ups, using secure passwords, using a secure document sharing system and following strict procedures. In addition, the company works continuously with its IT consultant to optimize and perfect its security mechanisms.

However, given the nature of the internet as a public network, you acknowledge and accept that the security of Internet transmissions cannot be guaranteed. Consequently, the companies cannot guarantee or assume any responsibility for any breach of confidentiality, hacking, virus, loss or alteration of data transmitted via the internet.

Document Digitization

The company chooses a medium or technology on which to store its documents, as well as procedures that enable it to comply with the following conditions:

1. The information contained in digitized documents has not been altered and has been maintained in its entirety;
2. The digitization process and the medium used to store the digitized documents must ensure the stability and durability of the documents.

When companies carry out digitization, they apply the procedures set out in APPENDIX 2.

Retention

The Companies use and retain your personal information only as long as necessary to fulfill the purposes for which it was collected, or as permitted or required by law.

The companies reserve the right to retain, for a reasonable period of time, certain personal information in order to comply with the law, prevent fraud, resolve a claim or certain other related issues, cooperate in an investigation and for any other purpose permitted by law. At the end of this period, your personal information is removed from the servers of the companies.

External Links

This Policy does not apply to third-party websites that may be accessed by clicking on links, and the Companies are not responsible in any way for third-party websites. The companies make no representations whatsoever about any other site which you may access through our communications. If you follow a link to a third-party Web site, that Web site will have its own privacy policies that you should review before submitting any requested personal information.

In addition, a link to such a site does not mean that the Companies endorse the third-party site or assume any responsibility for its content or use. It is up to you to take precautions to ensure that whatever you select for your use is free of such items as viruses and other items of a destructive nature.



Additional Information

For any information request or update concerning your personal information, please call Julien Surprenant, Privacy Officer, at 514-695-4883 ext. 232.

Modifications

The Companies reserve the right to modify this Privacy Policy at their discretion. The companies will make available any changes to this Privacy Policy.

Appendix 2 – Digitization Procedure

The person responsible for digitization:

1. Performs physical preparation of documents to be scanned (removes paper clips and staples);
2. Scans the documents and remains present throughout the process to protect the integrity of the scanned data;
3. Performs an exhaustive verification of scanned documents to ensure quantity, quality and integrity of reproduced documents. It verifies that :
 - the digitized documents conform to the source documents;
 - data is legible and of good quality (without loss of detail or information);
 - duplexing has been carried out, if necessary; if the duplexing option has left blank pages, it eliminates them;
 - documents or pages have been scanned in the right direction.
4. Checks that the number of documents or pages is correct (if pages are missing, it resumes the entire scan);
5. Renames PDF files according to company naming convention;
6. Saves the PDF file(s) in the appropriate company software.

Appendix 3 – Confidentiality Incident Registry

Confidentiality Incident Registry								
Date or period of incident	Incident awareness	Number of people affected by the incident	Persons concerned (compromised information)	Description of incident	Description of risks of damage	Date notice sent to 'Commission d'accès à l'information'	Date notices sent to persons concerned	Description of measures taken



Appendix 4 – Procedure For Handling Complaints Related To The Protection Of Personal Information

Reception of Complaint

Any person wishing to make a complaint concerning the application of this policy or, more generally, the protection of his or her personal information by the Companies, must do so in writing to the Companies' Privacy Officer.

The individual must provide his or her name, contact information, including a telephone number, as well as the subject and reasons for the complaint, giving sufficient details to allow the complaint to be evaluated. If the complaint is not specific enough, the Privacy Officer may request any additional information he or she deems necessary to assess the complaint.

Complaint Handling Procedure

The companies undertake to treat all complaints received confidentially.

An assessment is made to determine whether the companies' handling of personal information complies with the Policy, with the practices in place within the organization and with applicable legislation or regulations.

Complaints are dealt with within a reasonable timeframe. The Privacy Officer shall assess the complaint and issue a written response to the complainant.

Complaints File

Companies are required to maintain a separate file for each complaint received under this Complaint Handling Procedure. Each file contains the complaint, the analysis and documentation supporting its evaluation, as well as the written response sent to the complainant.