Enterprise Privacy Directive [CGD2]

Table of contents

Section 1: Overview

1.1 Scope

LABORIE strives to comply with applicable laws and regulations related to Personal Data protection in countries where it operates. This Policy sets forth the basic principles by which LABORIE 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.

LABORIE's Enterprise Privacy Directive has been developed to govern the collection, use and disclosure of personal data (PD)/personal information (PI) in a manner that will facilitate business operations and service delivery while protecting the rights and privacy of staff, clients and members of the public.

LABORIE shall provide its personnel and third-party providers with formal direction on their accountabilities, roles and responsibilities for protecting privacy. Means of providing such direction may include: training and awareness programs, agreements and written policies and procedures and job descriptions.

LABORIE shall publish its privacy policies and practices on its website and make copies of them available through the Data Protection Office. For the benefit of clarity, LABORIE shall not publish or make available policies or practices if doing so could compromise the security of personal data or would reveal a trade secret or confidential scientific, technical, commercial or labour relations information.

1.2 Responsibilities

Role	Responsibility
LABORIE's Board of Directors	• Oversees the protection of privacy at the Company.
President and Chief Executive Officer (CEO)	• Manages the privacy protection at, including ensuring that LABORIE complies with applicable privacy requirements in each of jurisdiction it operates and fostering a culture of privacy protection. • Delegates responsibility of the data protection program to the DPO.
Data Protection Officer (DPO)	• Leads the design and operation of data protection program, including privacy-related governance bodies. • Provides advice, support and direction to personnel about privacy matters applicable to their areas of responsibility. • Monitors and reports on privacy protection at LABORIE. • Advises managers about the privacy implications of, and requirements for, policies and practices in their areas of responsibility. • Establishes and maintains written policies and practices that direct the design and management of the privacy protection program.

	• Creates and maintains a Register of the Privacy Notices. • Reviews and updates the training program annually.

1.3 Definitions

NOTE: The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation.

Term	Definition
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.
Cross-border processing of personal data	Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
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/Electronic Service Provider	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
Group Undertaking	Any holding company together with its subsidiary.
Lead supervisory authority	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.
Local supervisory authority	Local supervisory authority will still maintain in its own territory, and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers includes conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

Term	Definition
Main establishment as regards a controller	Main establishment as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.
Main establishment as regards a processor	Main establishment as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.
Personal Data (PD)/Personal Information (PI	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.
Privacy Commissioner	A regulatory authority responsible for enforcing privacy and data protection legislation in Canada.
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.
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.
Sensitive Personal Data/Personal Health Information (PHI)	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.
Supervisory Authority	An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR.

1.4 Reference Documents

- 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)
- Health Insurance Portability and Accountability Act (HIPAA)
- Personal Information Protection and Electronic Documentation Act (PIPEDA)
- Personal Health Information Protection Act (PHIPA)
- Data Governance and Protection Directive [CGD2] (PRC-021293)
- Governance Program – Section 5: Data Protection [CGD2] (PRC-019363600

NOTE: Refer to the Document Management System for the latest version.

Section 2: Building Data Protection in Business Activities

2.1 Notification to Data Subjects

LABORIE shall 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, should post the Privacy Notice. The Privacy Notice shall explain the types of personal data collected, the purposes of the processing and the legal basis for the processing, processing methods, the identity of the data controller, 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, the security measures to protect personal data and contact details of the data controller and the data protection officer.

Where sensitive personal data is being collected, the Data Protection Officer must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

DPO is responsible for creating and maintaining a Register of the Privacy Notices.

For more information, refer to:

☐Privacy Breach Management Procedure [CGD3] (PRC-021299)

2.2 Data Subject's Choice and Consent

LABORIE shall maintain a record of data processed with consent of the individual.

LABORIE shall provide data subjects with options to provide the consent. The Company must inform data subjects that their consent can be withdrawn at any time.

LABORIE shall put in place technical capabilities and business processes

- To comply with data subject request for consent withdrawal.
- To retain a record of consent processing.
- To process consent related to a child under the age of 16.

For more information, refer to:

☐***Consent Management Procedure [CGD2] (PRC-021296)***

2.3 Collection

LABORIE must strive to collect the least amount of personal data possible. If personal data is collected from a third party, it must ensure that the personal data is collected lawfully.

Personal data must only be processed for the purpose for which they were originally collected. In the event that LABORIE process personal data for another purpose, it 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).

For more information, refer to:

☐***Consent Management Procedure [CGD2] (PRC-021296)***

☐***Laborie Data Processing Agreement [CGD4] (PRC-021452)***

2.4 Withdrawal of Consent

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. It shall be as easy to withdraw as to give consent.

For more information, refer to:

☐***Consent Management Procedure [CGD2] (PRC-021296)***

☐***Withdrawal of Consent - Patients [CGD4] (PRC-021304)***

☐***Withdrawal of Consent - Employees [CGD4] (PRC-021493)***

2.5 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. LABORIE must maintain the accuracy, integrity, confidentiality and relevance 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.

The staff shall not access Personal Data unless:

- Access is necessary in order to perform their roles;
- They have been authorized to do so by the requisite authority;
- They agree to Laborie Confidentiality Agreement and completed applicable privacy training;
- They have formally agreed to comply with any additional privacy-related requirements and restrictions established by LABORIE; and they are in compliance with all applicable policies.

For more information, refer to:

☐***Laborie Security Awareness Training | GDPR module***

☐***Data Inventory and Retention Table [CGD4] (PRC-021503)***

2.6 Disclosure to Third Parties

LABORIE must ensure that third party processor will provide security measures to safeguard personal data that are appropriate to the associated risks.

LABORIE must contractually require the supplier or business partner to provide the same level of data protection as it provides to its own data. These contracts shall set out expectations regarding compliance with relevant data protection legislation (GDPR, PIPEDA, HIPPA, and PHIPA), policies and procedures, and responsibilities for the protection and safeguarding of PI.

The supplier or business partner must only process personal data to carry out its contractual obligations or upon the instructions of LABORIE and not for any other purposes. When LABORIE processes personal data jointly with an independent third party, it must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document.

For more information, refer to:

☐***Laborie Data Processing Agreement [CGD4] (PRC-021452)***

2.7 Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained. The entity receiving the personal data must comply with the principles of personal data processing.

2.8 Data Subject Requests

LABORIE is responsible to provide data subjects with access their personal data, and must allow them to update, rectify, erase, block or transmit their Personal Data, if appropriate or required by law. If LABORIE is required to take such actions by law, please refer to sections 2.9 – 2.14 below

2.9 Data Subject Request for Information

LABORIE is responsible to provide data subjects with a reasonable access mechanism to enable them to access their personal data.

LABORIE must ensure that request for access to patients own information shall be handled in a reasonable timeframe and as required by law. A log for request to access data should be maintained.

For more information, refer to:

☐ ***Data Access Request Procedure [CGD3] (PRC-021295)***

☐***Data Subject Access and Transfer Request Form [CGD4] (PRC-021305)***

2.10 Data Subject Request for Rectification

LABORIE shall provide the possibility for Data Subjects to without undue delay obtain the rectification of inaccurate personal data concerning him or her.

LABORIE must communicate any rectification of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

2.11 Data Subject Request for Data Portability

LABORIE shall provide the option to Data Subjects to transmit the data they provided to the Company in a structured format and to transmit those data to another controller, for free.

LABORIE shall put in place processes for the fulfilment of such request from the Data Subject.

> ***For more information, refer to:***
>
> ***☐Data Access Request Procedure [CGD3] (PRC-021295)***
>
> ***☐Data Subject Access and Transfer Request Form [CGD4] (PRC-021305)***

2.12 Data Subject Request for Restriction of Processing

LABORIE shall provide the possibility for Data Subjects to obtain restrictions of processing where one of the following applies:

(i) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(iii) LABORIE no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

(iv) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State.

LABORIE must communicate any restriction of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

2.13 Data Subject Right to Object

Where personal data are processed based on a public interest, balancing of interest or for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such purposes.

2.14 Data Subject Request for Erasure (Right to be Forgotten)

Upon request, Data Subjects have the right to obtain from LABORIE the erasure of its personal data.

LABORIE shall put technical capabilities and business processes in place to fulfil this request from Data Subjects. LABORIE must communicate any erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

Section 3: Privacy Training and Awareness

LABORIE shall provide a foundational privacy training program suitable for all personnel. The DPO shall review and update the program at least annually to address any substantive changes to data protection and privacy requirements and any other relevant matters.

The DPO shall develop and provide role-based privacy training for personnel commensurate with their responsibilities and whether or not personnel may have access to PI/PHI.

LABORIE shall protect PI/PHI with technical, administrative, and physical safeguards that:

- Are appropriate to the information's sensitivity, the format in which it is held, and the related privacy risks; and
- Secure the PI/PHI against: theft, loss, unauthorized access, collection, use or disclosure and unauthorized copying, modification, retention or disposal.

For more information, refer to:

Laborie Security Awareness Training | GDPR module

Q620-FRM-03: Role-Based Training Matrix

Section 4: Response to Personal Data Breach Incidents

LABORIE shall ensure protection of the persona data in its control. In the event of the data breach, it shall follow the notification requirements as stipulated in the relevant legislative requirements (i.e. GDPR, PIPEDA, PHIPA and HIPPA).

LABORIE shall develop a comprehensive data breach management procedure. The Procedure should include at minimum the process for:

- Notification of data privacy breach to the DPO.
- Containment of the data privacy breach.
- Investigation of data privacy breach.
- External notification protocol per GDPR, PHIPA, PIPEDA and HIPPA.
- Data subject notification.

For more information, refer to:

Privacy Breach Management Procedure [CGD3] (PRC-0121299)

Section 5: Complaints and Inquiries

LABORIE shall manage and respond to complaints, questions and feedback about its privacy practices. LABORIE shall review, investigate and document every complaint received and shall monitor for any trends arising.

If the sender provides contact information, LABORIE shall:

- Acknowledge the complaint, question or feedback within five (5) business days of receipt and provide information about any relevant internal and external complaint mechanisms;
- Respond to the sender's question, feedback or complaint within thirty (30) business days of receipt; and
- Notify the sender of its expected timeframe for responding if it anticipates a delay arising.

LABORIE shall take appropriate measures to respond to complaints and feedback, which may include changing its policies and practices.

LABORIE shall provide a means for personnel to share privacy-related concerns in confidence and shall ensure that reporting personnel suffer no reprisals.

Section 6: Record Retention

LABORIE shall develop a record retention schedule of the information in its custody and control. The record retention schedule should be reviewed and updated on a yearly basis.

For more information, refer to:

Data Inventory and Retention Table [CGD4] (PRC-021503)