Terumo Asia Holdings Pte. Ltd ("PTTI")

Classification: Bye Laws

Subject : Indonesia Supplemental Rules for Privacy and Personal Information Protection Policy	
Policy No: TAP-025-002	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 This document is prepared to supplement the Indonesia Privacy and Personal Information Protection Policy (the "Indonesia **Policy**").

1.2 This document is evolving document and may be revised by the APAC Regional Legal Representative from time to time.

2. Scope

2.1 This document applies to all Personal Information processed by Terumo entities incorporated under the laws of Indonesia 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 Indonesia.

3. Priority

3.1 This document has the same priority as the Indonesia Policy. If there is any discrepancy between the Indonesia Policy and this document, the Indonesia Policy shall prevail.

4. Definitions

4.1 Unless otherwise defined in this document, the terms defined in the Indonesia Policy have the same meanings when used in this document.

Chapter II Organization and Responsibility

5. Privacy governance

See Annex 1 for responsibilities of departments and associates composing privacy governance and role of privacy office.

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

Chapter III Processing of Personal Information

Section 1. Principles for Processing Personal Information

7. Personal Information protection by design and default

8. Lawfulness, fairness and transparency principle

9. Processing of Sensitive Information principle

10. Purpose limitation principle

11. Proportionality and data minimization principle

12. Quality and accuracy principle

13. Security, integrity and confidentiality principle

14. Retention, storage and disposal principle

Section 2. Activities for Processing Personal Information

15. Record keeping

15.1 In order to ascertain the actual status of the processing of Personal Information and to regularly confirm that appropriate management is being carried out, it is necessary to record certain items for each activity in which Personal Information is processed. For details of each item, refer to the Data Mapping Manuals on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html).

16. Privacy Impact Assessment

16.1 Overview of PIA Implementation

16.1.1 Privacy impact assessment (PIA) is a process designed to help us systematically analyze, identify and minimize the data protection risks of a project or plan. It does not have to eradicate all risk, but should help us minimize and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve. PIA should begin early in the life of a project, before we launch a new processing, and run alongside the planning and development process.

16.1.2 PIA shall be conducted for the following processing regardless of whether any Applicable Law requires it or not, if it is likely to result in a high risk to rights and freedoms of individuals:

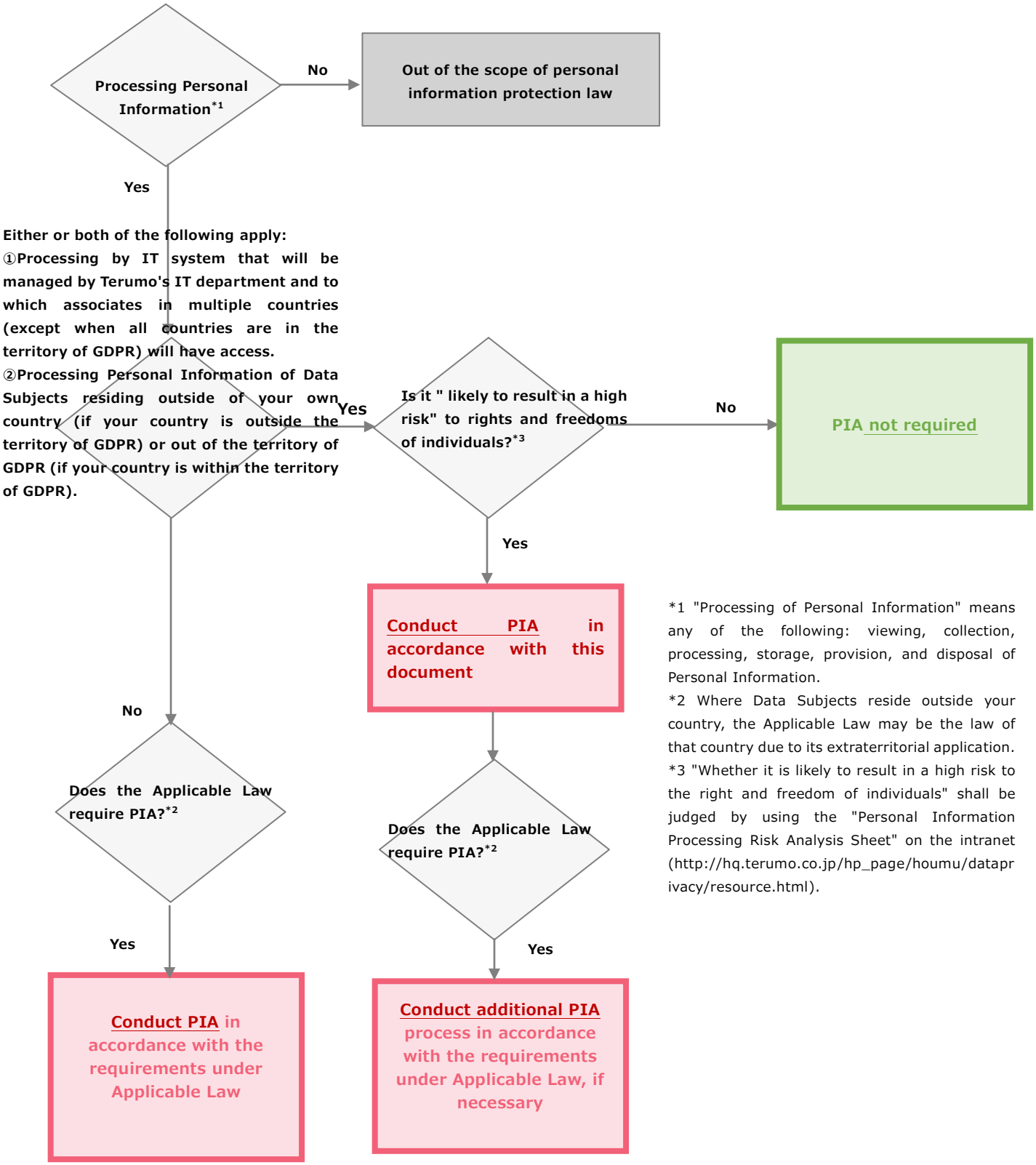
(i) Processing by IT systems that will be managed by Terumo's IT departments and to which associates in multiple countries (except when all countries are within the territory of GDPR) will have access; and

(ii) Processing of Personal Information of the Data Subject residing out of your country (if your country is outside the territory of GDPR) or out of the territory of GDPR (if your country is within the territory of GDPR).

16.1.3 In such case, PIA shall be carried out as per the process set forth in this document. However, if any Applicable Law requires PIA for the above processing, additional PIA process may be required under the Applicable Law. The project owner shall consult with the Legal Associate to ask whether such additional process is required under the Applicable Law.

The Legal Associate, if necessary, shall contact the Regional Legal Representative of a Regional Unit covering the country where the Data Subjects reside to discuss if additional process is required by the Applicable Law of such country.

16.1.4 If the Applicable Law requires PIA for other processing of the Personal Information, PIA shall be conducted in accordance with the Applicable Law. Process should be established by regional or entity's policy or related instruments to make sure that such PIA is conducted in a compliant manner.



*1 "Processing of Personal Information" means any of the following: viewing, collection, processing, storage, provision, and disposal of Personal Information.

*2 Where Data Subjects reside outside your country, the Applicable Law may be the law of that country due to its extraterritorial application.

*3 "Whether it is likely to result in a high risk to the right and freedom of individuals" shall be judged by using the "Personal Information Processing Risk Analysis Sheet" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html).

16.2 PIA analysis

16.2.1 Risk assessment

Prior to the processing which falls in either/both of the following cases, the project owner needs to determine whether it is "likely to result in a high risk" to rights and freedoms of individuals with the criteria listed in the "Personal Information processing Risk Analysis Sheet" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html). If two or more of the criteria are met, the processing is "likely to result in a high risk" and PIA needs to be conducted according to the process described in this document:

(i) Processing of Personal Information by IT system that will be managed by Terumo's IT departments and to which associates in multiple countries (except when all countries are within the territory of GDPR) will have access; and

(ii) Processing of Personal Information of the Data Subject residing out of your country (if your country is outside the territory of GDPR) or out of the territory of GDPR (if your country is within the territory of GDPR).

16.2.2 Preparation

PIA should start as early as is practicable in the design of the processing even if some of the processing operations are still unknown. The owner of the project to launch the above processing ("**project owner**") takes initiative in PIA. For a preparation, the project owner should do the following things:

(i) Check or collect relevant Applicable Law, guidelines, internal rules, internal documents, etc.,

(ii) Check or collect materials related to system development (requirement definition document, design document, etc.) (if system is related),

(iii) Understand the flow of Personal Information for each process, such as collection, storage, transfer, use, and disposal, and

(iv) Identify stakeholders (contractors, other departments, etc.) and involve them in the plan.

The project owner may nominate a responsible person (or a team) to carry out PIA.

16.2.3 Basic principles check

The project owner completes "①Description of Project" and "②Basic Principles" of the "PIA Sheet" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html) to describe the outline of the processing and to check whether the basic principles in processing Personal Information are (or will be) satisfied, and submits them to Legal Associate for review. The project owner interviews the relevant stakeholders who will process Personal Information, if necessary.

16.2.4 Security controls check

If the processing uses IT system, the project owner also fills out "③Security Controls" of the "PIA Sheet" to check whether appropriate security control to protect Personal Information is (or will be)

in place. The project owner submits the completed "③Security Controls" to the Information Security Function for review.

16.2.5 Review and feedback

<Legal Associate>

Legal Associate reviews "①Description of Project" and "②Basic Principles" completed by the project owner and provides, if necessary, advice for improvement. Legal Associate writes down such advice in "②Basic Principles" and sends it back to the project owner.

<Information Security Function>

Information Security Function reviews "③Security Controls" completed by the project owner and provides, if necessary, advice for improvement. Information Security Function writes down such advice in "③Security Controls" and sends it back to the project owner.

16.2.6 Response to the feedback

The project owner reviews advice provided by Legal Associate and/or Information Security Function and decides whether it follows or overrule the advice. When the project owner decides to follow the advice, it writes down the corrective measures in "②Basic Principles" and/or "③ Security Controls" and re-submitting it to Legal Associate and/or Information Security Function. If the project owner decides to overrule the advice provided by Legal Associate and/or Information Security Function, it writes down the reasons in "②Basic Principles" and/or "③Security Controls" and re-submitting it to Legal Associate and/or Information Security Function.

Legal Associate and/or Information Security Function reviews the corrective measures and evaluates whether they are "unsatisfactory" or "acceptable". Legal Associate and/or Information Security Function notes such evaluation in "②Basic Principles" and/or "③Security Controls" and sends it back to the project owner.

16.2.7 Risk assessment

If the project owner decides to overrule the advice provided by Legal Associate and/or Information Security Function or the evaluation by Legal Associate or Information Security Function is "unsatisfactory", the project owner needs to assess risks to rights and freedoms of Data Subjects. In this assessment:

(i) sources of risks need to be taken into account;

(ii) nature of potential impacts to the rights and freedoms of Data Subjects needs to be identified in case of illegitimate access, undesired modification and disappearance of data;

(iii) threats that could lead to illegitimate access, undesired modification and disappearance of data need to be identified;

(iv) likelihood and severity needs to be estimated;

(v) the likelihood that the proposed collection, use or disclosure of the data of a Data Subject will have an adverse effect on a Data Subject; and

(vi) determine whether the collection, use or disclosure of personal data about a Data Subject is in the legitimate interests of Terumo Indonesia entities or another person and whether the legitimate interests of the Terumo Indonesia entities or other person outweigh any adverse effect on the Data Subject.

Unless the overall risks are negligible, the project owner considers additional measures to reduce or eliminate such risks and identify the residual risks after taking the additional measures.

To document this risk assessment, the project owner completes "④Risk Assessment" of the "PIA Sheet" and shares it with Legal Associate and Information Security Function.

16.2.8 Conclusion and communication

To conclude PIA, the project owner records the name and title of the approver of the measures to reduce or eliminate risks and residual risks in "⑤Conclusion".

The project owner does not always have to "eliminate" every risk. The project owner may decide that some risks, and even a significant or maximum risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a significant or maximum risk, the project owner needs to consult an external expert before it may go ahead with the processing. The advice of such external expert needs to be summarized and the project owner needs to note whether it has accepted such advice and if not the reasons in "⑤Conclusion". To ensure the implementation of the security control after the system has been developed, the project owner fills in the measures and their evidences in “⑥Completion Check”. The Information Security Function should check the implement status and fill in whether or not the measures have been completed in “⑥Completion Check”.

The project owner shares the completed entire "PIA Sheet" to Legal Associate. Legal Associate shares it with the Information Security Function and CLO.

16.2.9 Compliance with PIA

The project owner needs to integrate the approved measures into the project plan and ensure that they are implemented before the processing.

Even after the processing starts, the project owner needs to keep PIA under review, as it may need to repeat it if there is a substantial change to the nature, scope, context or purposes of the processing.

16.3 PIA required under PDPL

16.3.1 Associates shall implement additional risk assessment when Processing Sensitive Information.

16.3.2 Associates shall adopt the following measures when conducting additional risk assessment of Sensitive Information:

(1) Identify Sensitive Information This involves inventorying all data across various systems and platforms to discover where Sensitive Information is stored. This data could include customer details, company financials, intellectual property and other data.

(2) Classify the Data: Once the Sensitive Information is identified, classify it according

to sensitivity levels. This could range from Personal Information, public information to strictly confidential data.

(3) Discover Data Processing Activities: This involves mapping the Sensitive Information flow - how it is collected, stored, used, and disposed of.

(4) Identify & Evaluate Potential Risks: Risks could range from data breaches, unauthorized access, data loss, etc. Evaluate these risks for probability and impact on the business. Consider both internal and external threats.

(5) Prioritize Risks: Prioritize risks based on their potential impact and likelihood. High-priority risks will require immediate attention and robust control measures.

(6) Develop a Risk Mitigation Plan: For every risk identified, develop strategies to either avoid, reduce, share, or accept the risk. This can include implementing secure data access controls, encryption techniques, data anonymization, regular audits and/or other measures.

(7) Implement Mitigation Strategies: This can involve changes in business processes, IT systems, employee training, or limiting access to the Sensitive Information. Implementation should be monitored to ensure that these risk mitigation strategies are effectively executed.

(8) Document the Risk Assessment Findings: Findings and risk mitigation recommendations should be documented in a risk assessment report.

17. Associate training

18. Internal monitoring

18.1 Scope

All processing activities.

18.2 Frequency

18.2.1 In principle, monitoring on organizational measures should be conducted at least once every three years. However, for the processing which is "likely to result in a high risk to the rights and freedoms of individuals", the monitoring on organizational measures should be conducted at least once a year. Whether the activity is likely to result in a high risk to the rights and freedoms of individuals is assessed by "Personal Information Processing Risk Analysis Sheet".

18.2.2 Monitoring on technical measures should be conducted once a year.

18.3 Monitoring items

For organizational measures, refer to the "**Check Sheet for Organizational Measures**" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html). For technical measures, refer to the "**Check Sheet for Compliance with the Global Information Security Guideline**" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html).

18.4 Monitoring procedures

18.4.1 Heads of departments shall monitor in their own departments as to the status of compliance following the instructions of Legal Associates (or Privacy Office) and report the results of the monitoring to Legal Associates (or Privacy Office). Legal Associates (or Privacy Office)

shall also monitor the status of compliance. Information Security Function shall collaborate with Legal Associates.

18.4.2A Organizational measures (for the processing that is not likely to result in a high risk to rights and freedoms of individuals)

Step	Party	Contents
1	Chief Legal Officer	Request Legal Associates to conduct internal monitoring (CC: Regional Legal Representative).
2	Legal Associate	Request departments to conduct internal monitoring.
3	Departments	Complete "Check Sheet for Organizational Measures For Departments" and submit it to Legal Associate.
4	Legal Associate (or Privacy Office)	Review the "Check Sheet for Organizational Measures For Departments" completed by the department from the viewpoint of whether the department's personal information protection measures are implemented in accordance with the rules of the Group/Region/Entity. Give feedback to the department by writing comments and returning the sheet to the department with, if appropriate, any advice for improvement.
5	Legal Associate	Complete "Check Sheet for Organizational Measures For Entities" and send it to the Chief Legal Officer (CC: Regional Legal Representative). It should include the summary of the improvement advice given to the department regarding the items.
6	Regional Legal Representative	Review the "Check Sheet for Organizational Measures For Entities" completed by the Legal Associate from the viewpoint of whether their responses are sufficient and appropriate under the rules of the Region. Support the Chief Legal Officer by writing comments and advice for improvement (if any) and sending the sheet to the Chief Legal Officer.
7	Chief Legal Officer	Review the "Check Sheet for Organizational Measures For Entities" completed by the Legal Associates from the viewpoint of whether his/her responses are sufficient and appropriate under the rules of the Group, taking Regional Legal Representatives' comments into account. Give feedback to the Legal Associates by writing comments and returning the sheet to the Legal Associates with, if appropriate, any advice for improvement (CC: Regional Legal Representative).
8	Chief Legal Officer	Report the overview of the monitoring results to the Internal Control Committee of Terumo Corporation.

18.4.2B Organizational measures (for the processing that is likely to result in a high risk to rights and freedoms of individuals)

Step	Party	Contents
1	Chief Legal Officer	Request Legal Associates to conduct internal monitoring (CC: Regional Legal Representative).
2	Legal Associate	Request the department that conduct high risk processing to conduct internal monitoring.
3	Departments that conduct high-risk processing	Complete the "Check Sheet for Organizational Measures For Departments" and submit it to Legal Associate.
4	Legal Associate (or Privacy Office)	Review the "Check Sheet for Organizational Measures For Departments" completed by the department from the perspective of whether the department's personal information protection measures are being implemented in accordance with rules of Group/Region/Entity. Give feedback by writing comments and returning the sheet to the department with, if appropriate, any advice for improvement (CC: Chief Legal Officer and Regional Legal Representative).
5	Regional Legal Representative	Review the "Check Sheet for Organizational Measures For Departments" completed by the Legal Associate from the viewpoint of whether his/her responses are sufficient and appropriate under the rules of the Region. Support the Chief Legal Officer by writing comments and advice for improvement (if any) and sending the sheet to the Chief Legal Officer.
6	Chief Legal Officer	Review the "Check Sheet for Organizational Measures For Departments" completed by the Legal Associates from the viewpoint of whether his/her responses are sufficient and appropriate under the rules of the Group, taking Regional Legal Representatives' comments into account. Give feedback by writing comments and returning the sheet to the Legal Associates with, if appropriate, any advice for improvement (CC: Regional Legal Representative).
7	Chief Legal Officer	Report the overview of the monitoring results to the Internal Control Committee of Terumo Corporation.

18.4.3 Technical measures

Upon the instructions of the Chief Information Security Officer, the Information Security Function associates complete "Check Sheet for Compliance with the Global Information Security Guideline" by fulfilling self-assessment about the entities they are in charge and submit it to the Chief Information Security Officer. The Chief Information Security Officer shares the result with the Chief Legal Officer.

Section 3. Processors and Third Parties

19. Selection of Processors

19.1 Exemptions

External Processors must be selected in accordance with certain selection criteria. However, external Processors who have globally recognized certification (e.g., ISO_IEC_27701, ISO 27018, SOC 2 type 2 reports, BCR or CBPR) are deemed to have measures to protect Personal Information in place and do not require to be selected based on the selection criteria.

19.2 Selection based on the selection criteria

External Processors that do not meet any of the above exemption conditions must be selected based on the selection criteria associated with the risk level of processing activities and the Personal Information protection level of the external Processor. The procedure is as follows.

Step 1: Evaluate the risk level of the processing of Personal Information to be outsourced

The department that intends to select an external Processor to be entrusted with the processing of Personal Information should evaluate whether the processing of Personal Information to be entrusted is "likely to result in a high risk" to the rights and freedoms of Data Subjects with the "**Personal Information Processing Risk Analysis Sheet**" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html). The processing falls under two or more of the items is considered to be "likely to result in a high risk".

Step 2: Assessing the level of Personal Information protection of external Processors

If the processing is considered to be "likely to result in a high risk", the department that intends to select an external Processor shall assess the level of Personal Information protection of that external Processor by sending the "External Processor Selection Criteria" in "**External Processor Selection Criteria & Monitoring Checklist**" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html).

However, if it is difficult to get response to the above checklist from the Processor, we may assess the level of protection of Personal Information of that Processor by reviewing security whitepaper published by that Processor as an alternative method.

20. Execution of contracts with Processors

20.1 The contract shall provide that the Processor shall appropriately manage Personal Information and implement appropriate security measures.

20.2 The following Processor's obligations are recommended to be included in the contract.

#	Processor's obligations recommended for inclusion in contracts with Processors
1	External Processor shall process Personal Information only in accordance with Terumo's instructions and only for the purposes of performing the contract.
2	External Processor shall ensure that persons authorized to Process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
3	External Processor shall take appropriate information security measures relating to Personal Information of Data Subjects.
4	External Processor shall not engage another outsource company without prior written approval, and if another outsource company is engaged, require the same data protection obligations as those specified in the contract between Terumo and the external Processor.
5	External Processor shall not (or shall not further) transfer or Disclose any of the Personal Information to another country without first notifying Terumo and obtaining Terumo's written consent to do so.
6	External Processor shall assist Terumo in fulfilling its obligations as a controller by taking appropriate organizational and technical measures for the protection of Personal Information according to the nature of the activities in which Personal Information is Processed and comply fully with Applicable Law in respect of data privacy and data protection.
7	If Personal Information entrusted by Terumo is breached (or is likely to be breached), the external Processor shall promptly report it to Terumo and investigate the cause and effect of the breach. If Terumo initiates an investigation on its own, Processor shall , cooperate with the investigation conducted by Terumo, work to prevent the damage from spreading, and indemnify Terumo for any and all damages, losses, and expenses (including legal damages and damage to reputation). In addition, external Processor shall cooperate with Terumo to fulfill its legal obligations to Data Subjects, personal information supervisory authorities, and other third parties.
8	External Processor shall cooperate with Terumo in fulfilling its legal obligations to Data Subjects and personal information supervisory authorities, including notifying Terumo when a Data Subject exercises its rights granted under the Applicable Law directly applying to the Processor instead of Terumo.
9	External Processor shall promptly delete or return to Terumo all the Personal Information after the end of the provision of services relating to processing and delete existing copies of Personal Information and shall certify or confirm to Terumo that it no longer possesses any Personal Information of Terumo associates or customers.

10	External Processor shall cooperate with monitoring and auditing conducted by Terumo, including preserving relevant records to facilitate such monitoring and audit and consequences if a breach is found by such monitoring or audit.
11	External Processor shall inform Terumo of any complaints or loss in certifications (where applicable) and the reasons for the same.
12	The Processor shall provide Terumo with access to the Personal Information that the Processor has in its possession or control, as soon as practicable upon Terumo's written request.

21. Monitoring of Processors

21.1 Monitoring of exemption conditions

Subject: External Processors exempted from "selection based on the selection criteria" (i.e., selected based on the certification)

When: From time to time (at least when the department that selected the Processor gets aware of loss or change of the certification)

Step	Executing party	Contents
1	Department that selected the external Processor	Confirm the continuity of the certification of the external Processors from time to time.
2	Department that selected the external Processor	When it is found that the certification is no longer valid, selection shall be conducted based on the selection criteria as soon as possible, if processing of Personal Information to be entrusted is "likely to result in a high risk". The results shall be reported to the Legal Associates.
3	Legal Associate	If the result report from the department is "meets the selection criteria," advise the department to review the contract as necessary. If the result reported by the department is "does not meet the selection criteria," advise on termination of the contract.
4	Department that selected the external Processor	Review or terminate the contract based on the advice of the Legal Associate.

21.2 Monitoring of entrusted activities

Subject: External Processors considered not "likely to result in a high risk" at the time of appointment

When: From time to time

Step	Executing party	Contents
1	Department that selected the external Processor	Confirm the consistency of outsourcing details as appropriate.
2	Department that selected the external Processor	If the details of the outsourced processing have changed, evaluate whether the outsourced processing has become "likely to result in a high risk. If it is concluded that the processing has become "likely to result in a high risk," the level of Personal Information protection of the external Processor shall be re-evaluated and the necessity of reviewing or terminating the contract shall be determined. Along with the results, a request for review or termination of the contract shall be submitted to the Legal Associate.
3	Legal Associate	Upon receipt of a request from a department to review or terminate a contract, advise the department on contract review or termination, as appropriate.
4	Department that selected the external Processor	Revise or terminate the contract based on the advice of the Legal Associate.

21.3 Monitoring by external Processor monitoring checklist or security whitepaper

Subject: External Processor selected based on the selection criteria or security whitepaper

When: As provided in the contract with the Processor

Monitoring items: Refer to the "**External Processor Monitoring Checklist**" in "**External Processor Selection Criteria & Monitoring Checklist**" on the intranet (http://hq.terumo.co.jp/hp_page/houmu/dataprivacy/resource.html).

Step	Executing party	Process
1	Department that selected the external Processor	Conduct monitoring, as necessary, using the "External Processor Monitoring Checklist" in "External Processor Selection Criteria & Monitoring Checklist" or security whitepaper. Submit the completed checklist to the Legal Associate.
2	Legal Associate	Review the submitted "External Processor Monitoring Checklist" or security whitepaper and provide feedback to the department on improvement measures, if necessary.

22. Disclosure of Personal Information to Third Parties

22.1 Disclosure to a Third Party requires the Data Subjct's consent, unless Disclosure without the Data Subject's consent is required or authorized under the Applicable Law.

Section 4. Cross-border Transfer

23. Cross-border Transfer

23.1 Cross-border Transfer can be divided into the following two patterns:

Intra-group transfer: Regular, occasional or ongoing transfer of Personal Information between or among group entities located in different jurisdictions (e.g., registering names, contact information, and departments of associates in all group entities in Outlook, and using such information at all group entities); and

Extra-group transfer: Regular, occasional or ongoing transfer of Personal Information between a Terumo entity and a Third Party located in different jurisdictions (e.g., a company in Europe sends Personal Information of associates to a company in India to outsource payroll for the associates in Europe).

23.2 Intra-group transfer

23.2.1 To ensure that every Terumo entity takes appropriate safeguards to protect Personal Information, Terumo entities enter into an intra-group transfer agreement.

23.2.2 In principle, the items to be included in the intra-group transfer agreement are as follows:

	Item
1	Scope and definition
2	Subject Matter, term and accession
3	Details of processing activities – Register
4	Controller-to-Processor activities
5	Controller-to-Controller activities
6	Joint Controller activities
7	Processor-to-Sub Processor activities
8	Cross-border transfer of data

9	Data protection officer – Privacy point of contact
10	Personal data breach
11	Liability
12	Main establishment – Notices
13	Final provisions

23.2.3 The intra-group transfer agreement is executed between the entities representing both source and destination entities. In addition, if, given the contents of the transfer and requirements under the Applicable Law, it is required or desirable to execute an intra-group transfer agreement directly between the transfer entity and the transferee entity, such entities may execute an intra-group transfer agreement directly.

(i) Each group entity authorizes its respective representative entity (as described below) to execute the intra group transfer agreement.

(ii) The Chief Legal Officer prepares the intra-group transfer agreement in consultation with Regional Legal Representatives and Legal Associates of each representative entity, and prepares an original copy for signature.

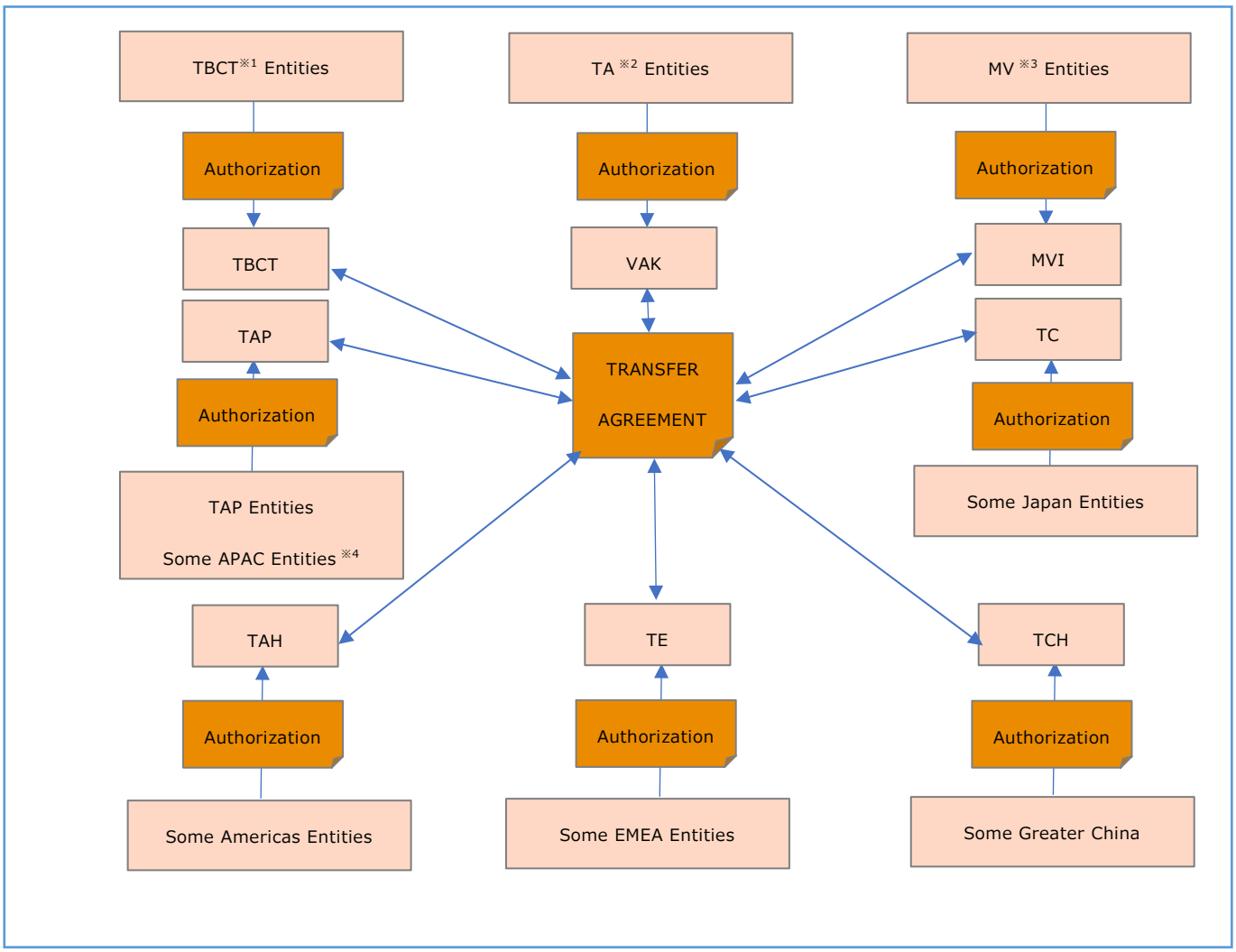
(iii) Each representative entity executes the intra-group transfer agreement.

(iv) The original copy of the intra-group transfer agreement (including the signed page of each representative entity) is kept by CLO Office.

(v) In case a new entity is added to the group after the execution of the intra-group transfer agreement, one of the representative entities is authorized by the new entity to execute a letter of accession to become a party to the intra-group transfer agreement. The original copy of such letter, together with the original copy of the intra-group transfer agreement, is kept by CLO Office.

23.2.4 Chief Legal Officer, using internal monitoring, data mapping and other opportunities, monitors so that the newly added group entities are covered by the intra-group transfer agreement and that the content of the intra-group transfer agreement is in line with the actual status of intra-group data transfers.

<Method of executing the intra-group transfer agreement>



※1 All TBCT Entities in Japan, EMEA, APAC, Americas, Greater China Region

※2 All TA Entities in Japan, EMEA, APAC, Americas, Greater China Region

※3 All MV Entities in Japan, EMEA, APAC, Americas, Greater China Region

※4 Terumo Philippines Corp., Terumo Vietnam Co., Ltd., Terumo India Private Ltd.

23.2.5 Additional measures shall also be taken if such measures are required by any Applicable Law and cannot be covered by the intra-group transfer agreement. Legal Associate reviews the requirements for Cross-border Transfer under the Applicable Law of the country where the entity is located and implements the measures to address such requirements that cannot be addressed by the intra-group transfer agreement. However, if the Applicable Law of more than one country within the Regional Unit specify requirements for Cross-border Transfer, the Regional Legal Representative determines the most appropriate method for the Regional Unit.

23.3 Extra-group transfer

23.3.1 If there are restrictions on Cross-border Transfer under the Applicable Law, the transferor Terumo entity shall take measures required under the Applicable Law to enable the envisaged extra-group transfer.

23.3.1A Unless allowed under 23.3.1B, consent shall be obtained from the Data Subject to extra-group Cross-border Transfer.

23.3.1B In any of the following cases, Cross-border Transfer to an external Third Party is possible without obtaining a consent to the Cross-border Transfer from the Data Subject:

(i) If the Third Party is located in the countries that have laws imposing on the recipient legally enforceable obligations to provide adequate protection standards to the transferred Personal Information that are comparable to the protection provided under the Applicable Law.

(ii) If "appropriate safeguards" are in place, such as standard contract clauses relating to the recipient's use, processing or disclosure of Personal Information.

(iii) Other cases designated under the Applicable Law.

23.3.2 If there are no restrictions on Cross-border Transfer under the Applicable Law, a transferor Terumo entity shall, in principle, execute a transfer agreement (that may be an independent contract, but may also be addendum to or part of another contract (such as a processor agreement when the transferee is a Processor)) to ensure that the transferee takes appropriate safeguards to ensure the same level of protection of Personal Information as the transferor (i.e., a Terumo entity).

23.3.3 If re-transfer of Personal Information is envisaged, the Terumo entity transferor shall demand the transferee obtain a prior approval from the Terumo entity transferor for the re-transfer. Before giving the approval, the Terumo entity transferor shall know the location of the re-transferee and evaluates its measures to protect Personal Information. When giving the approval, the Terumo entity transferor shall obtain the transferee's undertaking to procure that the re-transferee complies with the transferee's obligations to protect Personal Information under the transfer agreement.

23.3.4 Legal Associate in charge of the transferor entity (or the Regional Legal Representative if the transferor is multiple entities in a Regional Unit, or the Chief Legal Officer if the transferor is multiple companies in multiple Regional Units) prepares the extra-group transfer agreement, while reviewing the requirements of Applicable Law.

23.3.5 After the execution of the extra-group transfer agreement, the department which is a party to the transfer agreement periodically reviews the contents of the transfer and submits a request for review of the extra-group transfer agreement to Legal Associate if the contents of the transfer have changed.

23.3.6 Legal Associates, using internal monitoring, data mapping, and other opportunities, monitors so that the content of the extra-group transfer agreement is in line with the actual status of the data transfer.

Section 5. Response to Data Subjects

24. Data Subjects' rights

24.1 See Annex 2 for guidance to develop policy and process for responding to Data Subject rights.

24.2 Policy for responding to the requests based on Data Subject rights

If a request is received from the Data Subject:

- to get explanation about the legal basis, purpose of use and Processing of Personal Information in possession or under the control,

- to complete, update, rectify errors or inaccuracy in Personal Information in possession or under the control,

- to access and obtain copy of Personal Information in possession or under the control,

- to end Processing, erase or destroy Personal Information,

- to withdraw consent,

- to file an objection to a decision solely based on automated Processing (e.g., profiling),

- to postpone or restrict Processing of Personal Information,

- to claim for recovery of damages for a breach of Processing, or

- to data portability,

such request shall be responded according to the process described below.

24.3 Response process

24.3.1 Data Protection Officer or Legal Associate receives a request form from the Data Subject in a manner designated by the APAC Regional Legal Representative from the methods permitted under the Applicable Law (such as letters, email, website announcement etc.). After the receipt, the Data Protection Officer and Legal Associate shall assess and decide whether such request needs to be responded.

24.3.2 Identity of the requesting Data Subject shall be verified with identification documents upon receipt of the request.

24.3.3 Legal Associate and the Data Protection Officer shall check whether the request has legal ground and if not clear request the requesting Data Subject to provide further information as necessary.

24.3.4 If the Data Protection Officer and Legal Associate determine that Terumo should accept the request, Data Protection Officer and Legal Associate and other related departments shall arrange for the requested action.

24.3.5 If the Data Protection Officer and Legal Associate determine that Terumo should reject the request entirely or partially, Legal Associate shall notify the Data Subject of such decision without delay and make effort to explain about the reason for the decision.

24.3.6 It is necessary to respond to the request of the Data Subject without undue delay. In principle, the response shall be completed within one month of the receipt of the request satisfying the method provided in 24.3.1, unless more time is necessary, depending on the content of the request.

24.4 Report

24.4.1 In the following cases, Legal Associates shall report to the APAC Regional Legal Representative, after the completion of response to the Data Subject's request or after the notice of rejection to the Data Subject, for a statistical purpose:

(i) Requests from subjects of clinical trials/clinical researches

(ii) Requests from patients

24.4.2 When the APAC Regional Legal Representative received the report in the previous paragraph, the APAC Regional Legal Representative shall report the same to the Chief Legal Officer.

24.5 Record

The Legal Associates shall record and keep the request and response in cooperation with the related

24.6 Involvement of APAC Regional Legal Representative

24.6.1 When Legal Associate becomes aware that a Data Subject is making similar requests to two or more group entities in Singapore, the Legal Associate shall notify the APAC Regional Legal Representative of the same. The APAC Regional Legal Representative then decides how to handle the request in collaboration with the related Legal Associate(s).

24.6.2 When the Legal Associate receives a request from a Data Subject residing outside Singapore but in a country within the Regional Unit the APAC Regional Legal Representative is responsible for (i.e., Asia/India/Oceania excluding Japan and Greater China), the Legal Associate shall notify the APAC Regional Legal Representative, and the APAC Regional Legal Representative then decides how to handle the requests in collaboration with the related Legal Associate(s).

24.6.3 When the Legal Associate receives a request from a Data Subject residing outside the Regional Unit the APAC Regional Legal Representative is responsible for (i.e., Asia/India/Oceania excluding Japan and Greater China), the Legal Associate shall notify the APAC Regional Legal Representative and the APAC Regional Legal Representative shall notify the Regional Legal Representative of the relevant Regional Unit of the same. Such Regional Legal Representative then decides how to handle the request in collaboration with the APAC Regional Legal Representative and the related Legal Associate(s).

25. Privacy notice

25.1 The following items shall be notified to the Data Subject. For details, refer to the "Template of Privacy Notice" on the intranet. If Applicable Law requires the notification of other items, these items must also be notified.

(i) Terumo contact information

(ii) Purpose of Processing

(iii) Retention period

(iv) Rights of the Data Subject

(v) Categories of Personal Information collected

(vi) Source of Personal Information

(vii) Disadvantage due to his/her rejection to provide Personal Information

(viii) Third Party shared the Personal Information with

(ix) Security measures

(x) Cross-border Transfer of Personal Information

25.1A When obtaining consent from Data Subjects for the collection, use or disclosure of Personal Information, it is necessary for Terumo Indonesia entities to provide the Data Subjects the following information in order for the consent from Data Subjects to be valid:

(i) the legality of the Personal Information Processing;

(ii) the purpose of the Personal Information Processing;

(iii) the type and relevance of the Personal Information to be Processed;

(iv) the retention period of documents containing Personal Information;

(v) details regarding the Personal Information collected;

(vi) period of Personal Information Processing; and

(vii) rights of the Data Subjects.

25.1B Terumo Indonesia entities shall inform the Data Subjects by written notice if there is any changes to the information provided to the Data Subjects in 25.1A.

25.2 There are two methods of notifying Data Subjects: "individual notice" and "general notice". Which method is used is guided by the Applicable Law. If the Applicable Law does not require individual notice, general notice is acceptable as the notification method.

<Individual notice>

A method of notifying Data Subject directly via e-mail, a person-specific application web page/application, or a contract, depending on the method of interaction with the Data Subject, such as electronic or in paper. Which method you choose shall base on the principle of easy accessibility for the Data Subject. The purpose of directly notifying the Data Subject him/herself is for a better transparency.

<General notice>

A method of notifying Data Subject via a privacy policy posted on a website. The purpose is to notify Data Subject of the required items that are not covered by individual notice.

"General notice" is the primary method of notification for collecting Personal Information. However, associates may issue Individual Notice when he/she thinks it necessary. Also, if Individual Notice is required under the Applicable Law, Individual Notice shall be used.

26. Response to complaints and inquiries

Section 6. Data Breach

27. Data Breach

27.1 Examples of Data Breach

- theft of data or equipment on which data is stored e.g. work mobile with access to work emails is stolen;
- loss of data or equipment on which data is stored e.g. loss of USB stick containing lists of customer contact data;
- accidental loss e.g. leaving papers containing health related data on public transport;
- unlawful disclosure of personal data to a third party e.g. sending email to the wrong person;
- unforeseen circumstances such as a fire or flood e.g. where our hard copy papers are lost and we do not have electronic copies;
- cyber attack on our systems or system operated by an external service provider who handles personal data on our behalf, malware, blackmailing by cybercriminals after cyber attack;

27.2 See Annex 3 for guidance to develop Data Breach procedures.

27.3 When a Data Breach has occurred or may have occurred, the parties stated below shall take actions described below.

27.3.1 Associate who found a Data Breach

He/she shall report the Data Breach to the Legal Associates and the Information Security Function in email (security_admin@terumo.co.jp) in principle. He/she shall include the related departments' heads and persons in charge in C.C. to share the information. If reporting by email is difficult, telephone call can be used.

27.3.2 The related departments' heads and persons in charge

(i) Cooperate with the investigation team and investigate the Data Breach

(ii) Improve the matters in accordance with the recommendation from the investigation team and report to the monitoring team the improvement

27.3.3 Data Protection Officer and Legal Associates

Data Protection Officer and Legal Associates take report from the Associate who found the Data Breach. Then, they shall organize investigation team and monitoring team. However, if the investigation team makes recommendation for improvement (e.g., review of process, rules and standards as necessary) to the Legal department, the investigation team shall timely report to the internal audit and perform the following actions under its supervision.

27.3.4 Information Security Function

Information Security Function shall assist in the investigation and assessment.

27.3.5 Investigation team

Investigation team must take reasonable and expeditious steps to conduct investigation as per the steps described below, in cooperation with the associate who found the Data Breach, a system administrator of the relevant system, and heads and persons in charge of the related departments. After recommendation is made, the matter shall be handed over to the monitoring team.

(i) Collect information and conduct initial investigation

Based on the initial investigation, conduct initial assessment, within 30 calendar days of it receiving a report regarding a Data Breach, on the impact of the Data Breach and determine whether the matter is notifiable; namely, the matter results in, or is likely to result in, "significant harm" to an affected Data Subject, or is, or is likely to be, of a significant scale. "**Significant harm**" could include physical, psychological, emotional, economic, financial and reputational harm. A "**significant scale**" breach is a Data Breach that involves the Personal Information of 500 or more Data Subjects in Singapore. More detailed investigation takes place after the initial assessment:

(ii) Takes actions or makes recommendation to prevent extension of damage, to minimize loss, to collect evidence, to preserve evidence and to pursue liabilities (civil, criminal and disciplinary).

(iii) Report the result of the initial assessment to the APAC Regional Legal Representative and discuss with the APAC Regional Legal Representative whether the matter should be immediately reported to Ministry of Communication and Informatics ("MOCI")

and/or notified to the Data Subject. If the discussion has reached a conclusion that the matter should be reported and/or notified, in principle, the entity, through Data Protection Officer (if appointed), which is the origin of the Data Breach shall notify MOCI as soon as practicable, but in any case, no later than 3 calendar days, and where required, notify the affected Data Subject as soon as practicable, at the same time or after notifying the MOCI of the notifiable Data Breach. In its Data Breach notification to the MOCI, the Data Protection Officer must provide relevant details of the data breach and management and remediation plans. The notification must be submitted in the form and manner required by the MOCI. Unless it is clearly determined that the matter does not fall in any of the cases stated in 27.3.5 (i), the matter shall be reported to the MOCI. In case of a failure to reach a conclusion, the APAC Regional Legal Representative shall make a decision based on the discussion and external expert's opinion. After the report is made to the MOCI and/or the notice is given to the Data Subject, their contents shall be reported to the APAC Regional Legal Representative .

(iv) Continue the investigation and impact assessment.

(v) Report the outcome of the investigation to the APAC Regional Legal Representative and discuss with the APAC Regional Legal Representative whether a conclusive report should be made to the MOCI and/or a conclusive notice should be given to the Data Subject. If the discussion has reached a conclusion that such report and/or notice is necessary, in principle, the entity through Data Protection Officer (if appointed) which is the origin of the Data Breach shall make a conclusive report to the MOCI and/or give a conclusive notice to the Data Subject. In case of a failure to reach a conclusion, the APAC Regional Legal Representative shall make a decision based on the discussion and external expert's opinion. After the report is made to the MOCI and/or the notice given to the Data Subject, their contents shall be reported to the APAC Regional Legal Representative.

(vi) Record the Data Breach and make a recommendation for improvement (e.g., review of process, rules and standards as necessary) to the heads and persons in charge of the relevant departments (i.e., the departments related to the cause of the Data Breach) and/or the legal departments and/or the Information Security Function.

27.3.6 Internal Audit

Internal Audit audits whether the actions for improvement taken by the relevant departments and/or the legal departments or the Information Security Function are appropriate given the outcome of the investigation and the recommendation by the investigation team.

27.3.7 APAC Regional Legal Representative

(i) Take a report from the Legal Associates in relation to the Data Breach

(ii) Take a report from the investigation team on the result of the initial assessment. Based on the result, discuss with the investigation team whether the preliminary report to the MOCI should be made. Unless the matter does not fall in the material incident, the matter should be reported to the MOCI. In case of a failure to reach a conclusion, the APAC Regional Legal Representative shall make a decision based on the discussion

and external expert's opinion. After the preliminary report is made to the MOCI and/or the notice is given to the Data Subject, take a report on their contents.

(iii) Take a report on the outcome of the investigation from the investigation team and discuss with the investigation team whether a conclusive report should be made to the MOCI and/or a conclusive notice should be given to the Data Subject. In case of a failure to reach a conclusion, the APAC Regional Legal Representative shall make a decision based on the discussion and external expert's opinion. After the report is made to the MOCI and/or the notice given to the Data Subject, their contents shall be reported to the APAC Regional Legal Representative.

(iv) Report to the Chief Legal Officer if (i) a Data Breach has been reported either preliminary or conclusively to the MOCI, (ii) a Data Breach occurs regarding the Personal Information of subjects of clinical trials/clinical researches or patients, (iii) a Data Breach occurs about the Personal Information of Data Subjects in multiple Regional Units, (iv) more than 500 Personal Information are or may be leaked, and (v) a Data Breach occurs due to a cyber attack.

(v) Take a report from the Data Protection Officer, Legal Associate and the Information Security Function if any internal rule was revised after the occurrence of the Data Breach.

Chapter IV Miscellaneous Rules

28. Penalty

29. Owner

30. Revisions

Revision History

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

Reference: Methods for assessing the Severity of data Breach by Legal Associate

Severity of a Personal Data Breach

The severity of a Personal Data Breach is defined, for the purposes of this procedure, as the 'estimation of the magnitude of potential impact on the individuals derived from the data breach' (see ENISA Recommendations).[1]

a. Assessment Criteria

The main criteria taken into account while assessing the severity of a Personal Data Breach are:

- **Data Processing Context (DPC):**

DPC addresses the type of breached data, together with a number of aggregating or mitigating factors linked to the overall context of the processing.

DPC evaluates the criticality of a given data set in a specific processing context.

- **Ease of Identification (EI):**

EI determines how easily the identity of the individuals can be deduced from the data involved in the breach.

EI is a correcting factor of the DPC. The overall criticality of a data processing can be reduced depending on the value of the EI, namely, the lower the ease of identification is, the lower gets the overall score. Therefore, the combination of the EI and DPC (multiplication) gives the initial score of the severity (SE) of the Data Breach.

- **Circumstances of the Breach (CB):**

CB addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

CB quantifies specific circumstances of the breach that may be present or not in a particular situation. When present, CB can only add to the severity of a specific data breach and the initial score can be further adjusted by the CB.

b. Calculation of the severity

To calculate the severity result, all three criteria should be scored. In order to assess the overall severity of a Personal Data Breach, and to obtain a result that will be easy to interpret, the following formula shall be used:

[1] ENISA Recommendations for a methodology of the assessment of severity of Personal Data Breaches, Working Document, v1.0, December 2013
https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport

SE = DPC x EI + CB*

*Whereas SE means Severity, DPC means Data Processing Context, EI means Ease of Identification and CB means Circumstances of Beach.

The result belongs to a certain range of values which corresponds to one of four severity levels: low, medium, high and very high.

At the end of the assessment, other possibly relevant criteria (number of individuals, unintelligibility of data) that may have not been considered are evaluated and flagged to the supervisory authority when applicable.

c. Scoring of the criteria

- **c.1. DPC Scoring**

DPC can be represented with a value of 1, 2, 3 or 4, depending on the category of the personal data involved in the data breach. To find the score for the DPC, the following steps must be followed:

i. Define the types of the personal data involved in the Breach.
ii. Classify the data in at least one of four data categories: simple, behavioral, financial and sensitive.
iii. Assess the occurrence of certain factors that could increase or decrease the basic score (data volume, special characteristics of the controller or the individuals, invalidity/inaccuracy of data, public availability (before the breach), nature of data).
iv. If such factors exist, adjust the basic score accordingly (increase or decrease).

Please refer to Annex 1 of the ENISA Recommendations, for a list of contextual factors and specific examples of DPC scoring.

- **c.2. EI Scoring**

For the purpose of this assessment, we will define four levels of EI: negligible, limited, significant, and maximum, represented with a value of 1, 2, 3 or 4 accordingly.

The lowest score is given when the possibility to identify the individual is negligible, namely it is extremely difficult to match the data to a particular person, but still it could be possible under certain conditions.

The highest score is selected when identification is possible directly from the data breached with no special research needed to discover the individual's identity.

Identification may be directly (e.g. on the basis of a given name) or indirectly (e.g. on the basis of ID number) possible from the breached data.

Please refer to Annex 2 of the ENISA Recommendations for specific examples of EI scoring using common identifiers.

- **c.3. CB Scoring**

The elements that are considered under CB are the loss of security (confidentiality, integrity, availability) and malicious intent and are complementary to DPC and EI, as follows:

Loss of confidentiality: Loss of confidentiality occurs when the information is accessed by parties who are not authorized or don't have a legitimate purpose to access it. The extent of loss of confidentiality varies by the scope of disclosure, i.e. the potential number and type of parties that may have unlawfully access to the information.

Loss of integrity: Loss of integrity occurs when the original information is altered, and substitution of data can be prejudicial for the individual. The most severe situation occurs when there are serious possibilities that the altered data have been used in a way that could harm the individual.

Loss of availability: Loss of availability occurs when the original data cannot be accessed when there is a need for it. It can be either temporal (data are recoverable but it will take a period of time and this can be detrimental for the individual), or permanent (data cannot be recovered).

Malicious intent: This element examines whether the breach was due to an error or mistake, either human or technical, or it was caused by an intentional action of malicious intent. Non malicious breaches include cases of accidental loss, inadequate disposal, human error and software bug or misconfiguration. Malicious breaches include cases of theft and hacking aiming to harm the individuals (e.g. by exposing their personal data to unauthorized third parties). In other cases malicious intent might include transfer of personal data to third parties for profit (e.g. selling of lists of personal data). In some cases malicious intent could also be inferred from actions aiming to harm the data controller (e.g. through stealing and exposing the personal data to unauthorized parties). Malicious intent is a factor that increases the likelihood that the data is used in harmful way, since this was the initial purpose of the breach.

With regard to CB scoring, contrary to DPC and EI where the maximum score reached is chosen, the points obtained for each CB element are added to obtain the final score, as different circumstances can occur in the same breach.

Please refer to the Annex 3 of the ENISA Recommendations for specific examples of CB scoring.

c.4. Severity Levels

The final score shows the level of severity of a certain breach, taking into account the impact to the individuals.

Severity of a Data Breach		
SE score	Impact on affected Data Subjects	Possible Consequences for the Data Subjects
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Annex 1

1. Chief Legal Officer

Chief Legal Officer has the following roles, responsibilities and authorities.

① Building and maintaining Terumo's privacy program to ensure the protection of privacy and Personal Information

② Establishing framework for Terumo's internal rules (e.g., policy, standards, procedures) in relation to protection of privacy and Personal Information

③ Developing, maintaining and implementing internal rules (e.g., policies, standards, procedures, forms, guidance and training) which are commonly applied throughout Terumo (collectively, together with this Policy, the "**Group Privacy Program**")

④ Chairing the Privacy Office established at a group level

⑤ Monitoring the status of protection of privacy and Personal Information in Terumo based on the reports from the Legal Associates

⑥ Monitoring Regional Legal Representatives' activities for protection of privacy and Personal Information

⑦ Coordinating Regional Units

⑧ Reporting to the senior management and committees of Terumo Corporation about the status of protection of privacy and Personal Information in Terumo

⑨ To perform its roles and responsibilities, Chief Legal Officer has the following authorities.

- Establishing a group-level Privacy Office
- Requesting reports, cooperation and actions from Regional Legal Representatives and Legal Associates as well as Information Security Function, as necessary

2. Regional Legal Representatives

Regional Legal Representatives have the following roles and responsibilities.

① Coordinating the implementation of the Group Privacy Program and Regional Privacy Program in the Regional Unit in collaboration with the Legal Associates in the Regional Unit to ensure alignment and common approach

② Building and maintaining the Regional Unit's integrated structure for managing protection of privacy and Personal Information

③ Establishing framework for the Regional Unit's internal rules (e.g., policy, standards, procedures) in relation to protection of privacy and Personal Information

④ In collaboration with the Legal Associates and other stakeholders developing and maintaining internal rules (e.g., policies, standards, procedures, forms, guidance and training) which are commonly applied to all companies in the Regional Unit (collectively,

the "**Regional Privacy Program**") for the following purposes:

- To implement the Group Privacy Program and Regional Privacy Program
- To meet legal requirements in the Regional Unit which are stricter than the Group Privacy Program
- To uniformly respond to the issues of protection of privacy and Personal Information in the Regional Unit, based on the comprehensive consideration of internal and external risks of the companies in the Regional Unit
- To uniformly respond to the issues of protection of privacy and Personal Information in the Regional Unit, based on the comprehensive consideration of efficiency and/or consistency in the Regional Unit

In doing so, Regional Legal Representative needs to discuss with the Chief Legal Officer in advance.

⑤ In collaboration with the Legal Associates determining a direction for planning training for the associates in the Regional Unit for protection of privacy and Personal Information

⑥ Chairing the Privacy Office established at a Regional Unit level

⑦ Supporting the Chief Legal Officer in monitoring the status of protection of privacy and Personal Information in the Regional Unit based on the reports from the Legal Associates

⑧ In addition to the general matters set forth above, doing matters which are stated to "be done by the Regional Legal Representative" in the Group Privacy Program or the Regional Privacy Program

⑨ To perform their roles and responsibilities, Regional Legal Representatives shall collaborate with the Legal Associates and other stakeholders such at Information Security to establish a Regional Unit-level Privacy Office. When the Regional Legal Representative has established the Privacy Office, it reports to the Chief Legal Officer.

3. Legal Associates

Legal Associates have the following roles and responsibilities.

① Implementing the Group Privacy Program and Regional Privacy Program in the company the Legal Associate is in charge

② Developing, maintaining and implementing internal rules (e.g., policies, standards, procedures, forms, guidance and training) for the company the Legal Associate is in charge (collectively, the "**Local Privacy Program**") for the following purposes:

- To implement the Group Privacy Program and the Regional Privacy Program
- To meet legal requirements in the country which are stricter than the Group Privacy Program and the Regional Privacy Program
- To address the company's unique risk or circumstance which cannot be, or is not

appropriate to be, covered by the Regional Privacy Program

In doing so, Legal Associate needs to discuss with Regional Legal Representative in advance.

③ Conducting training for the associates for protection of privacy and Personal Information

④ Responding to the enquiries from associates about protection of privacy and Personal Information and, as necessary, sharing it to the Regional Legal Representative about it

⑤ Monitoring and reporting the status of protection of privacy and Personal Information in the company based on the reports from departments

⑥ Attending meetings of the Privacy Office of the Regional Unit (if any) and collaborating, sharing reports and information with the other Legal Associates and Regional Legal Representative

⑦ In addition to the general matters set forth above, doing matters which are stated to "be done by the Legal Associate " in the Group Privacy Program or the Regional Privacy Program

4. Information Security Function

Information Security Function has the following roles and responsibilities.

① Being part of the Privacy Office, if it is organized

② Ensuring the security of Personal Information processed by Terumo's information technology infrastructure (including systems, applications, networks, and servers).

③ When introducing or altering information technology/information systems related to the processing of Personal Information, implementing measures to protect privacy and Personal Information required by the Group Privacy Program, the Regional Privacy Program or the Local Privacy Program in collaboration with the legal function, and conduct privacy impact assessments and other measures as necessary.

④ Documenting the results of the implementation of protection measures for privacy and Personal Information and store the documents appropriately for internal audits and inspections by privacy supervisory authorities

⑤ In the event of a Data Breach, collaborating with the legal function and, if applicable, as part of the Privacy Office, identifying and analyzing the technical causes of the Data Breach, documenting the identified causes, and communicating the identified causes to the legal function

⑥ Implementing necessary information security technologies addressing the cause of the Data Breach

⑦ In addition to the general matters set forth above, doing matters which are stated to "be done by the Information Security Function" in the Group Privacy Program, the Regional Privacy Program or the Local Privacy Program

4A. Data Protection Officer

① Unless required under Applicable Law, a Data Protection Officer ("DPO") will be appointed locally to assume this role. The Data Protection Officer function may be a dedicated responsibility or added to an existing role. The appointed Data Protection Officer may delegate certain responsibilities to other officers or individuals.

② The roles and responsibilities of a DPO include, but are not limited to:

- Ensuring compliance with the Applicable Data Protection Law;
- Fostering a compliant Data Protection culture;
- Handling of Personal Information inquiries;
- Alert management on Personal Information leakage or handling risks;
- Report to the Chief Legal Officer of any Data Breach;
- Assess Data Breach with Legal Associate; and
- Liaise with and submit reports to Personal Data Protection Commission when required.

Annex 2

1. Policy and process for responding to Data Subject rights

1.1 The policy and process for responding to requests based on Data Subject rights (e.g., right to information, right of access, right to correction, right to erasure, right to restriction, right to object, right to portability, right not to be subject to decision by automated process only) shall be established by the Regional Legal Representative or Legal Associate.

1.2 The response policy shall, at least, specify the rights to be responded to the request in principle and the grounds for exceptions.

1.3 The process of response shall describe the following elements at least:

- How to accept a request
- Confirmation of the requestor's identity: Request the requestor to present identification documents to confirm the requester's identity.
- Clarification of the content of the request: Examine the exact content of the request. If necessary, request the requestor to provide information to help us understand the exact content of the request.
- Confirmation of the legal basis of the right: Examine the legal basis of the right. If necessary, request the requestor to provided information to help us confirm whether the requestor's right is based on Applicable Law.
- Prepare response: If we approve the request, prepare the appropriate response.

- Rejection of the request: Determine what information should be provided to the requestor when denying his or her request.
- Time limits: Set internal time limits to ensure that we can respond to the requestor without undue delay and within the legal deadline at the latest.
- Approval of response: Obtain the approval of the Legal Associate (and the DPO, if one has been appointed) before providing a response to the requestor.
- Involvement of Regional Legal Representative (as stated in 8.2).
- Report: Report any matters that are required to be reported to the Chief Legal Officer or Regional Legal Representative.
- Record keeping: Keep the request and response in a designated manner.

2. Involvement of Regional Legal Representative

2.1 When Legal Associate becomes aware that a Data Subject is making similar requests to two or more group entities within a Regional Unit, the Legal Associate shall notify the Regional Legal Representative of the same. The Regional Legal Representative then decides how to handle the request in collaboration with the related Legal Associate(s).

2.2 When an entity located in a Regional Unit (A) receives a right request from a Data Subject residing in another Regional Unit (B), the Legal Associate for the entity in Regional Unit (A) shall notify the Regional Legal Representative of the Regional Unit (B) of the same. The Regional Legal Representative then decides how to handle the request in collaboration with the related Legal Associate(s).

3. Reporting

3.1 Statistical report from Regional Legal Representative to Chief Legal Officer on the below items:

- Requests from subjects of clinical trials/clinical researches
- Requests from patients

3.2 Statistical report from Legal Associate to Regional Legal Representative

The items to be reported from Legal Associate to Regional Legal Representative shall be determined by Regional Legal Representative. However, the items to be reported from Regional Legal Representative to Chief Legal Officer shall be included.

Annex 3

Regional Legal Representative or Legal Associates shall establish Data Breach procedures, which reflect the following (i) basic role of Legal Associates, Information Security Function, Regional Legal Representative and Chief Legal Officer and Function and (ii) reporting to Regional Legal Representative and Chief Legal Officer.

Regional Legal Representatives and Chief Legal Officer may establish additional requirements for such procedures, or separate procedures, for the matters reported (or to be reported) to them.

1. Basic role regarding Data Breach

1.1 Legal Associates

- Examining and deciding on response direction and implementing response measures, in consultation with Regional Legal Representative and, in respect of the cases reported to Chief Legal Officer
- Assessing the severity of the Data Breach
- Involving Information Security Function for investigation
- Sharing with Privacy Office/Data Protection Office of the entity
- Reporting to Regional Legal Representative on the cases that meet reporting criteria

1.2 Information Security Function

- Investigating, analyzing, and reporting on technical causes and impact of a Data Breach, damage prevention, and recovery measures

1.3 Regional Legal Representatives

- Monitoring response direction and response status for the reported cases
- If necessary, supporting Legal Associates in determining response direction and response
- Sharing with Privacy Committee in the Regional Unit
- Reporting to the Chief Legal Officer on the cases that meet the reporting criteria

1.4 Chief Legal Officer

- Monitoring response direction and response status for the reported cases.
- If necessary, supporting Regional Legal Representatives and/or Legal Associates in the determination of response direction and responses.
- Reporting on the status of the reported cases to the senior management and organizational bodies of Terumo Corporation
- Providing the senior management and organizational bodies of Terumo Corporation with the overview of the management of Data Breach in Terumo

- Accumulating results of responses to Data Breach and reflect them as "lessons learned" in the education of associates

2. Reporting to Chief Legal Officer and Regional Legal Representatives

2.1 Criteria for reporting to the Chief Legal Officer from Regional Legal Representative

① When the incident will have a significant impact on the Data Subject (including when the possibility of such an impact has occurred)

(Examples)

- When a Data Breach requires a report to the supervisory authority
- When a Data Breach occurs regarding the Personal Information of subjects of clinical trials/clinical researches or patients

② Large-scale Data Breach (including the possibility of such breach):

(Examples)

- When a Data Breach occurs about the Personal Information of Data Subjects in multiple Regional Units
- When more than 500 cases of Personal Information are breached
- When a Data Breach occurs due to a cyber attack

Details will be established by Chief Legal Officer.

2.2 Criteria for reporting to Regional Legal Representative from Legal Associate

The criteria for reporting from Legal Associate to Regional Legal Representative shall be determined by Regional Legal Representative. However, the criteria for the matters to be reported to the Chief Legal Officers shall be included.