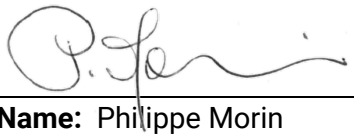
PERSONAL DATA PROTECTION POLICY

Version:	2.1
Date of version:	03-01-2023
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

Approval:



Name: Philippe Morin
Title: Chief Executive Officer
Date: 2023-03-01

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 Data protection in countries where EXFO operates. This Policy sets forth the basic principles by which EXFO processes the Personal Data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing Personal Data.

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

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of EXFO.

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 data 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.

Data Protection Committee: An internal EXFO committee which the primary role is to ensure that the organisation processes the personal data 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.

Personal Data: 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.

Sensitive Personal Data: Personal data 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 Data include Personal Data 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.

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 Data.

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

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

Processing: An operation or set of operations which is performed on Personal Data or on sets of Personal Data, 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.

Anonymization: Irreversibly de-identifying Personal Data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The Personal Data processing principles do not apply to anonymized data as it is no longer Personal Data.

Pseudonymization: The processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link Personal Data to a Data Subject. Because pseudonymized data is still Personal Data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of Personal Data: Processing of Personal Data 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 Data 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;

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

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 Data; 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;

Group Undertaking: Any holding company together with its subsidiary.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations handling Personal Data.

4.1. Lawfulness, Fairness and Transparency

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

4.2. Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3. Data Minimization

Personal data 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 Data if possible and commercially relevant to reduce the risks to the Data Subjects concerned, pursuant to its internal policies.

4.4. Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

4.5. Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.

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 Data risks, EXFO must use appropriate technical or organizational measures to process Personal Data in a manner that ensures appropriate security of Personal Data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

4.7. Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

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 Data possible. If Personal Data is collected from a third party, the Data Protection Committee must ensure that the Personal Data is collected lawfully.

5.4. Use, Retention, and Disposal

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

5.5. Disclosure to Third Parties

Whenever EXFO uses a third-party supplier or business partner to process Personal Data on its behalf, the Data Protection Committee must ensure that this processor will provide security measures to safeguard Personal Data 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 Data 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 Data

Before transferring Personal Data 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 Data must comply with the principles of Personal Data processing set forth in the relevant contract or any other legal binding document, as well as in the applicable law.

5.7. 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 Data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law.

5.8. 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 Data of other individuals.

5.9. Right to be Forgotten

Upon request, Data Subjects have the right to obtain from EXFO the erasure of its Personal Data, 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.

5.10. 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 data 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 Data 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 Data collected, the purposes of the processing, processing methods, the Data Subjects' rights with respect to their Personal Data, the retention period, potential international data transfers, if data will be shared with third parties and EXFO's security measures to protect Personal Data. This information is provided through Privacy Notice and will differ depending on the processing activity and the categories of personal data collected.

6.2. Obtaining Consents

Whenever Personal Data 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 Data 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 data must only be processed for the purpose for which they were originally collected. In the event that EXFO wants to process collected Personal Data 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.

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 Data processing lies with everyone who

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

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

The **board of directors** makes decisions about and approves EXFO's general strategies on Personal Data protection.

The **Data Protection Officer (DPO) or Data Protection Committee**, as the case may be, is responsible for managing the Personal Data protection program, the development and promotion of end-to-end Personal Data protection policies and acting as a contact point for Data Subjects and the relevant authorities, as defined in Data Protection Officer Job Description or in the Data Protection Committee's mission. The Data Protection Officer also supervises the Data Protection Committee, if applicable.

The **Legal advisors acting through the Data Protection Committee** monitors and analyses Personal Data laws and changes to regulations, develops compliance requirements, and assists business departments in achieving their Personal data goals.

The **Security specialist acting through the Data Protection Committee** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The **Marketing manager acting through the Data Protection Committee**, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.

- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with the Data Protection Committee to ensure marketing initiatives abide by data protection principles.

The **Human Resources Manager acting through the Data Protection Committee** is responsible for:

- Improving all employees' awareness of user Personal Data protection.
- Organizing Personal data protection expertise and awareness training for employees working with Personal Data.
- End-to-end employee Personal Data protection. It must ensure that employees' Personal Data is processed based on the employer's legitimate business purposes and necessity.

The **Procurement Manager** is responsible for passing on Personal Data protection responsibilities to suppliers and improving suppliers' awareness levels of Personal Data protection as well as flow down Personal Data requirements to any third party a supplier they are using. The Procurement Department must ensure that EXFO reserves a right to audit suppliers.

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 Data Breach Incidents

When EXFO learns of a suspected or actual Personal Data 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 EXFO at one of the following contact information:

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

Person in charge of the protection of personal information (Quebec)
Philippe Morin
Chief Executive Officer
EXFO Inc.
400 Godin Avenue
Quebec, QC, G1M 2K2
Canada
data.privacy@exfo.com
1-800-663-3936

Approval:

Name: Philippe Morin
Title: Chief Executive Officer
Date: 2023-03-01