Version 180518

TERUMO EUROPE

Group:	Legal	Doc. No.:	
Section:	Privacy	Master:	TEMEA Legal Dept.
Title:	**PRIVACY AND DATA PROTECTION POLICY**		

1. PURPOSE AND SCOPE

1.1 Why do we have this Policy?

The processing of personal data is subject to strict rules and regulations throughout the world, including the European General Data Protection Regulation (the GDPR). Terumo is committed to protect personal data and privacy rights of its employees and contractors, HCPs, patients, customers and other business partners and to comply with applicable privacy regulations and practices. These privacy regulations impose restrictions on the use of personal data. Violating these privacy regulations may expose us to severe sanctions and damage claims.

This Policy describes the data privacy program including the requirements and principles that Terumo will observe for the collection, use, disclosure, transfer storage, and other processing of personal data, the rights of individuals and our privacy organization and structure. This Policy is managed by the Terumo Privacy Office (referred to below) and is supported by the Data Privacy Breach Procedure and the Personal Data Categorization and Handling Guidelines, which are referenced below. Further guidance on specific requirements may be provided in separate Standards and Procedures, which you can find on the Terumo intranet.

Where national laws deviate from or impose regulations that are stricter than the requirements set out in this Policy, Terumo will process personal data in accordance with such stricter regulations. Any such deviations or amendments to this policy shall be coordinated with the Privacy Office.

1.2 For whom is this Policy?

This Policy applies to all Associates and independent contractors processing personal data for or on behalf of any Terumo group entity (herein "Terumo", "we", "us" or "our"), regardless of where the processing takes place.

Compliance with this Policy is an obligation for all Associates and Contractors. It is the responsibility of the management of the respective business, function or Affiliate to make the terms of this Policy binding on their employees and independent contractors and adopt disciplinary sanctions in case of violations of this Policy. (Suspected) breaches must immediately be notified to the Privacy Office.

1.3 What does this Policy cover?

The Policy applies to any and all types of processing of personal data relating to all individuals ("data subjects") whose data we receive, create or otherwise process in the context of our activities (e.g. customers, HCP's, suppliers, etc.) and independent from whether these are undertaken electronically or in paper form.

It covers the processing of any information, which we can directly or indirectly link back to an individual person. This could be a name, an address, a telephone number, a patient number, a preference or personal interest, a professional position, a membership, an IP address, an image, a system log, etc. Data can fall within the scope of the definition of "personal data", regardless whether it is publicly available or confidential, whether you have the name of the individual or whether the data is collected or processed in a professional context or not.

The way we collect, store, transfer, protect and otherwise process personal data at Terumo varies depending on criteria such as the sensitivity of the personal data, the type of data subject to whom it relates (e.g. patients, employees, customers, …) or the public availability of the data. To this effect, we have developed a Personal Data Classification and Handling Policy distinguishing between Restricted Data, Confidential Data and Internal Data. This Classification is used to determine appropriate access rights, data deletion terms and other IT or organizational measures to protect our data.

2. PROCESS

How do we handle the protection of privacy and the processing of personal data? [1]

2.1 Role of Terumo

With the exception of a few activities (such as activities we perform on behalf of other Terumo group entities, or limited cases where we process personal data upon request of our customer), Terumo qualifies as Data Controller in the sense of the GDPR. This means that Terumo decides on the purposes and the means of the processing and is the primary responsible for compliance with applicable laws and regulations in the field of privacy and data protection.

2.2 Principles of Data Protection

When we process personal data, you must observe the following key data protection principles:

1. **Transparency**:

   You will need to provide the relevant individuals with the necessary information about what data we process about them and how. The Terumo Privacy Office has developed a Standard Information Notices regarding Protection of Privacy and the Processing of Personal Data and ensures the concerned individuals are at the appropriate time informed about (changes to) the processing of their personal data by Terumo.

2. **Lawfulness**:

   You may only process personal data in so far as we have a clear and defined legal basis to do so. An acceptable legal basis can be one of the following:

   a) The processing is necessary in view of the conclusion or for the execution of a contract with the data subject, e.g. name, function, contact data, account number, expense information of HCP to be able to reimburse expenses or other costs foreseen in the consultancy agreement

   b) The processing is necessary to comply with our legal obligations, e.g. transfer of payroll and benefit information of Affiliates to tax authorities to comply with our social security obligations

   c) The processing is necessary for a legitimate business interest we aim to pursue, e.g. HR evaluation data in the context of our employer authority; video surveillance data to protect the security and safety of our premises and our Associates; information about purchases or interests of our existing customers1 to inform them about updates, events or new releases about similar products.

   d) The data subject has provided a clear and informed consent, e.g. clinical trial data based on the patient consent form; the preferences and contact information of prospects when they have explicitly indicated the interest and accepted to receive information about certain products or events

   If none of the above apply, you can reach out to the Terumo Privacy Office for further instruction.

[1] Processing of personal data for **direct marketing** processes is strictly regulated. Direct marketing is a broad concept and covers the sending of newsletters, invitations to events, information about products or services as well as the preparatory actions (e.g. profiling or analysing preferences to tailor a certain message). Processing of personal data for direct marketing purposes can be based on legitimate interest e.g. if for *existing customers* for similar products but usually requires an explicit ('opt-in') consent e.g. direct marketing to *prospects*. Consult the Privacy Office for further guidance in case of specific questions or before launching new marketing and communication campaigns

3. **Security and confidentiality:**

   Within Terumo, we take appropriate technical and organizational measures to protect data from unauthorized and unlawful processing, unauthorized access or transmittal, accidental loss, accidental amendment, destruction or damage. Measures in place include confidentiality obligations on our Associates, access rights and identity management, training programs on data protection and privacy, encryption and pseudonymisation techniques to secure data, policies and processes relating to the processing of personal data, etc. For more information, consult the Terumo Corporate Information Security Policy. If you consider that additional measures are needed, discuss this further with the Terumo Privacy Office.

4. **Purpose limitation and data minimization:**

   It is important that you identify the reason why you collect or process data upfront and in a clear manner. You must only process data for as long and in so far we need it for that purpose. If we do not absolutely need data, we do not collect it. If we no longer need it or we do not know why we still have it, we stop processing it. Do not reuse data for a purpose, which is incompatible with the purpose for which you originally collected it, unless the individual agrees with it or there is a different legal basis to do so.

5. **Data protection by design and by default:**

   Aim to integrate privacy right from the start into the specifications and the architecture of data-processing systems and activities by technical means ("data protection by design") and by data protection friendly settings ("data protection by default") in order to facilitate compliance with the principles of the protection of privacy and data protection. Where you want to call upon a vendor, try to select a vendor with a privacy-friendly solution. When you are working to implement a new process or new application, strive to configure it in a way that it protects and respects privacy and data protection rights. Also consider the possibility of using dummy data or anonymous data or implement pseudonymisation as a way to minimize the data and the processing.

6. **Data quality:**

   Collect and only work with accurate data and try to maintain it up-to-date. If you see that data is incomplete or inaccurate, rectify, supplement, update and/or erase it without undue delay.

7. **Deletion and Storage limitation:**

   Avoid storing data longer than necessary for the purposes for which you originally started processing it. Consult our Document Retention Policy setting forth our standard company retention periods (largely based on the statutory retention periods) and the type of action which we take when a retention period lapses (archiving, deletion, destruction, anonymization, restriction of the processing or other).

2.3 Documentation duties

We must at all times be able to demonstrate compliance with the provisions of this Policy. The capability to provide such evidence shall be secured in particular by definitive and comprehensive documentation, which shall be centralized at the level of the Terumo Privacy Office and will include at least the Register of Processing Activities (the Data Register) as imposed under the GDPR.

The Data Analyst within the Privacy Office is responsible to maintain this Data Register and keep it up to date, where needed with support from the Data (Process) Owners.

When starting or changing an activity, consult with the Data Analyst and/or the respective Data (Process) owner so that the Terumo Data Register can be completed accordingly and other necessary compliance actions can be initiated.

The Terumo Privacy Office shall, on behalf of the respective Group Company, provide the competent supervisory authority with the (excerpt of the) Data Register on request and handle further discussions with such authority in close co-ordination with the respective Terumo entity management.

2.4 Risk Evaluation and Data Protection Impact Assessment

Each processing activity as reflected in the Register must be subject to a risk analysis to see whether it likely entails a high risk for the data subject.
If so, the Data (Process) Owner shall be responsible to conduct a Data Protection Impact Assessment (DPIA) in line with the GDPR, as the case may be with support from the Terumo Privacy Office.

A DPIA must be documented and performed based on the Terumo DPIA Methodology (see Terumo DPIA Form).

If the measures proposed to mitigate the high risk of the envisaged data processing to an acceptable level, do not seem to be sufficient, the Terumo Privacy Office will co-ordinate with business or function management to report to senior management and, as the case may be, initiate a consultation with the competent data protection authority as required by the GDPR.

2.5 Transfer of Personal Data

When we transfer data, whether within Terumo (e.g. per e-mail) or outside of Terumo (e.g. to service providers), we must also make sure the data protection principles are respected.

For data transfers to third parties the Terumo Privacy Office has developed specific contract templates which are available on the Terumo intranet.

For data transfers between Terumo entities, Terumo has put in place an Intragroup Framework Data Processing Agreement, to which Terumo entities have adhered to. Inform the Terumo Privacy Office of new intragroup data transfers you become aware of so that the Intragroup Data Processing Agreement can be updated if needed.

In the event that the recipient of personal data is located in a country outside the European Union or the European Economic Area (hereafter "Third Country"), specific measures are required to protect the rights and interests of the data subjects. Where there is a necessity to transfer personal data to a Third Country, the Terumo Privacy Office shall be consulted beforehand.

2.6 Processors: vendor selection and due diligence process

To the extent the processing of personal data is conducted by external service providers (e.g. for payroll accounting, conducting of advertising measures, IT services) qualifying as "data processors" in the meaning of the GDPR, Terumo at all times remains responsible for the compliance by the external service provider with this Policy and the applicable privacy and data protection laws.

If an external service provide needs access to personal data, the Terumo Privacy Office must be notified beforehand.

Processors must be selected carefully based on their expertise and approach relating to privacy (see Terumo Vendor Questionnaire. The Terumo procurement team involved shall document the selection of the Processor.

For every Processor, we need to ensure that an agreement is concluded making sure the Processor solely processes the transferred data strictly according to instructions and for the specified purposes. For this, the Terumo Standard Data Processing Agreement (DPA) shall be used. Each amendment to the Standard or, as applicable, the entering into an agreement provided by the external service provider is subject to prior review and sign-off by the Terumo Privacy Office.

The business unit or function responsible for the instruction shall further document their instructions to the Processor regarding the data processing. The signed Agreement and any further documented instruction shall be provided to the Terumo Privacy Office.

Depending on the risk level of the data processing, the compliance of the Processor shall be monitored during the contractual term on a regular basis. The results of the review(s) shall be documented.

2.7 Rights of Data Subjects

A data subject – independent of age, domicile or nationality – has specific rights with respect to the processing of his/her personal data. This includes the right to information, the right to access, the right to rectification, the right to erasure, the right to restriction of the processing, the right to data portability, the right to object or the right to withdraw a consent given.

With each request of a data subject relating to the processing of his/her personal data, it is important to determine the identity of the data subject beyond reasonable doubt and to assess whether the request is sufficiently founded, meets the respective conditions of the law and is not excessive.

In any case, before responding, always consult with the Terumo Privacy Office for guidance and/or template answers. The Terumo Privacy Office should be kept in copy of all correspondence.

2.8 Personal Data Breach and interaction with (privacy) authorities

We count on you to notify violations of this Policy or any laws or regulations relating to the Protection of Privacy and the Processing of Personal Data. You can do so by contacting the Terumo Privacy Office directly, by speaking to your direct line manager and/or by raising an issue through other communication channels available to you.

In particular, it is of utmost importance that you inform at least the Terumo Privacy Office from the moment that you become aware or have reasonable grounds to suspect:

- the unlawful disclosure or transfer of personal data eg payroll data are put on a public drive or sent to the wrong email address
- the unlawful access to personal data eg attack on our IT systems
- the loss of personal data, eg. USB stick loaded with customer contact details is lost on the train
- any other event which potentially can affect the confidentiality, availability, integrity or resilience of our systems and/or data

You can notify an incident or suspected incident by following the Terumo Data Breach Procedure and completing the Data Breach Notification Form. To enable us to swiftly assess the incident, engage with other stakeholders and, if need be, notify the breach to the competent supervisory authorities, we underline the importance to complete this Form as much as possible. Timing is of the essence as we need, in certain countries, to notify a breach within 72hours after becoming aware of it.

Only the Privacy Office will be competent to deal or otherwise interact with (privacy) authorities or other third parties requesting access to our data. When you receive a complaint, question or in the event of a visit by authorities at the Terumo premises, immediately contact the Privacy Office and your direct line manager.

3. Privacy Compliance

How do we ensure ongoing privacy compliance?

3.1 Governance structure and strategy

We have set up a Governance Structure and Strategy to ensure and monitor compliance with this Policy and the applicable laws and regulations in the field of privacy and data protection including;

- A **Privacy Committee** with senior representatives from the business units
- A central multidisciplinary **Privacy Office** within Terumo Europe NV
- *Ad hoc* **Privacy Working Groups** advising or supporting on specific topics or issues
- **Privacy Point of Contacts** acting as champions within the different functions and businesses
- **Data (process) owners** per type of processing activity a.

The Terumo Privacy Office will regularly review and update this Policy. The latest version will be available on the Terumo Intranet.

3.2 Training

a. All Affiliates or independent contractors within Terumo who have access to personal data will receive appropriate training.

b. The Terumo Privacy Office shall prepare, in co-ordination with the HR responsible and the direct line managers or representatives of the different business units or functions a training plan and decide on the form and frequency of the corresponding training sessions per profile.

3.3 Audits

Compliance with the Policy shall be reviewed on a regular basis by audits by Internal Audit,. Internal Audit will handle and report the audit according to its internal procedures. If an audit reveals any failure to comply with this Policy or with any applicable national privacy laws, Terumo will take action to remediate such failure to comply.

4. Questions

Any further questions?

For all your questions, questions or concerns relating to the protection of privacy or the processing of personal data in the context of your professional activities within Terumo, you can always reach out to the Privacy Point of Contact within your function or business unit, your direct line manager and/or contact the Terumo Privacy Office directly as follows:

TERUMO Privacy Office
Terumo Europe NV (Belgium)

E-mail: privacy@terumo-europe.com