Data Governance and Protection Directive [CGD2]

Change history

Version	Date	Description of change	Reason of change
1.00	2018/04/26	Initial Draft	Set up for GDPR legislation

Table of contents

Section 1: Overview....4

1.1 Scope 4

1.2 Responsibilities 4

1.3 Definitions 6

1.4 Reference Documents 8

Section 2: Basic Principles Regarding Personal Data Processing....8

2.1 GDPR Guiding Principles 8

2.2 Canadian/USA: Fair Information Principles 9

Section 3: Privacy Protection Program....10

Section 4: Organization....10

Section 5: Managing Data Subject Rights....11

Section 6: Audit and Accountability....11

Appendix A Appendix 1: Summary of Data Protection Procedures, Forms and Processes....12

Section 1: Overview

1.1 Scope

In this Directive, "LABORIE" refers to Laborie Medical Technologies Canada, ULC and all affiliates and subsidiaries. LABORIE, strives to comply with applicable laws and regulations related to Personal Data protection in countries where LABORIE operates. This Directive sets forth the basic principles by which the 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.

This Directive applies to LABORIE and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA, Canada and the United States of America.

The Directive supports decision-making by establishing guiding principles

- On how LABORIE will protect privacy, and the confidentiality of personal information.
- Establishes policies about how LABORIE manages privacy protection in order to achieve privacy compliance and a culture of privacy protection
- Identifies core privacy responsibilities for LABORIE's personnel to foster co-ordination among LABORIE's divisions and teams in protecting privacy.

LABORIE maintains a comprehensive set of privacy and data protection policies that are subordinate and complementary to the Data Governance and Protection Policy. The subordinate policies, define privacy roles, responsibilities, accountabilities and requirements for the protection of personal and sensitive personal data.

LABORIE believes that protecting privacy effectively involves not only complying with applicable privacy requirements but also having a strong culture of privacy protection. This Data Governance and Protection Policy mandates the LABORIE Privacy Protection Program. The Privacy Protection Program comprises comprehensive safeguards for personal data and programs, practices, processes, tools and techniques to protect privacy proactively.

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

1.2 Responsibilities

Role	Responsibility
LABORIE's Board of Directors	• Makes decisions about; and approves LABORIE's general strategies on personal data protection.
Data Protection Officer (DPO)/Chief Privacy Officer	• Manages the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies. • Monitors and analyses personal data laws and changes to regulations. • Develops compliance requirements.

	• Assists business departments in achieving their Personal data goals.
Lead Supervisor Authority	• Authority of the Main LABORIE establishment in the EU, where cross-border processing of personal data is carried out in the EU.
IT Manager	• Ensures all systems, services and equipment used for storing data meet acceptable security standards. • Performs regular checks and scans to ensure security hardware and software is functioning properly.
Marketing Manager	• Approves any data protection statements attached to communications such as emails and letters. • Addresses any data protection queries from journalists or media outlets like newspapers. • Where necessary, works with the Data Protection Officer to ensure marketing initiatives abide by data protection principles. • Advises the DPO is any potential data breach or concern.
Human Resources Manager	• Improves all employees' awareness of user personal data protection. • Organizes Personal data protection expertise and awareness training for employees working with personal data. • Provides end-to-end employee personal data protection • Ensures employees' personal data is processed based on the employer's legitimate business purposes and necessity. • Advises the DPO is any potential data breach or concern.
Procurement Manager	• Forwards personal data protection responsibilities to suppliers. • Improves suppliers' awareness levels of personal data protection. • Forwards personal data requirements to any third party a supplier they are using. • Ensures that the Company reserves a right to audit suppliers. • Advises the DPO is any potential data breach or concern.
Clinical Research Manager	• Improves all patients' awareness of user personal data protection. • Provides end-to-end patient personal data protection for clinical studies. • Ensures patient's personal data is processed based on the employer's legitimate research purposes and necessity. • Advises the DPO is any potential data breach or concern.
Finance Manager	• Ensures all financial data (e.g, payroll, benefits, etc.) are protected. • Ensures employees' personal data is processed based on the employer's legitimate business purposes and necessity. • Advises the DPO is any potential data breach or concern.

R&D Manager	• Ensures data protection measures are embedded early in the design and development of new/upgraded/modified products and services, including outsourced products and services
Regulatory Affairs Manager	• Advises the DPO is any potential data breach or concern.
Customer Service Manager	• Ensures data protection measures are maintained during service, repair and in the call centre. • Advises the DPO is any potential data breach or concern.
Operations / Production Manager	• Ensures data protection measures are maintained during production. • Advises the DPO is any potential data breach or concern.
Quality Manager	• Ensures data protection measures are maintained during Quality-related tasks in design, production and post-production. • Advises the DPO is any potential data breach or concern.

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.

Term	Definition
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 include 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.
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.

Term	Definition
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)
- Enterprise Privacy Directive [CGD2] (PRC-021294)
- Governance Program [CGD2] – Section 5: Data Protection (PRC-019363600

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

Section 2: Basic Principles Regarding Personal Data Processing

2.1 GDPR Guiding Principles

The data protection principles outline the basic responsibilities for organisations handling personal data. Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*."

Lawfulness, Fairness and Transparency	Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
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.
Data Minimization	Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Company must apply anonymization or pseudonymization to personal data if possible to reduce the risks to the data subjects concerned.
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.
Storage Period Limitation	Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed.
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, the Company 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.
Accountability	Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

2.2 Canadian/USA: Fair Information Principles

The Fair Information Principles (FIP) on which both the Canadian and the US privacy legislations are based upon are noted below. The Fair Information Principles closely align with principles on processing of data as per GDPR.

Principle 1 - Accountability	Laborie is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
Principle 2 - Identifying Purposes	The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
Principle 3 - Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
Principle 4 - Limiting Collection	The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
Principle 5 - Limiting Use, Disclosure, and Retention	Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
Principle 6 - Accuracy	Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
Principle 7 - Safeguards	Personal information must be protected by appropriate security relative to the sensitivity of the information.
Principle 8 - Openness	An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Principle 9 - Individual Access	Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Principle 10 - Challenging Compliance	An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with privacy and data protection laws.

Section 3: Privacy Protection Program

LABORIE shall maintain a Privacy Protection Program that comprises comprehensive and aligned safeguards for Personal Data and programs, practices, processes, tools and techniques that enable it to:

- Protect individuals' privacy and the confidentiality of their Personal Data and Sensitive Personal Data proactively and respect their privacy preferences;
- Comply with its privacy requirements, particularly those derived from its Enabling Regulation, from GDPR, HIPAA, PIPEDA, PHIPA and the Regulations made under those Acts, and from its policies.

The Privacy Protection Program shall include processes, practices and tools and techniques to:

- Build privacy and security protection into the design and operation of the Company's programs, operations and services, including business practices, systems and physical design and infrastructure;
- Safeguard Personal Data and Sensitive Personal Data throughout its lifecycle;
- Achieve, monitor, assess and enforce privacy compliance;
- Identify and manage privacy risks proactively;
- Train personnel about protecting privacy;
- Develop and implement privacy and data protection policies, practices and standards;
- Manage, investigate and respond to privacy- and security- related incidents, breaches, complaints and inquiries;
- Conduct data risk assessment/privacy risk assessments as appropriate.

For more information, refer to:

☐Enterprise Privacy Directive [CGD2] PRC-021294

Section 4: Organization

LABORIE policies and practices shall:

- Protect privacy and the confidentiality of Personal Data and Sensitive Personal Data while achieving LABORIE's business interests and objectives (e.g. effectively facilitating the delivery of services and programs and realizing value for money); and
- Comply with all applicable privacy requirements, in particular the Guiding Principles and Policy Requirements articulated in the Data Governance and Protection Policy.
- The Data Protection Officer (DPO) and/or Chief Privacy Officer (Canada/USA) shall ensure that LABORIE's policies and practices that protect individuals' privacy and the confidentiality of their Personal Data and Sensitive Personal Data are comprehensive, aligned and complementary.
- LABORIE shall comply with its policies and practices that protect individuals' privacy and the confidentiality of Personal Data and Sensitive Personal Data.
- LABORIE shall enter into signed, written agreements with third party providers that include appropriate privacy requirements prior to the third parties providing services or goods to the Agency.

Section 5: Managing Data Subject Rights

LABORIE shall put in place process and procedures to manage data subject right such as consent management, data access request. The Enterprise Privacy Directive and the relevant procedures provide detailed information on managing rights of the individuals on collection, use and disclosure of their Personal Data.

> ***For more information, refer to:***
>
> ***Enterprise Privacy Directive [CGD2] PRC-021294***

Section 6: Audit and Accountability

The Audit Department is responsible for auditing how well business departments implement this Directive and associated procedures.

Any employee who violates this Policy will 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.

Appendix A Appendix 1: Summary of Data Protection Procedures, Forms and Processes

Procedure [CGD3] and/or Topic	Supporting Form(s) [CGD4]	Other Supporting Documents
Consent Management Procedure [CGD3] (PRC-02126)	• Consent Form – Employees [CDG4] (PRC-021370) • Withdrawal of Consent Form - Employees [CDG4] (PRC-021493) • Consent Form – Patients [CDG4] (PRC-021303) • Withdrawal of Consent Form – Patients [CGD4] (PRC-021304)	• Q736-PRO-01: Clinical Evaluations • Q905-FRM-05: Informed Consent Form
Data Privacy Impact Assessment (DPAI) Procedure [CGD3] (PRC-021297)	• DPIA Questionnaire [CGD4] (PRC-021308) • Privacy Risk Register [CGD4] (PR-021306) • Threshold Questionnaire [CGD4] (PRC-021307)	• Q754-WI-01: HIPAA,HITECH & PIPEDA Summary • Q710-PRO-01: Product Realization Planning • Q710-PRO-02: Risk Management • Q731-PRO-01: Design and Development Planning • Q732-PRO-01: Design and Development Inputs
Data Subject Access Request Procedure [CGD3] (PRC-021295)	• DPO Contact information [CDG4] (PRC-021298) • Data Subject Access and Transfer Request Form [CDG4] (PRC-021305)	
Privacy Breach Management Procedure –CGD3] (PRC-021299)	• Privacy Breach Log [CDG4] (PRC-021723)	• Q710-PRO-02: Risk Management
Privacy Communications		• Laborie Security Awareness Training • Q620-FRM-03: Role Based Training Matrix

Procedure [CGD3] and/or Topic	Supporting Form(s) [CGD4]	Other Supporting Documents
Procedure [CGD3] (PRC-021302)		
Data Protection in R&D / Design and Development		• Q710-PRO-01: Product Realization Planning • Q731-PRO-01: Design and Development Plan • Q732-PRO-01: Design Inputs • Q738-PRO-02: Design History File
Data Protection in Service		• Q754-PRO-01: Customer Property • Q751-PRO-02: Control of Production and Servic e-Service and Repair • Q751-PRO-03: Control of Production and Service – Installations • Q830-WI-03: Wiping Data from Hard Disk • Q821-PRO-01: Complaint Feedback and Handling
Data Protection in Regulatory Affairs		• Q851-PRO-01: Vigilance Monitoring and Recalls • Q851-PRO-02: Medical Device Reporting
Data Protection in Purchasing	• Laborie Data Processing Agreement [CGD4] (PRC-021452)	• Q741-PRO-01: Supplier Approval and Control • Q741-PRO-02: Distributor Approval and Control
Data Protection in Clinical Trials		• Q736-PRO-02: Clinical Evaluations • Q905-PRO-01: Conducting Clinical Trials • Q905-FRM-05: Informed Consent Form • Q906-PRO-01: Investigator Initiated Research • Q906-FRM-03: IIR Study Agreement

Procedure [CGD3] and/or Topic	Supporting Form(s) [CGD4]	Other Supporting Documents
Data Protection in Marketing		• Q723-PRO-01: Customer Communication • Q723-FRM-01: Global Communication Bulletin
Data Protection in HR	• Employee Onboarding Checklist [CGD4] • Employee Exit Checklist [CGD4]	•
Data Protection in Finance	• Employee Onboarding Checklist [CGD4] • Employee Exit Checklist [CGD4] • Employee Expense Report - NA [CGD3] (PRC-019796)	• 0045-FRM-005: Employee Expense Report (PRC-004134) Enschede only
Data Protection in Operations		• Q738-PRO-01: Design Transfer • Q751-PRO-05: Device History Record • Q753-PRO-01: Identification and Traceability • Q753-PRO-03: Product Traceability and DHR
Data Protection in Quality		• Q424-PRO-01: Control of Quality Records • Q737-PRO-01: Control of Design and Development Changes • Q738-PRO-03: Device Master Record • Q760-PRO-01: Control of Monitoring and Measuring Devices • Q830-PRO-01: Control of Nonconforming Product • Q850-PRO-01: Corrective and Preventive Action