Terumo Malaysia Sdn Bhd ("TMSB")

Classification: Standards

Subject : Malaysia Privacy and Personal Information Protection Policy	
Policy No: TAP-025-003	Effective Date: 01-JUL- 2025
Policy Owner: Legal Department	Approved by: Hock Lin Tan, Regional Director, Legal & Compliance

Contents

Chapter I General Rules

1. Purpose

1.1 Creating excellent products and services through utilization of data is essential for the growth of Terumo's business. By doing so, Terumo may make even better contribution to society. On the other hand, increase of utilization of personal data gives various impact to privacy and right and freedom of individuals, and furthermore, to society. Therefore, many countries have data privacy laws to regulate how personal information is collected, used, stored and dispose of, how data subjects are informed, and what control a data subject has over his/her information. Taking action with due consideration of impact to individuals and society according to the types of utilization of personal data, beyond just complying with legal requirements, will help Terumo win trust from society and achieve sustainable growth while we expand our business by active utilization of personal data. Therefore, the Terumo Group Code of Conduct provides that associates should handle personal information with care and respect confidentiality and should protect it when processing personal information.

1.2 The Group Privacy and Personal Information Protection Policy has been established to set forth the basic requirements to be observed in the processing of Personal Information by Terumo entities (herein individually or collectively referred to as "Terumo").

1.3 This policy has been established under the Group Privacy and Personal Information Protection Policy to set forth the basic requirements to be observed in processing of Personal Information by Terumo entities incorporated under the laws of Malaysia.

2. Scope

2.1 This policy and its supplemental rules (collectively, the "Policy") applies to all Personal Information processed by Terumo entities incorporated under the laws of Singapore, including Sensitive Information, and applies to all Associates and independent contractors allowed to use Terumo IT system/intranet who process Personal Information for or/and on behalf of Terumo entities incorporated under the laws of Singapore.

3. Priority

3.1 The Group Privacy and Personal Information Protection Policy and its supplemental rules which may be implemented by the Chief Legal Officer (collectively, the "Group Policy") determines the minimum standards to lawfully process and protect Personal Information in Terumo. Accordingly, any Personal Information protection standards outlined by any policies and associated instruments (e.g., procedures and

guidance) implementing or supplementing the Group Policy of any Regional Unit or entity shall be consistent with the Group Policy.

3.2 Personal Information protection standards of any entity shall be consistent with the Personal Information protection standards of the Regional Unit where the entity is located.

3.3 When the Applicable Law provides for stricter standards than this Policy, the Applicable Law shall prevail to that extent. On the other hand, in the event that the Applicable Law provides standards that are less strict than this Policy or there are no Applicable Law, this Policy shall apply.

3.4 This Policy is written in both English and Malay, and in case of any discrepancy, the English version shall prevail.

4. Definitions

4.1 The terms used in this Policy have the following meanings:

(1) (1) "Applicable Law" means laws of the country or region where the Data Subject resides, or the laws of the country or region where the Controller or the Processor, as the case may be, resides, or both. The law of the country or region where the Data Subject resides becomes Applicable Law in the event that such law applies outside the country or the region by an extraterritorial provision (i.e., a provision to apply such law outside the country or region) included in such law. In Malaysia, the Applicable Law includes the Personal Data Protection Act 2010 (as amended) (the "PDPA") and related ordinances and regulations..

(2) "Associate" means an associate as defined in the Terumo Group Code of Conduct.

(3) "Controller" means the person or organization that determines when, why and how to process Personal Information.

(4) "Cross-border Transfer" means the transmission or disclosure of Personal Information to a different jurisdiction or reference to Personal Information from a different jurisdiction.

(5) "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise

processed that could compromise the confidentiality, integrity, or availability of the Personal Information.

(6) "Data Subject" means a living, identified or identifiable individual who holds Personal Information. Data Subject may be a national or resident of any country or territory and have legal rights regarding its Personal Information.

(7) "Disclosure" means transfer of Personal Information and transmission of Personal Information to a third party, including the providing of reference to and use of Personal Information to a third party.

(8) "Information Security Function" means associates or organizations who/which are responsible for designing and deploying security control that protect the confidentiality, availability, and integrity of confidential, personal or sensitive data from threats and vulnerabilities.

(9) "Legal Associate" means an associate who belongs to the legal department or who has responsibilities for legal matters.

(10) "Personal Information" means information that can directly or indirectly identify a natural person (including online identifiers that can identify a natural person), such as name, date of birth, contact information, address, identification card number, email address, photograph, biometric information, etc.

(11) "Privacy Office" means an organization established, as necessary, at a global level and/or at a Regional Unit level and/or at an entity level to manage protection of privacy and Personal Information.

(12) "Process," "processing," or "processed" means any activities that involve the use of Personal Information, including the collection, recording, storage, or organization of Personal Information, structuring, correction, modification, restoration, consultation, transfer, retention, retrieval, use, disclosure, erasure, or deletion of Personal Information.

(13) "Processor" means an organization or person who processes Personal Information for or on behalf of Controller and in accordance with Controller's direct instructions. It may be called "vendor" or "service provider" in business terms.

(14) "Regional Legal Representative" means one person appointed by the

Chief Legal Officer for each Regional Unit among the associates who belong to the legal departments of the entities in each Regional Unit.

(15) "Regional Unit" means each of Japan, Greater China, the rest of Asia/India/Oceania, Europe/UK/Middle East/Africa, and North America/Latin America.

(16) "Sensitive Information" means Personal Information as to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person. (Examples: physical disability, intellectual disability, mental disability (including developmental disorders), results of medical checkup and other examinations conducted by medical doctors for prevention or early finding of diseases, the fact that medical doctors, etc. gave instructions or diagnosis or prescription for medicines to improve physical or mental conditions, the fact that criminal proceeding such as arrest, search, seizure, detention or prosecution was conducted, the fact that protection proceeding for minors such as investigation, monitorship, judgment, protection order.

(17) "Third Party" means any person or organization (corporation, industry group, government agency, etc.) other than Data Subjects, Terumo and Processors. A Terumo entity is treated as a Third Party when any Personal Information is disclosed or transferred to that entity.

Chapter II Organization and Responsibility

5. Privacy governance

5.1 In order to practice Terumo's view to the proper handling of privacy and Personal Information, Terumo nominates a person with comprehensive responsibility for it and assigns Terumo Corporation's Chief Legal Officer to such position.

5.2 Furthermore, Terumo establishes Privacy Office to facilitate protection of privacy and Personal Information. Privacy Office shall be cross-functional to enable multilateral examination and efficient operation. Legal and Information Security Function are the core functions but associates in other functions such as HR and business units may be added, as necessary. In respect of legal function, Regional Legal Representative is nominated for each Regional Unit for the purpose of facilitating implementation of integrated measures effectively and efficiently based on the consideration of legal requirements in the Regional Unit.

5.3 Privacy Office shall organize internal structure to be ready to demonstrate documents and other proof of compliance with the Applicable Law in response to the request by the competent data protection authorities.

6. Role and responsibility of departments and associates who process Personal Information

6.1 Head of each department processing Personal Information shall properly manage the department so that its business operation and products/services it deals with do not cause a breach of privacy or a violation of the Applicable Law, this Policy or any other internal rules, and take measures necessary for the proper management of privacy and Personal Information including security measures.

6.2 All associates and independent contractors who are subject to this Policy shall conduct business with due care to protect privacy and Personal Information in accordance with the Applicable Law, this Policy and any other internal rules when they conduct business processing Personal Information.

Chapter III Processing of Personal Information

Section 1. Principles for Processing Personal Information

When processing Personal Information (either directly or by Processor), associates shall ensure the processing respects the following key information protection principles in this Section 1.

7. Personal Information protection by design and default

7.1 Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing: associates need to integrate Personal Information protection into all processing activities and business practices (such as designing and planning new operations, products, and services, and updating existing operations, products, and services) from the design stage right through the lifecycle of the processing activity ("data protection by default"); and also need to implement all appropriate technical and organizational measures in an effective manner to ensure compliance with the Applicable Law and this Policy ("data protection by design").

8. Lawfulness, fairness and transparency principle

8.1 Associates may only process Personal Information in so far as they have a clear and defined legal basis. An acceptable legal basis can be one of the following:

(1) *Intentionally left blank.*

(2) Contractual necessity: the processing is necessary in view of the conclusion or performance of a contract with the Data Subject.

(3) Compliance with legal regulations: the processing is necessary to comply with legal obligations.

(4) Intentionally left blank.

(5) Other legal basis: the processing the Applicable Law explicitly allows without consent of the Data Subject.

(6) Consent: If there is no legal basis provided in any of (1) through (5) above, a consent for one or more specific purposes must be obtained from the Data Subject. The consent shall satisfy the conditions of "being given with free will", "based on sufficient prior information", "a clear statement of the Data Subject's consent to the processing of the Personal Information relating to him or her, either by language or by clear positive action", and being capable of being recorded and maintained.

8.2 Personal Information shall not be processed in a way unjustly detrimental, unexpected or misleading to the people concerned.

8.3 It should be transparent to the Data Subjects that Personal Information concerning them are collected, used or otherwise processed and to what extent the Personal Information is or will be processed.

9. Processing of Sensitive Information principle

9.1 Any restrictions under the requirements of the Applicable Law for processing the Sensitive Information need to be understood and fully complied with when processing the Sensitive Information.

9.2 Associates shall not process Sensitive Personal Information without explicit consent of the Data Subject, except when such consent is not required under the Applicable Law.

10. Purpose limitation principle

10.1 Personal Information must be collected only for specified, explicit and legitimate purposes. Associates shall be as clear as possible from the start why they are

collecting Personal Information and what they intend to do with it.

10.2 Associates shall not reuse Personal Information in a manner that is incompatible with the purpose for which it was collected, except with the consent of the Data Subject or it is lawful under the Applicable Law.

11. Proportionality and data minimization principle

11.1 The collection and processing of Personal Information by associates shall be limited to that which is necessary for the purposes deemed legitimate.

12. Quality and accuracy principle

12.1 Associates shall endeavor to keep Personal Information accurate and up to date by regular checks and other means.

13. Security, integrity and confidentiality principle

13.1 Terumo establishes and maintains appropriate technical and organizational measures to protect against unauthorized access, loss, leakage, damage or falsification of Personal Information, that are appropriate for the nature and sensitivity of the information.

14. Retention, storage and disposal principle

14.1 Associates shall ensure that Personal Information is not stored for a period longer than is necessary for the purpose of the processing, except as required by the Applicable Law or as may be required to protect a known interest of the Data Subject. When that period has lapsed, associates shall properly destroy or delete the Personal Information, depending on the type of storage media.

Section 2. Activities for Processing Personal Information

15. Record keeping

15.1 Associates shall endeavor to maintain complete and accurate records of Personal Information processing activities.

16. Privacy impact assessment

16.1 Associates shall conduct privacy impact assessment when it is required by the Applicable Law or when they intend to carry out events which give impact to privacy such as development of new products/services, commencement of new processing of Personal Information and building or altering IT system.

17. Associate training

17.1 Associates who process Personal Information shall take training on personal information protection at least once a year.

18. Internal monitoring

18.1 To ensure that the Applicable Laws and internal rules regarding the protection of Personal Information are being observed and that Personal Information is being managed appropriately, it is necessary to conduct internal monitoring on a regular basis.

18.2 If the internal monitoring identifies a failure to comply with the Applicable Law or this Policy or any other internal rules regarding protection of Personal Information, the associate(s) responsible for the failure shall discuss the failure with Legal Associates and take measures to correct the failure.

Section 3. Processors and Third Parties

19. Selection of Processors

19.1 Prior to entering a contract for processing Personal Information with any Processor who is outside Terumo, associates shall ensure that the Processor provides sufficient guarantees and technical and organizational measures that will allow the protection of the rights of the Data Subject. Processors must be selected carefully based on their expertise and approach relating to privacy and in accordance with the designated selection criteria.

20. Execution of contracts with Processors

20.1 Prior to requesting processing any Personal Information by any Processor who is outside Terumo, associates shall execute a written contract ("data processing agreement") with the Processor.

21. Monitoring of Processors

21.1 According to the risk level of Personal Information processing, associates shall monitor the compliance status of the Processor (outside Terumo) during the contract period. The results of the monitoring shall be documented.

22. Disclosure of Personal Information to Third Parties

22.1 In principle, Disclosure of Personal Information to Third Parties is prohibited. However, Disclosure to Third Parties is permissible if there is a legal basis for such Disclosure, or if such Disclosure is permitted or required under the Applicable Law, court decree, or other legal basis.

22.2 "Third Parties" in 22.1 includes Terumo entity. Therefore, associates shall ensure, prior to Disclosing Personal Information to a Terumo entity, that there is a legal basis for such Disclosure, or that such Disclosure is permitted or required by the Applicable Law, court decree or other legal basis. If the Disclosure is to a Terumo entity in another jurisdiction, it is qualified as Cross-border Transfer and additional requirements may apply depending on the countries or regions involved as are set out in Section 4.

Section 4. Cross-Border Transfer

23. Cross-border Transfer

23.1 In the event of Cross-border Transfer, a lawful and appropriate transfer measure (e.g., agreement, intragroup framework agreement, adequacy decision) with the transferee or re-transfer recipient shall be in place.

23.2 In addition, if there is a change in the original legal basis or purpose after the transfer, the Data Subject shall be notified of the necessary information related to the Cross-border Transfer again and the consent of the Data Subject shall be obtained, if required under the Applicable Law.

23.3 It shall not be considered a Cross-border Transfer where Personal Information of Data Subjects has been transferred, processed and stored overseas but the possession or control of such Personal Information has not been relinquished to Third Parties.

Section 5 Response to Data Subjects

24. Data Subjects rights

24.1 When associates receive a request from a Data Subject to exercise his/her rights about his/her Personal Information, associates shall take timely and appropriate action, after consulting with Legal Associate (or Privacy Office).

24.2 To ensure legal, proper and transparent processing of Personal Information, Terumo establishes and follows procedures to realize Data Subjects' rights granted by the Applicable Law.

25. Privacy notice

25.1 When associates collect Personal Information directly from a Data Subject or indirectly (e.g., from a Third Party or publicly available source), they shall inform the Data Subject about the processing of the Data Subject's Personal Information unless the Applicable Law provides such information is not required.

25.2 The notice provided to the Data Subject shall be concise, transparent, understandable, and written in clear and plain (and, in principle, local) language so that Data Subject can understand it easily.

26. Response to complaints and inquiries

26.1 When receiving a complaint or an inquiry from a Data Subject regarding the processing of Personal Information by Terumo, associates shall provide an appropriate response.

26.2 Terumo shall provide the Data Subject with contact information for receiving complaints and inquiries regarding Personal Information from the Data Subject.

Section 6. Data Breach

27. Response to a Data Breach

27.1 A Data Breach can cause significant information security and privacy risks. In addition, certain laws impose duty to notify Data Breach to competent authorities and/or affected Data Subjects by a strict deadline. Therefore, associates shall report to the Legal Associate (or to a specified reportee, such as the Privacy Office or Data Protection Office) when he/she becomes aware of, or has a reasonable suspicion of, any Data Breach.

27.2 To ensure timely handling of a Data Breach, Terumo establishes procedures to handle Data Breach. It is critical that each associate and Processor processing Personal Information for or on behalf of Terumo follows the requirements of the applicable procedures.

Chapter IV Miscellaneous Rules

28. Penalty

28.1 If an associate violates this Policy intentionally or negligently, he/she may be disciplined in accordance with the relevant internal rules.

29. Owner

29.1 The Group Policy is owned by CLO Office, Terumo Corporation.

29.2 This Policy is owned by APAC Regional Legal Representative.

30. Revisions

30.1 Process for revision or abolition

30.1.1 Revision or abolition of the Group Policy shall be done pursuant to the Group Policy of Group Policy Management.

30.1.2 Revisions or abolition of this Policy shall be proposed by the APAC Regional Legal Representative and decided after discussion with the Chief Legal Officer and the Legal Associates.

30.1.3 Revisions or abolition of the entity's policies and/or associated instruments shall be proposed by the Legal Associates and shall be approved in accordance with the internal approval procedures of the entity after prior discussion with the APAC Regional Legal Representative and the Chief Legal Officer.

30.2 Where revision is required

30.2.1 When laws and regulations of a major region or country are enforced or significantly revised, the Chief Legal Officer shall carefully review such laws and regulations and reflect, as necessary, the requirements in the Group Policy.

30.2.2 When laws and regulations of Malaysia are enforced or significantly revised, the APAC Regional Legal Representative shall carefully review such laws and regulations and reflect the requirements, as necessary, in this Policy and/or associated instruments. When the Group Policy is revised, such revision shall be reflected in this Policy and/or associated instruments.

30.2.3 When laws and regulations of Malaysia are enforced or revised, the APAC Regional Legal Representative or Legal Associate in charge of the Malaysian entity shall carefully review such laws and regulations and reflect, as necessary, their requirements in the entity's policies and/or associated instruments. When this Policy and/or associated instruments are revised, such revision shall be reflected in the entity's policies and/or associated instruments.

Rev	Date	Description of change	Revised by
0	1 July 2025	Initial version	THL