## TABLE OF CONTENTS

## INTRODUCTION

This Privacy Policy ("**Policy**") describes the guiding principles of Theratechnologies Inc. (including its subsidiaries Theratechnologies Europe Limited and Theratechnologies U.S. Inc., collectively referred to as "**Thera**") concerning the collection, use, disclosure, and protection of Personal Information (as defined below) and how such Personal Information can be consulted and corrected, if necessary.

Thera, a clinical-stage biopharmaceutical company focused on the development and commercialization of innovative therapies, is committed to protecting the confidentiality and accuracy of all the Personal Information it will collect, use, disclose or retain and to comply with all Applicable Privacy Laws (as defined below).

While doing business, Thera, acting as data controller, will process Personal Information of identifiable individuals, including, but not limited to, customers, website visitors, employees or patients indirectly gaining access to any of Thera's products.

## 1. DEFINITIONS

- "**Applicable Privacy Laws**" means any legislation, regulation or recommendation related to privacy matters and applicable to Thera, including notably, the *Act Respecting the protection of personal information in the private sector* ("**Quebec Private Sector Act**"), the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and the European Union ("**EU**") *General Data Protection Regulation* ("**GDPR**"). Applicable Privacy Laws shall also include any legislation, regulation, recommendation or official guidance replacing, adding to, amending, extending, reconstituting or consolidating any of the foregoing laws;

- "**Confidentiality Incident**" shall have the meaning ascribed thereto in section 10.3;

- "**Data Minimization Principle**" shall have the meaning ascribed thereto in section 5.4;

- "**Data Protection Officer**" or "**DPO**" shall have the meaning ascribed thereto in section 13.1;

- "**Employees**" means all employees i.e., director, employee, trainee, and any other person who works either on a full-time or part-time, a permanent or temporary basis and who is entitled to receive a salary from Thera;

- "**Individual**" means an identified or identifiable natural person;

- "**Minors**" shall have the meaning ascribed thereto in section 11;

- "**Non-Personally Identifiable Information**" or "**Non-PII**" means information which does not relate to an identified or identifiable natural Individual. Non-PII also includes Personal Information aggregated or rendered anonymous in such a manner that an Individual is no longer identifiable;

- "**Personal Information**" means any factual or subjective information, recorded or not, about an identifiable Individual, such as age, gender, birth date, province of residence, preferences, opinions, that can directly identify that Individual (for example an individual's name), or that could identify that Individual once the information is combined (for example the elements of a physical description). Personal Information does not include information that has been anonymized or aggregated in such a way that there is no serious possibility that it can be used to identify an individual, whether on its own or in combination with other information;

- "**Policy**" shall have the meaning ascribed thereto in the introduction;

- "**Privacy Impact Assessment**" or "**PIA**" shall have the meaning ascribed thereto in section 7.4b;

- "**Privacy Officer**" shall be the person identified in section 13.1;

- "**Processing**" means any operation which is performed on Personal Information or on sets of Personal Information, whether by automated means or not, 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;

- "**Purpose**" shall have the meaning ascribed thereto in section 5.3;

- "**Sensitive Information**" shall mean any Personal Information which, due to its nature, either medical, biometric or otherwise intimate nature, entails a high expectation of privacy. Under the GDPR, Sensitive Information is Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation;

- "**Regulatory Authority**" means an independent public authority, established by law, which has jurisdiction to oversee privacy and Personal Information protection matters.

- "**Thera**" shall have the meaning ascribed thereto in the introduction;

- "**Transfer Impact Assessment**" or "**TIA**" shall have the meaning ascribed thereto in section 7.4b;

- "**Websites**" shall have the meaning ascribed thereto in section 3 (iv).

## 2. OBJECTIVES

This Policy sets forth a specific privacy framework and is the overriding policy regarding the protection of Personal Information at Thera. The objectives of this Policy are, notably, to:

- Set out governance principles, roles and responsibilities within Thera, with respect to the protection of Personal Information throughout its life cycle;
- Provide a clear procedure for Individuals to be able to exercise their rights; and
- Provide the process for handling privacy complaints.

## 3. SCOPE

This Policy applies to all Personal Information of Individuals Processed by Thera or disclosed to Thera by third parties, including, but not limited to, the Personal Information of:

(i) Individuals collected through their professional interactions with Thera's Employees or Thera's service providers;
(ii) Members of the general public contacting Thera to inquire about services or products;
(iii) Visitors entering Thera's business premises; and

(iv) Visitors or users of Thera's websites and online services (collectively, the "**Websites**") located at:

a. https://www.theratech.com
b. https://www.trogarzo.com
c. https://www.egriftasv.com

## 4. RESPONSIBILITIES

Protecting the privacy of Individuals is the responsibility of every Employee and each one must read, understand and comply with this Policy. For clarity, each Employee is responsible for verifying that all of the necessary measures to meet the requirements outlined in this Policy are in place before processing any Personal Information. The Employees are encouraged to contact privacy@theratech.com for any assistance to confirm that sufficient measures are in place.

## 5. COLLECTION OF PERSONAL INFORMATION

### 5.1 Source of Personal Information

#### a. Provided by Individuals

Generally speaking, the Personal Information collected is provided from an Individual through its interaction with Thera. When contacting or being contacted by Thera, Individuals may be required to provide Personal Information, namely when:

- Interacting with Thera's Employees via phone calls, emails, web forms, social media and other methods of communication;
- Subscribing to Thera's promotional tools;
- Entering Thera's premises; and
- Visiting or using Thera's Websites.

#### b. Personal Information Obtained Lawfully from Third Parties

When interacting with third parties, Thera must only accept the disclosure of Personal Information that has been lawfully collected or otherwise obtained by such third parties, whom must also have in place a privacy policy governing the protection of Personal Information compliant with Applicable Privacy Laws.

Before the exchange of Personal Information, Thera's Employee shall obtain a confirmation in writing from the third party that: (i) it has lawfully collected the Personal Information; and (ii) it has the right to disclose such Personal Information to Thera.

#### c. Personal Information Collected Automatically

Thera may also collect both Personal Information and Non-PII about Individuals related to their web browsing habits when they visit or use Thera's Websites, mobile apps or other social media platform. For more information, please refer to our Cookie Policy.

## 5.2 Legal Basis for Collection

### a. Consent

Except in situations of alternative legal basis, Thera will always obtain an Individual's consent prior to the Processing of Personal Information and such consent will be documented in writing. Any Employee collecting an Individual's consent shall also note the date the consent was given, and the nature of the consent collected (e.g., written, check box, etc.).

The consent shall be clear, free and informed and be given for a specific Purpose (as defined in section 5.3). The foregoing means that an Individual must understand what he/she is consenting to, and it must be reasonable to expect that such Individual understands the nature, purpose and consequences of the Processing of his/her Personal Information. If the Processing involves a transfer of Personal Information to third parties, Thera will obtain the Individual's consent for such transfer and the consent shall expressly include the jurisdiction where the Personal Information will be transferred to.

Individuals may, at any time, modify or withdraw their consent. Employees collecting Personal Information shall provide Individuals with a comprehensive manner in which to exercise their withdrawal right as provided for in section 11 below.

### b. Alternative Legal Basis under the GDPR

When applicable, the GDPR enables Thera to rely upon alternative legal basis for the Processing of Personal Information instead of obtaining the consent of an Individual.

The alternative legal basis for Processing the EU residents' Personal Information as set out in this Policy are as follows:

- When the use of Personal Information is necessary to perform Thera's obligations under a contract with an EU resident (for example: when the EU resident uses the Websites);
- When the use of Personal Information is necessary for Thera's legitimate interests or the legitimate interests of others (for example, to ensure Thera's Website security or to prevent fraud related to any of Thera's products or services). In such situation, Thera shall consider the Individuals' rights under the GDPR and balanced them against Thera's legitimate interests;
- When the use of Personal Information is necessary to comply with legal requirements or defend Thera's legal rights.

## 5.3 Information to Be Provided at Time of Collection

The specific legitimate business purposes of the Processing ("**Purpose**") must always be identified by Thera before or at the time of collecting such Personal Information. Thera shall always limit the collection of Personal Information only to what is strictly necessary to achieve the Purpose.

In addition to the Purpose being identified, the following questions should be answered and provided to an Individual prior to the collection of his/her Personal Information:

- What Personal Information is collected?
- Why is it collected?
- How is it collected?
- Where is it kept?
- How is it secured?
- Who has access to or uses it?
- Who is it shared with?
- When applicable, is Thera using a technology that includes features to identify, locate or profile the Individuals and in the affirmative, what are the means offered to activate/de-activate these functions?
- When is it disposed of?

## 5.4 Personal Information Minimization Principle

Except if otherwise permitted under this Policy, Thera shall always Process the minimum amount of Personal Information necessary to accomplish the Purpose (the "**Data Minimization Principle**").

### a. Applicability of Data Minimization Principle

The Data Minimization Principle will apply to all services and activities of Thera involving the Processing of Personal Information.

### b. General Procedures for Implementing Data Minimization Principle

- ***Implementation of Technical and Organizational Measures***. Thera will, both at the time of determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organizational measures in order to comply with the Data Minimization Principle. For example:

    - ***Persons with Access***. Thera's Privacy Officer (as identified in section 13) will identify a limited number of Employees who shall be authorized to Process Personal Information.
    - ***Identification of Purpose for Processing.*** Prior to Processing any Personal Information, the Employee will identify the Purpose for which it needs to be Processed.
    - ***Limitation on Access and Processing of Personal Information***. Thera will provide the authorized Employee access to the Personal Information and such access shall be limited only to what is necessary to accomplish the identified Purpose.

## 6. USE OF PERSONAL INFORMATION

## 6.1 Purpose

The Personal Information must only be used: (i) for the Purpose identified by Thera when consent was obtained in accordance with this Policy; or (ii) for purposes in accordance with alternative legal basis under the GDPR. The foregoing purposes may include:

- Processing orders for Thera's services and/or products;
- Sending promotional materials, newsletters, offers or other information;
- Processing and responding to complaints and inquiries;
- Compliance with legal or regulatory requirements; and
- Any additional purposes mentioned in other applicable internal policies.

### 6.2 Use for Automated Processing

It Thera uses Personal Information to render a decision based exclusively on an automated Processing of such information, Thera must inform the Individual concerned accordingly not later than at the time it informs the Individual of the decision. Upon request, Thera must also provide the following:

(i) The Personal Information that was used to render the decision;

(ii) The reasons and the principal factors and parameters that led to the decision; and

(iii) The right of the Individual concerned to have the Personal Information used to render the decision corrected.

The Individual concerned must be given the opportunity to submit observations, by contacting privacy@theratech.com.

### 6.3 Secondary use of Personal Information in Quebec

The *Quebec Private Sector Act* allows companies to use Personal Information for another purpose without the consent of an Individual in specific situations when:

- It is for a purpose consistent with the initial Purpose for which the information was Processed (consistent purposes does not include commercial or philanthropic prospecting);
- It is clearly for the benefit of an Individual;
- It is necessary for the prevention and/or detection of fraud or the evaluation and improvement of safeguards and security measures;
- It is necessary for the purpose of providing or delivering a product or service requested by an Individual; and
- It is necessary for study, research or statistical purposes and the information is de-identified.

When the contemplated secondary use involves Sensitive Information, Thera shall obtain the express consent of the Individual concerned.

## 7. DISCLOSURE OF PERSONAL INFORMATION

### 7.1 Within Theratechnologies

Personal Information handled within Thera shall only be accessed or disclosed to Employees identified by the Privacy Officer who have a need to know such information to perform their duties as required by their position, the whole in accordance with the Purpose identified at the time of Processing Personal Information.

## 7.2 To Third Parties

Thera may share Personal Information with third parties who have a need to know such information to assist Thera in achieving the business Purposes identified at the time consent was given.

When Thera transfers Personal Information to third parties for Processing, it can only be used for the Purposes for which the consent was originally given. Further, the third party must provide adequate level of protection that can be compared to the level of protection the Personal Information would have received if it had not been transferred. Adequate protection includes:

**a.** ***A written agreement*** setting forth the roles and responsibilities of the parties with regards to the Personal Information, in particular, the measures put in place by the third party to:

- Protect the confidentiality of the Personal Information provided;
- Ensure that the Personal Information is used only for the Purpose identified in the agreement; and
- Ensure that the Personal Information is not retained after the expiration or early termination of the agreement.

In addition, the agreement must state that:

- The third party shall promptly notify Thera's Privacy Officer of any breach or attempted breach of the confidentiality obligations contained in the agreement; and
- Thera reserves the right to conduct any audit relating to the confidentiality measures implemented by the third party.

**b.** ***Policies*** governing the Processing of Personal Information.

Further, Personal Information may be disclosed to third parties in the following situations:

- As permitted under Applicable Privacy Laws. In such a case, Thera will endeavor to not disclose more Personal Information than that is legally required;
- To comply with valid legal proceedings such as search warrants, subpoenas or court orders;
- During emergency situations or when necessary to protect the safety of a person or Thera's premises or assets; or
- When the Personal Information is already publicly available at the time of disclosure.

## 7.3 Specific Permitted Disclosure under Quebec Private Sector Act

Thera may, without the consent of an Individual, communicate the Personal Information to the following:

- To a person or body with the power to compel the disclosure of Personal Information and who requires it in the course of his or her duties;
- To a person who must receive the Personal Information because of an emergency that threatens the life, health or security of an Individual, or to whom Thera may disclose the information to prevent an act of violence, including suicide, if there is a serious risk of death or serious injury to an Individual;

- To any person, if the Personal Information is more than 100 years old or if the Individual concerned has been dead for more than 30 years;
- To a person or organization for the purposes of a mandate or contract for services or contract of enterprise;
- To the other party to a business transaction if the disclosure is necessary to complete the transaction;
- To a person who may use it for study, research or statistical purposes or to a person authorized by the *Commission d'accès à l'information* to use it;
- To a person who is authorized by law to collect debts for others and who requires it for that purpose in the course of his or her duties; and
- To a person if the Personal Information is required for the purpose of collecting a debt owed to Theratechnologies.

Thera will maintain a record of the foregoing disclosure of Personal Information.

## 7.4 Transfer of Personal Information outside the EU / European Economic Area ("EEA") or Quebec

Transfer of Personal Information outside of the EU/EEA or Quebec, within Thera or to third parties, is acceptable:

**a.** If in the United States, the third party receiving Personal Information is part of the EU-U.S. Data Privacy Framework. For a full list of participating companies please consult: https://www.dataprivacyframework.gov/s/participant-search

**b.** If outside Canada or the United States, the country has been recognized as offering an adequate legal privacy framework by the EU Commission. For the full list of countries offering an adequate legal privacy framework, please consult: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en and https://www.cnil.fr/en/data-protection-around-the-world.

**c.** Where a country's legal privacy framework is not considered adequate, a Transfer Impact Assessment ("**TIA**") under the GDPR or a Privacy Impact Assessment ("**PIA**") under the *Quebec Private Sector Act* needs to be conducted prior to the transfer of Personal Information.

- A TIA or PIA essentially aims to assess the impact that a transfer to a country outside the EU/EEA or outside Quebec may have on the protection and safeguarding of the Personal Information and on the privacy rights of the Individuals.
- The first part of the assessment involves an analysis of the laws, practices and public authorities in place in the receiving jurisdiction in order to determine whether anything in such jurisdiction would have a negative impact on the effectiveness of the measures relied upon to ensure the protection of the Personal Information.
- The second part of the TIA or PIA involves an analysis of the nature of the Personal Information being transferred (in particular, whether it is Sensitive Information or not) and the security measures implemented. The measures referred to herein being for example, under the GDPR, the European Commission's so-called Standard Contractual Clauses ("**SCCs**").
- If the TIA or PIA reveals that there is no risk for the Personal Information of the Individuals, the transfer can occur with appropriate safeguards such as the above-

mentioned SCCs or a written agreement in Quebec, encryption of the information and application of the Data Minimization Principle.

- If the conclusion of the TIA or PIA is that the security of the Personal Information would not be guaranteed, the transfer should not occur.

Thera Employees contemplating the transfer of Personal Information should always consult with privacy@theratech.com prior to proceeding with any such transfer.

### 7.5 Other Situation Where a PIA is Needed

Under the supervision of the Privacy Officer, Thera will need to conduct a PIA in the following situation:

- Prior to undertaking any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of Personal Information; and

- Before disclosing Personal Information without consent to a person or organization that wishes to use the information for study, research or statistical purposes. In this particular situation, the request must be submitted to Thera's Privacy Officer. If the conclusion of the PIA is that Personal Information may be disclosed for the above-mentioned purposes, Thera shall enter into a written agreement and such agreement shall include the mandatory content of the legislation (as mentioned in section 7.2a and any additional protection measures identified in the PIA.

While conducting the PIA, Thera will consider if the Personal Information to be Processed is sensitive or not, the Purposes for which it will be used, the quantity, the means of distribution and the medium on which the Personal Information will be stored.

The completion of a PIA serves to demonstrate that Thera has taken the necessary steps to ensure the effective protection of the Personal Information.

## 8. RETENTION OF PERSONAL INFORMATION

Personal Information will always be retained in accordance with Applicable Privacy Laws and any other applicable laws (including, for the purpose of meeting any legal, accounting or other reporting requirements or obligations or for the purposes of establishing or defending potential legal claims), as outlined in Thera's retention calendar.

Except when legally permissible, Thera will retain Personal Information only for as long as it is necessary to fulfill the Purpose for which it was collected.

Once the Purpose of Processing Personal Information has been fulfilled, Thera will destroy or archive the Personal Information, or, if there is a serious and legitimate reason to do so, anonymized the Personal Information in accordance with Applicable Privacy Laws. The anonymized information will be stored in a different cold archive created on a need basis and will only be accessible if necessary and related to the initial Purpose of Processing. Personal Information, which is still of administrative interest to a business department (e.g., legal department) will be saved on a file server management software. Such Personal information should only be accessible on a "need to know" basis and kept for as long as prescribed in Thera's retention calendar. Only Personal Information of historical, scientific or statistical interest justifying

its retention may be stored for an indefinite period of time in the cold database. Any Employee wishing to anonymize Personal Information should make a request to privacy@theratech.com.

## 9. ACCURACY OF PERSONAL INFORMATION

Personal Information used by Thera is kept as accurate and complete as reasonably possible to minimize the possibility that a decision affecting an Individual be made based on inaccurate information. If the use of incorrect Personal Information may harm an Individual or Thera, it is essential that measures to verify the accuracy and completeness of such Personal Information be implemented prior to its use or disclosure.

If Personal Information is susceptible of being inaccurate or outdated, Employees must take note of the possible inaccuracy and inform others who may use such Personal Information. Where feasible, Thera will take appropriate measures to ensure that the Personal Information is updated to meet the above accuracy standard, such as conducting an annual review of the database.

Individuals who have provided Personal Information are encouraged to inform Thera of any necessary update concerning their Personal Information.

Each Employee shall be responsible to ensure that Personal Information Processed by Thera regarding him/her is accurate at all times.

## 10. SECURITY OF PERSONAL INFORMATION AND DATA BREACH

### 10.1 General Safeguards and Security

**a. Security Standard.** Thera shall implement and maintain security safeguards to protect Personal Information, regardless of the format in which it is held, against loss, theft, or unauthorized collection, use or disclosure (including unauthorized access, copying, or modification). These security safeguards must be appropriate with respect to the nature, the amount, the means of distribution, the format and the method of storage of the Personal Information.

**b. Security Methods.** The methods of protection include:

(i) Physical measures, for example, restricted access to Thera's premises and IT systems;
(ii) Organizational measures, for example, limiting access on a "need-to-know" basis; and
(iii) Technological measures, for example, the use of passwords and encryption, malware defenses, use of file server management software to provide audit trails of any access.

### 10.2 Secure Destruction, Archiving or Anonymization

**a. Destruction Standard**. Once the retention period of Personal Information has elapsed (in accordance with Thera's retention calendar), Thera will either destroy, archive or anonymized the Personal Information in accordance with Section 8 of this Policy.

**b. Destruction Methods**. Thera will apply the following principles with respect to destruction and archive of Personal Information:

(i) Personal information in a paper format will be destroyed by crosscut shredding;

(ii) Documentation containing Personal Information will not be placed in waste bins, unless that waste is subsequently crosscut shredded, and the information is secured from unauthorized access pending destruction; and
(iii) Electronic storage media will be subject to industry standard secure deletion software or techniques.

### 10.3 Privacy Breaches

A data breach or "**Confidentiality Incident**" is any (potential) breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Information that is Processed by Thera, as well as any other breach of the protection of such information.

Preventing a Confidentiality Incident is the responsibility of all Employees. Any Employee suspecting a violation of this Policy or an irregularity in relation to Personal Information Processing activities shall inform without delay his supervisor and the Privacy Officer at privacy@theratech.com.

**Contractual Obligations.** For insurance purposes, Thera may be subject to contractual obligations regarding how it must respond to Confidentiality Incident involving an Individuals' Personal Information, including who is to be notified, and how the notification is to occur, these requirements may supplement or deviate from this Policy. In exceptional circumstances, Thera may not notify the affected Individual until it has determined together with the insurance provider whether it is subject to specific requirements. The Privacy Officer will be responsible to determine whether any such contractual or legal obligations exist.

**Notice to Individuals and Regulatory Authorities.** The requirements to notify a Regulatory Authority or affected Individuals will be determined by the Privacy Officer. Thera may, on its own initiative, notify affected Individuals or organizations of any Confidentiality Incident, particularly when the breach gives rise to a real risk of significant harm to the affected Individuals or organizations. The Privacy Officer shall determine the content of any such notice.

**Record-keeping**. Thera will maintain a record of every Confidentiality Incident for at least five (5) years following any breach.

## 11. INDIVIDUALS' RIGHTS

Individuals have various legal rights pertaining to their Personal Information, such as:

- The right to gain access to the Personal Information that Thera holds about them;
- The right to rectification, meaning the right to request the correction, without undue delay, of any Personal Information that Thera holds about them and is either inaccurate or incomplete;
- The right to withdraw consent to the Processing of their Personal Information; and
- In addition to the above, Individuals have the right to file a complaint with the relevant Regulatory Authority.

Under the GDPR, additional rights are granted to Individuals in certain circumstances, such as:

- The right to obtain the erasure of their Personal Information, without undue delay, provided that the Personal Information is no longer necessary for the Purpose for which it was collected;

- The right to data portability, which means the right to request that Thera sends their Personal Information in a structured, commonly used and machine-readable format, and to receive such Personal Information;
- The right to restriction, according to which an Individual is entitled to ask Thera to suspend the Processing of certain Personal Information about them, for example to establish its accuracy or the reason for Processing it; and
- The right to object, which means that an Individual may challenge if Thera is Processing Personal Information based on a legitimate interest (or those of a third party) or for direct marketing purposes. However, under certain circumstances, Thera may be entitled to continue Processing the Personal Information.

Under the *Quebec Private Sector Act*:

- An Individual has the right to request the cessation of the dissemination of its Personal Information or the de-indexation of any hyperlink attached to his/her name and allowing access to that Individual's Personal Information when the dissemination of the Personal Information contravenes the law or a court order. Individuals may also request the de-indexation when the dissemination of the Personal Information causes them harm; and
- The right to contest any decision based exclusively on an automated Processing of their Personal Information where such decision has a legal or similar significant effect and ask for the decision to be reconsidered.

When requested, Employees must provide a comprehensive way for Individuals to exercise any of the above-mentioned rights or inquire about Thera's Processing of their Personal Information.

**PROTECTION OF MINORS**

Thera may collect Personal Information from Minors. As used herein "**Minors**" shall mean children under 16 years of age for EU residents or under 14 years of age for residents of Quebec. Minors merit specific protection, as they may be less aware of their rights or the risks involved with respect to the Processing of their Personal Information.

A Minor's consent must be provided by his/her parents or other legal representatives before any Processing of Personal Information. When feasible, a Minor should be able to participate in the decision to allow Processing of his/her Personal Information. If Thera learns that Personal Information has been collected directly from a Minor without verifiable parental consent, then Thera will take the appropriate steps to delete this Personal Information.

Given that Minors merit specific protection, any communication related to the Processing of a Minor's Personal Information should be in such a clear and plain language that the Minor can easily understand the consequences thereof. The validity of the consent is inextricably linked to the quality of the information given about the Purpose of the Processing.

If requested, Thera should enable a Minor to access its Personal Information in an easily readable format and allow for rectification and erasure.

Minors also have a right to request access, rectification, and erasure of their Personal Information. Minors must be able to withdraw their consents in an easy way, without any negative consequences in relation to the use of services or product from Thera.

## 12. TRAINING

Upon joining Thera, every new Employee must complete a cybersecurity awareness training and mandatory training is provided to every Employee on the importance of safeguarding the confidentiality of Personal Information.

## 13. CONTACT US

### 13.1 Contact Information

All comments, questions, concerns regarding Personal Information or our privacy practices should be sent to Thera's Privacy Officer as follows:

Address: Attention: Privacy Officer & Data Protection Officer
Jocelyn Lafond
General Counsel & Corporate Secretary, acting as Privacy Officer & Data Protection Officer
Theratechnologies Inc.
2015 Peel Street, 11th Floor
Montréal, Québec
Canada H3A 1T8

By e-mail: privacy@theratech.com

### 13.2 Complaints

The Privacy Officer will independently investigate all complaints and allegations of violations of this Policy.

The Privacy Officer will:

- Clarify the complaints to identify the source of the issues;
- If necessary, communicate with the plaintiff to gather sufficient evidence;
- Conduct an analysis of the information obtained during the investigation; and
- Determine the best approach for dealing with the matter and whether corrective actions are required.

Any person who violates this Policy will be subject to disciplinary action.

## 14. IMPLEMENTATION AND REVISION OF THIS POLICY

Thera may, from time to time, make changes to this Policy to reflect changes in its legal or regulatory obligations or in the manner in which it deals with Personal Information.

This Policy shall be deemed effective as of September 20, 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorized by:

| | |
|---|---|
| **Name:** | Jocelyn Lafond |
| **Position:** | General Counsel & Corporate Secretary, also acting as Privacy Officer & Data Protection Officer |
| **Due for Review by:** | September 20, 2025 |

Document Review History

| Version | Effective Date | Author | Summary of Changes |
|---|---|---|---|
| 01 | 20-Sept 2023 | Privacy Officer / Data Protection Officer | |