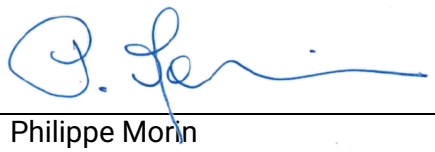
PERSONAL INFORMATION PROTECTION POLICY

Version:	2.2
Date of version:	20-09-2023
Created by:	Data Protection Committee
Approved by:	Philippe Morin, Chief Executive Officer
Confidentiality level:	Public
Internal Codification:	PL-31

Change history:

Date	Version	Created by	Description of change
12-09-21	0.1	Olivier Leclair	Basic document outline
10-27-22	1.0	Olivier Leclair	Beta version
01-16-23	2.0	Olivier Leclair & Marc-Antoine Denis	Release version
03-01-23	2.1	Olivier Leclair	Edits
20-09-23	2.2	Data Protection Committee	Edits

Approval:



Name: Philippe Morin
Title: Chief Executive Officer
Date: 2023-09-20

Table of contents

1. Purpose, Scope and Users

EXFO Inc., on behalf of itself and its affiliates, hereinafter referred to as “EXFO”, strives to comply with applicable laws and regulations related to Personal Information protection in countries where EXFO operates.

This Personal Information protection policy (the “Policy”) has the following objectives:

- Set out the orientations and guiding principles designed to ensure effective protection of personal information ("PPI");

- Protect Personal Information collected by EXFO throughout its life cycle, from collection, use, disclosure, retention to destruction or Anonymization;

- Ensure compliance with applicable legal requirements, including the General Data Protection Regulation, Quebec's Act respecting the protection of personal information in the private sector, and with recognized PPI practices;

- Ensure the trust of all stakeholders and be transparent about EXFO's handling of Personal Information and PPI measures

- Indicate the responsibilities of commercial departments and employees when handling personal information.

The policy applies to all EXFO employees, whether permanent or temporary, including, but not limited to, EXFO personnel, third parties with whom EXFO has a contractual relationship, subcontractors performing functions related to the processing of personal information, and all legal entities or individuals who use or have access to personal information collected by EXFO.

EXFO is responsible for ensuring that all such persons comply with the guiding principles set out in the Policy.

This Policy applies to EXFO and its directly or indirectly controlled wholly-owned subsidiaries.

2. References

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Information and on the free movement of such data, and repealing Directive 95/46/EC)
- LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
- Act respecting the protection of personal information in the private sector, CQLR c P-39.1(“LPDP”)
- Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5)

3. Definitions

Some terms may appear in this Policy that are not defined and any such terms shall be construed in accordance with their typical usage in the private sector of the applicable jurisdiction as of the effective date of this Agreement.

Anonymization: An irreversible process whereby Personal Information can no longer be used to directly or indirectly identify a natural person. Information is said to be "anonymized" when it is reasonable, at all times, to anticipate that it will no longer make it possible, in an irreversible manner, to directly or indirectly identify the person concerned with reasonable means.

Cross-border processing of Personal Information: Processing of Personal Information which takes place in the context of the activities of establishments outside the territorial scope of the applicable law (i.e. outside the EU in the case of GDPR and outside Quebec in the case of LPDP); or processing of Personal Information which takes place in the context of the activities of a single establishment of a local controller or processor but which substantially affects or is likely to substantially affect Data Subjects in more than one territory;

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Information.

Data Processor: A natural or legal person, public authority, agency or any other body which processes Personal Information on behalf of a Data Controller.

Data Protection Committee: An internal EXFO committee which the primary role is to ensure that the organisation processes the Personal Information of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules. The use of the term “Data Protection Committee” may designate the Data Protection Officer, when relevant pursuant to the applicable law.

Data Subject: Any living individual whose Personal Information is collected, held or processed by an organisation. Also refers to the concept of “person concerned” under Quebec law.

Group Undertaking: Any holding company together with its subsidiary.

Lead Supervisory Authority (LSA): The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a Data Subject makes a complaint about the processing of his or her Personal Information; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions of the EU GDPR;

Personal Information: Any information relating to an identified or identifiable natural person (Data Subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: An operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Depersonalization: Depersonalization consists in removing all information that allows direct identification of the person concerned, in particular identifying information. Generally, this information is replaced by a code. Personal Information is depersonalized when it can no longer be used to directly identify the person concerned. De-identified information remains Personal Information, as indirect identification of the person concerned is still possible. The processing of such data must comply with the principles of Personal Information Processing.

PPI Responsible: Person with the highest authority within the company to ensure compliance with and implementation of the Act respecting the protection of personal information in the private sector ("LPDP").

Sensitive Personal Information: Personal Information which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those Personal Information include Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority: An independent public authority which is established by a country, or a Member State pursuant to Article 51 of the EU GDPR;

4. Basic Principles Regarding Personal Information Processing

The Policy reflects EXFO's ongoing commitment to comply with the privacy requirements of the following categories of individuals:

a) current and former EXFO customers
b) Employees and other personnel of EXFO and candidates for employment;
c) Users of the website or users of an EXFO tool or application to the extent that PR is collected;
d) Any other natural person whose personal information is collected or processed in the course of EXFO's activities (e.g. a person invited to an event organized by EXFO);

(collectively the "Data Subject").

EXFO's PPI practices are based on the following guiding principles:

4.1. Lawfulness, Fairness and Transparency

Personal Information must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2. Purpose Limitation

Personal Information must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, subject to exceptions provided for by law or the obtaining of new consent.

4.3. Data Minimization

Personal Information must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. EXFO may apply Anonymization or pseudonymization to Personal Information if possible and commercially relevant to reduce the risks to the Data Subjects concerned, pursuant to its internal policies.

4.4. Accuracy

EXFO aims to ensure that the Personal Information it collects and retains is accurate and carries out validations with Data Subjects to this end as part of its activities. EXFO takes reasonable steps to ensure that Personal Information that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified in a timely manner.

4.5. Storage Period Limitation

EXFO retains data and documents containing Personal Information for the length of time necessary to fulfill the purpose for which they were collected, and the retention periods imposed by law.

When Personal Information is no longer required for the purposes for which it was collected and when the retention periods imposed by law have expired, EXFO must irreversibly destroy or anonymize it. Anonymization must be for serious and legitimate purposes, and the procedure must be reasonably irreversible. The Anonymization procedure must be approved by the Director of Information Security.

4.6. Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of Personal Information risks, EXFO must use appropriate technical or organizational measures to process Personal Information in a manner that ensures appropriate security of Personal Information, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

4.7. Accountability

EXFO, in its capacity as Data Controller, must be responsible for and be able to demonstrate compliance with the principles outlined above.

4.8. Transparency

EXFO documents its Personal Information management practices simply and clearly and makes them available on its websites.

5. Data Protection in Business Activities

Compliance with the principles of data protection requires EXFO to build data protection into its business activities.

5.1. Notification to Data Subjects

(See the Fair Processing Guidelines section.)

5.2. Data Subject's Choice and Consent

(See the Fair Processing Guidelines section.)

5.3. Collection

EXFO must strive to collect the least amount of Personal Information possible. If Personal Information is collected from a third party, the Data Protection Committee must ensure that the Personal Information is collected lawfully.

5.4. Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of Personal Information must be consistent with the information contained in the Privacy Notice. EXFO must maintain the confidentiality, integrity and availability of Personal Information based on the processing purpose. Adequate security mechanisms designed to protect Personal Information must be used to prevent Personal Information from being stolen, misused, or abused, and prevent Personal Information breaches.

5.5. Disclosure to Third Parties

EXFO may disclose Data Subjects' Personal Information to various business partners, suppliers or other third parties in the course of its business, including, but not limited to, the following depending on the Data Subject:

Category of Data Subject	Category of third parties concerned
Employees, other EXFO personnel (including candidates)	• Recruitment firms; • Companies providing evaluation platforms • Specialized due diligence firms • Insurance companies providing group insurance products; • Companies providing recognition platforms; • External auditors; • Financial institutions; • Control authorities (e.g. CNESST, TAT, Canada and Quebec Revenue Agencies, public investigative or enforcement bodies, including criminal prosecution authorities).
Visitor and/or user of the website and its applications	• Advertising service providers (e.g. Google, Meta); • Website hosts; • Analytics platforms (Google Analytics, Hotjar).

Whenever EXFO uses a third-party supplier or business partner to process Personal Information on its behalf, the Data Protection Committee must ensure that this processor will provide security measures to safeguard Personal Information that are appropriate to the associated risks. For this purpose, a Processor Privacy Compliance Questionnaire must be used.

EXFO must contractually require the supplier or business partner to provide the same level of data protection by explicitly specifying responsibilities in the relevant contract or any other legal binding document, such as a Data Processing Agreement. The supplier or business partner must only process Personal Information to carry out its contractual obligations towards EXFO or upon the instructions of EXFO and not for any other purposes.

5.6. Cross-border Transfer of Personal Information

Before transferring Personal Information out of the territories with international or extra-provincial data transfer provisions, adequate safeguards must be used, and, if required, authorization from the relevant Supervisory Authority must be obtained. The entity receiving the Personal Information must comply with the principles of Personal Information processing set forth in the relevant contract or any other legal binding document, as well as in the applicable law.

5.7. Privacy Impact Assessments (“PIA”) - Third parties and transfers outside Quebec

EXFO must conduct a PIA in the following cases:

1) Any project for the acquisition, development or redesign of a technological solution or computer system, including projects for the acquisition and implementation of software solutions and projects for the provision of electronic services involving the collection, use, disclosure, retention or destruction of Personal Information;

2) When Personal Information is transferred to third parties;

3) When Personal Information transferred outside Quebec.

5.8. Rights of Access by Data Subjects

When EXFO is acting as a data controller, the Data Protection Committee is responsible to provide Data Subjects with a reasonable access mechanism to enable them to access their Personal Information, and must allow them to update, rectify, erase, or transmit their Personal Information, if appropriate or required by law.

5.9. Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free, if appropriate or required by law. The Data Protection Committee is responsible to ensure that such requests are processed within reasonable delays, are not excessive and do not affect the rights to Personal Information of other individuals.

5.10. Right to be Forgotten

Upon request, Data Subjects have the right to obtain from EXFO the erasure of its Personal Information, if appropriate or required by law. When EXFO is acting as a Controller, the Data Protection Committee must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

5.11. Automated Processing

EXFO shall inform Data Subjects of any decision-making process that is based exclusively on automated Personal Information Processing (without human intervention), that they are the subject of such a process, of the decision that has been made, and of their right to comment on that decision. EXFO shall, upon request, inform the Data Subject of the following:

- Personal Information used to make this decision;
- Reasons for this decision;
- His right to have the Personal Information used to reach this decision rectified.

5.12. Concerns and complaints

EXFO shall address and respond to questions and complaints that may be raised by Data Subjects with respect to their Personal Information.

Any questions or complaints should be forwarded to the Data Protection Committee for processing and follow-up at the following address: data.privacy@exfo.com.

5.13. Data Protection by Design and by Default

Data protection by design is ultimately an approach that ensures EXFO considers privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

Data protection by default requires EXFO to ensure that it only processes the data that is necessary to achieve its specific purposes. It links to the fundamental data protection principles of data minimisation and purpose limitation.

6. Fair Processing Guidelines

Personal Information must only be processed within parameters explicitly authorised by the Data Protection Committee.

EXFO must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to its Data Protection impact assessment guidelines.

6.1. Notices to Data Subjects

At the time of collection or before collecting Personal Information for any kind of processing activities including but not limited to selling products, services, or marketing activities, the Data Protection Committee is responsible to properly inform Data Subjects of the following:

- the types of Personal Information collected and the purposes of the processing;
- processing methods;
- the Data Subjects' rights with respect to their Personal Information, including the right to withdraw consent to the use and disclosure of their Personal Information, subject to legal or contractual restrictions;
- the retention period;
- potential international data transfers;
- the categories of third parties to whom Personal Information may be shared and EXFO's security measures to protect Personal Information.

This information is provided through Privacy Notice and will differ depending on the processing activity and the categories of Personal Information collected.

6.2. Obtaining Consents

Whenever Personal Information processing is based on the Data Subject's consent, or other lawful grounds, the Data Protection Committee is responsible for retaining a record of such consent. The Data Protection Committee is responsible for providing Data Subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time.

When requests to correct, amend or destroy Personal Information records, the Data Protection Committee must ensure that these requests are handled within a reasonable time frame. Data Protection Committee or the Data Protection Committee must also record the requests and keep a log of these.

Personal Information must only be processed for the purpose for which they were originally collected. In the event that EXFO wants to process collected Personal Information for another purpose, EXFO must seek the consent of its Data Subjects in clear and concise writing. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). The Data Protection Committee is responsible for complying with the rules in this paragraph.

Consent must be manifest, free, informed and given for specific purposes. It must be expressed expressly in the following cases:

- Whether the Sensitive Personal Information collected will be used for a purpose other than that for which it was originally collected;
- If the data will be collected using a technological solution that includes functionalities enabling the identification, location or profiling of an individual.

Now and in the future, Data Protection Committee or the Data Protection Committee must ensure that collection methods are compliant with relevant law, good practices and industry standards.

Data Protection Committee or the Data Protection Committee is responsible for creating and maintaining a Register of the Privacy Notices.

7. Organization and Responsibilities

The responsibility for ensuring appropriate Personal Information processing lies with everyone who

works for or with EXFO and has access to Personal Information processed by EXFO.

The key areas of responsibilities for processing Personal Information lie with the following organisational roles:

Roles	Responsibilities
PPI Responsible or Data Protection Committee*	• Ensure implementation of the PPI program; • Define budgets to support the PPI program; • Supervise the management of confidentiality incidents (including keeping the PRP incident register); • Act as a contact point for Data Subjects; • Ensure communications with control authorities (e.g. Commission d'accès à l'information "CAI"); • Supervise the conservation and disposal of Personal Information in collaboration with IT teams; • Controlling third-party communication and cross-border Personal Information transfers • Develop PPI training and awareness campaigns; • Review the compliance of the PPI program; • Manage complaints and requests for rights; • Report to the Board of Directors; • Handle requests to exercise individual rights (rights of access, rectification, withdrawal of consent, etc.). • 2nd-line monitoring of PPI; • Manage Privacy Impact Assessments ("PIAs"); • Recommend adoption of PPI policy; • Ensuring accountability.
Steering Committee	• Approves organization-wide PPI processes and procedures.
Operational Committee	• Develop and maintain organization-wide PPI processes and procedures
Legal and Compliance Manager	• Monitor the legal aspects of PPI. • Develop compliance requirements and help business departments achieve their Personal Information objectives.

Roles	Responsibilities
Business departments	**Responsibilities common to all business departments* • Obtain consent from data subjects for Personal Information collection activities for which they are responsible; • Report privacy incidents within their respective departments to the PPI Responsible; • Support PPI deployments and ensure compliance with PPI processes.
Director of Information Security	• Ensure the adequacy of controls and safety measures applicable to Personal Information; • Support the completion of PIAs; • 3rd-line monitoring of PPI.
Board of Directors	• Make decisions and approve EXFO's general strategies regarding the protection of Personal Information.
Human Resources Director	• Coordinate PPI training and awareness campaigns; • Ensure that employees' Personal Information is processed on the basis of EXFO's legitimate business purposes and needs.
IT Manager	• Operationalize the destruction and anonymization, if necessary, of Personal Information.
Purchasing Manager	• Communicate privacy responsibilities to suppliers; • Improve supplier awareness of privacy issues; • Transmit Personal Information requirements to any third party or supplier it uses.
Marketing Director	• Develop a communication strategy for internal and external PPI training and awareness campaigns. • Approve any data protection statements attached to communications such as e-mails and letters. • Respond to data protection requests from journalists and media organizations such as newspapers.
* The PPI Responsible is a member of the Data Protection Committee and the Operational Committee.	

8. Establishing the Lead Supervisory Authority pursuant to GDPR

EXFO identifies the Commission Nationale de l'Informatique et des Libertés (CNIL) as its Lead supervisory authority (LSA), under GDPR and the Comission d'accès à l'information (CAI) as its lead supervisory authority (LSA) under LPDP.

9. Response to Personal Information Breach Incidents

When EXFO learns of a suspected or actual Personal Information breach, the Data Protection Committee must perform an internal investigation and take appropriate remedial measures in a timely manner, according to its data breach guidelines. Where there is any risk to the rights and freedoms of Data Subjects, EXFO must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

10. Audit and Accountability

The Data Protection Committee is responsible for auditing how well business departments implement this Policy.

Any employee who violates this Policy may be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

11. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which EXFO operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

12. Managing Records Kept on the Basis of this Policy

(Please refer to EXFO's Data Retention Policy)

13. Validity and Document Management

The owner of this Policy is the Data Protection Committee, who must check and, if necessary, update this Policy.

14. Contact

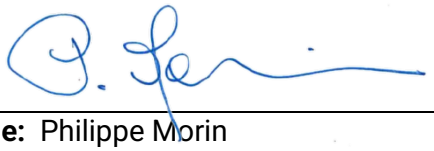
If you have any questions about this Policy, please contact the Data Protection Committee or the legal team:

Data Protection Committee
EXFO Solutions SAS
Z.A.C. Airlande - 2 rue Jacqueline Auriol
Saint Jacques de la Lande
CS 69 123 - 35 091 Rennes cedex 9
France
data.privacy@exfo.com

PPI Responsible (Québec)
Philippe Morin
Chief Executive Officer
EXFO Inc.
400 avenue Godin

Quebec City, QC, G1M 2K2
Canada
data.privacy@exfo.com
1-800-663-3936

Approval:



Name: Philippe Morin
Title: Chief Executive Officer
Date: 2023-09-20