ELEM
UNITING THE ELEMENTS

Privacy Policy

Personal information governance practices

(Article 3.2 of the *Act respecting the protection of personal information in the private sector*, Chapter P-39.1, and *Regulation respecting confidentiality incidents*, A-2.1. r. 3.1)

1. APPLICATION AND INTERPRETATION OF THE POLICY

1.1 Preamble

Your personal information plays an important role in some of our business processes and in fulfilling the mission entrusted to us. Your satisfaction and the respect for your privacy guide our daily activities. ELEM Group, and its affiliated companies: Ondel, Talvi, Descimco, Industro-Tech, Opting, Quantech, Qualifab, and AKT (hereinafter collectively referred to as "ELEM"), are responsible for protecting the personal information they hold. Personal information is confidential, except as provided by law. Any individual who, in the course of their duties, has access to personal information held by ELEM must take necessary measures to ensure its protection and confidentiality.

This policy (hereinafter the "Policy") considers the requirements of the *Act respecting the protection of personal information in the private sector* (hereinafter the "Act") and any other applicable laws or regulations. It aims to inform you about the practices in place regarding personal or otherwise confidential information. It also outlines the measures to be taken to reduce the risks of harm in such cases and prevent further incidents of a similar nature.

Any changes to the Policy will be communicated on our website, so we invite you to regularly check it for the latest rules we apply regarding the protection of personal information.

If you have any questions regarding this Policy, you can contact our Personal information protection officer - *Responsable de la protection des renseignements personnels* (hereinafter "RPRP"), whose contact information is provided in Section 3.3 of this document.

1.2 Objective and Normative Framework

The Policy governs how ELEM handles all personal information in its possession, regardless of the nature of its medium and the form in which it is accessible: written, graphic, audio, visual, computerized, or otherwise. However, the Policy does not apply to personal information that is deemed public under the Law.

It also specifies the steps to be taken when ELEM has reasonable grounds to believe that a confidentiality incident involving personal information it holds has occurred or if such an incident is confirmed, in accordance with the Law and the Regulation on confidentiality Incidents.

1.3 Definitions

The definitions to be considered for the application of the Policy, which may be supplemented by any other regulation policy, directive, or procedure referring to them, are as follows:

Personal Information: any information that pertains to an individual and allows for its identification. The name of a person, by itself, is not personal information. However, when the name is associated or linked with other information regarding the same person, it then becomes personal information.

Here are examples of personal information:

- The name of a person and its date of birth.
- Social insurance number.
- Credit card number.
- Health insurance number.
- Medical or financial information.
- The name of a person and its personal phone number.
- The name of a person and its home address.

Sensitive Personal Information: personal information is considered sensitive when, due to its nature such as medical, biometric (e.g., fingerprint, voice or facial recognition) or otherwise intimate, or due to the context of its use or communication, it creates a high degree of reasonable expectation of privacy.

This can include, for example, medical, biometric, genetic, or financial information, as well as information about ethnic origin, political beliefs, life or sexual orientation, and religious convictions.

Confidentiality Incident: unauthorized access, use, disclosure of personal information as defined by the Law, as well as its loss or any other form of failure to protect it.

Here are some examples:

- A staff member accesses personal information that is not necessary for its duties.
- A person uses personal information from a database it has access to as part of its duties to impersonate someone's identity.
- Communication is mistakenly sent to the wrong person.
- A person loses or has documents containing personal information stolen.
- Someone intrudes into a database containing personal information to alter it.
- A hacker infiltrates a system.

2. MANAGEMENT OF PERSONAL INFORMATION DURING ITS LIFECYCLE

2.1 Collection and Use

We primarily collect your personal information directly from you, especially when you communicate with us, whether through our website, as part of a contract or recruitment process, among others.

We only collect personal information that is necessary for carrying out our tasks, including:

- Communicating with you.
- Processing job applications for positions we advertise.
- Complying with legal and regulatory obligations imposed on us as a company.
- Ensuring the ongoing security, efficiency, and quality of our business processes and website.
- Ensuring the protection of individuals and property within our facilities.

When we ask for your personal information, unless it is explicitly stated in the context, we will inform you if you are required or not to provide this information. Not providing certain personal information may result in a refusal of the requested service.

Unless an exception provided by the Law applies, we seek your consent or refusal, in writing or verbally, in the cases specified by the Law, namely:

- When we wish to collect your personal information, but you are not obligated to provide it;
- When we wish to use your personal information for purposes other than those for which it was initially collected, and you are not obligated to accept.
- When we disclose your personal information to a third party that requests access to it.

In case of refusal to consent, we will explain the consequences thereof. On the other hand, we will inform you of how you can withdraw your consent if you change your mind and explain the consequences of such a decision.

Finally, for you to give your informed consent, we will provide you in advance, in a transparent, clear, and concise manner, with the information you need to make an informed decision.

2.2 Communication

ELEM does not disclose your information without your consent, unless authorized under the exceptions provided by the Law.

As part of our activities, we may sometimes need to disclose your personal information to regulatory authorities, government departments, and agencies that request it under powers granted to them by the Law or when such information is necessary for law enforcement. They may also be used for statistical purposes, studies, surveys, investigations, or verification.

2.3 Retention and Destruction

Most of the information we collect is stored within our premises.

We retain your personal information for as long as we use it to conduct our activities and provide you with services. Once the purposes for which confidential information has been collected or used are achieved, we destroy it following an additional retention period prescribed by the retention rules we have adopted and as required by applicable legislation.

This additional period is intended to allow us to fulfill certain legal or regulatory requirements or to produce such information as evidence in the event of a claim or legal action.

3. OUR RESPONSIBILITIES

3.1 Security

ELEM implements appropriate and reasonable security measures to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification as defined by the Law.

All your personal information is treated confidentially. Only staff members who absolutely need access to personal information within the scope of their duties are authorized to do so.

Security software, policies, administrative directives, and awareness and training activities for staff ensure the confidentiality of your information throughout its lifecycle (collection, use, disclosure, retention, and destruction).

The security measures we take fall into three main categories:

- Technological security measures (e.g., firewalls, management of information access privileges, encryption of information).
- Physical security measures (e.g., locking of filing cabinets, access restrictions to premises).
- Organizational security measures (e.g., policies, procedures, information security training and awareness, reliability and integrity checks).

ELEM staff members or those working on behalf of ELEM are informed about the existence of the Policy and must periodically consult it. Furthermore, we have implemented measures to raise awareness among our staff about the important role they play in protecting your privacy. Therefore, ELEM staff members must, among other things:

- Make reasonable efforts to minimize the risk of unintentional disclosure of personal information.
- Take special precautions to ensure that personal information is not monitored, heard, accessed, or lost when working in locations other than ELEM's offices.

- Take reasonable measures to protect personal information when moving from one place to another.

3.2 Reporting a confidentiality incident

Any individual to whom ELEM discloses personal information (management, colleagues, clients, suppliers, subcontractors, partners, and experts) must report when they have a reasonable belief that a confidentiality incident involving personal information they hold has occurred. To do so, this report must be made promptly to the person responsible for the protection of personal information.

An ELEM staff member who has a reasonable belief that a confidentiality incident involving personal information they hold has occurred must also immediately notify their supervisor or the person responsible for the protection of personal information (the contact information can be found in the following section of this document).

3.3 Personal information protection officer - Responsable de la protection des renseignements personnels ("RPRP")

The RPRP for ELEM is Ms. Megan Pajonkowski. She can be reached using the following contact information:

Email: rprp@elem.global
Phone: 1-418-664-1177 ext. 355

Her role includes:

- - Contributing to the implementation of the information security incident management process.
- - Maintaining the register of confidentiality incidents that may have compromised information security, documenting these incidents, and keeping the management of ELEM informed.
- - Contributing to information security risk assessments to identify threats and vulnerability situations and implementing appropriate solutions.

In the event of a confidentiality incident, the RPRP takes charge of handling the incident and collaborates with any other relevant individuals based on the nature of the incident.

As such, the RPRP:

- Assesses the risk of harm and determines its severity. During this assessment, factors such as the sensitivity of the affected information, anticipated consequences of its use, and the likelihood of it being used for harmful purposes are considered.

- Promptly notifies the individual whose personal information is involved in the incident when there is a risk of serious harm, except when it may impede an investigation conducted by a person or an organization responsible, under the Law, for preventing, detecting, or suppressing crime or offenses. This notice must include the following information:

  a) A description of the personal information involved in the incident or, if this information is not known, the reason why such a description cannot be provided.
  b) A brief description of the circumstances of the incident.
  c) The date or period when the incident occurred or, if not known, an approximation of the period.
  d) A brief description of the measures ELEM has taken or intends to take following the incident to reduce the risk of harm.
  e) Measures suggested by ELEM to the individual concerned to reduce the risk of harm or mitigate such harm.
  f) Contact information enabling the individual concerned to obtain further information regarding the incident.

- Notifies any person or organization that could mitigate the risk, providing only the necessary personal information for that purpose, without the consent of the individual concerned.

- Promptly notifies, in writing, the Commission d'accès à l'information of the confidentiality incident when there is a risk of serious harm. The notice must include the following information:

  a) The name of ELEM and the Quebec enterprise number assigned to it under the *Act respecting the legal publicity of entreprises.*
  b) The name and contact information of the relevant person within ELEM regarding the incident.
  c) A description of the personal information involved in the incident or, if this information is not known, the reason why such description cannot be provided.
  d) A brief description of the circumstances of the incident and, if known, its cause.
  e) The date or period when the incident occurred or, if not known, an approximation of the period.
  f) The date or period when ELEM became aware of the incident.
  g) The number of individuals affected by the incident, including the number of individuals residing in Quebec, or if not known, an approximation of these numbers.
  h) A description of the elements leading ELEM to conclude that there is a risk of serious harm to the affected individuals, such as the sensitivity of the personal information involved, potential malicious uses of this information, anticipated consequences of its use, and the likelihood of it being used for harmful purposes.
  i) The measures ELEM has taken or intends to take to notify individuals whose personal

information is involved in the incident, including the date when individuals were notified or the estimated timeframe for notification.

j) The measures ELEM has taken or intends to take following the incident, including measures to reduce the risk of harm or mitigate such harm and measures to prevent further incidents of a similar nature, along with the timeframe for implementing these measures or the estimated timeframe.

k) A mention, if applicable, that a person or organization located outside Quebec, exercising similar responsibilities to those of the Commission d'accès à l'information regarding the oversight of personal information protection, has been notified of the incident.

- Promptly notifies the insurers of ELEM, if applicable.
- Records the privacy incident in the designated register.
- Upon request, provides a copy of this register to the Commission d'accès à l'information.

3.5 Register of confidentiality incidents

ELEM maintains a register of confidentiality incidents (hereinafter referred to as the "Register").

The information contained in the Register must be kept up-to-date and retained for a minimum period of five years from the date on which we became aware of the incident.

4. EFFECTIVE DATE AND REVISION

The Policy comes into effect on September 22, 2023, and will be reviewed annually or earlier if legislative or regulatory changes necessitate it.