GENERAL POLICY FOR PROCESSING OF PERSONAL DATA IN FERROSAN MEDICAL DEVICES

Data controller

The Legal entity responsible for the processing of your personal data is:

Ferrosan Medical Devices A/S

CVR: 32942342

Sydmarken 5
DK-2860 Soeborg
Tel.: +4570252860
info@ferrosanmd.com

The responsible data controller can be reached at:

E-mail: gdpr@ferrosanmd.com

Purpose

The purpose of this general policy for processing of personal data is to ensure that Ferrosan Medical Devices (hereinafter "FeMD") is compliant with the legal requirements for processing personal data (collectively "Data Protection Laws"), including the, at any time in effect, national data protection laws and the general data protection regulation (”GDPR” - 2016/679).

Protection of personal data is a priority for FeMD. Therefore, the purpose of this policy is to ensure that FeMD is processing personal data responsibly and in compliance with the Data Protection Laws, including GDPR. This procedure sets out the general requirements for processing personal data within FeMD, and thus the scope of FeMD's internal guidelines for processing personal data. These internal guidelines for processing personal data will contribute to ensure that FEMD establishes suitable and effective procedures to manage risks when processing personal data, and thus minimize the risks related to processing personal data for FeMD as well as the data subjects.

Background

FeMD comprises two companies that both provide a range of innovative products used by health care professionals in the Fields of surgery and diagnostics. The technology includes Biomaterials used as haemostatic agent for surgery to control bleeding, and miniature Electromechanics used in devices for regional anesthesia and minimal invasive surgery.

The GDPR applies from the 25th of May 2018 and entails a number of requirements for FeMD in regards to processing of personal data, FeMD's ability to document how personal data is processed and how FeMD is complies with the rules.

Scope

This policy applies to all employees, including temporary employees, in FeMD. The policy is applicable to all processing or any access to personal data, which is part of the work carried out in FEMD. Consultants must when entering into an agreement be instructed to comply with the relevant parts of this policy compared to the scope of the assignment.

Definitions

Employees	Includes all employees and temporary employees.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

	alteration, retrieval, consultation, use, erasure or destruction
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

REQUIREMENTS FOR PROCESSING PERSONAL DATA

General requirements

All processing of personal data in FeMD must be in compliance with the Data Protection Laws.

All employees at FeMD are required to comply with this procedure, and other at any time effective internal guidelines, policies and procedures for processing personal data.

FeMD must ensure that any person, performing any type of work for FeMD and in this regard accesses personal data, only processes these data in accordance with appropriate instructions unless the processing is required pursuant to EU law or other legislation.

New or altered processing

Before any new processing of personal data or introducing any significant changes in existing processing of personal data, necessary steps must be taken to ensure that the processing going forward will be compliant with the GDPR.

Principles for processing

The following general principles must be complied with when processing personal data, and FeMD must - as data controller - be able to demonstrate compliance with these.

Good practices for processing personal data

Any processing of personal data must be in accordance with the good practices for processing personal data. Good practices for processing personal data means that the processing is lawful and fair, and that the data subjects receives sufficient information on what the data will be used for.

Purpose

Personal data may only be collected for one or more legitimate purposes, which must be defined at the time of collection. Personal data may - as a rule of thumb - only be processed for those purpose for which it was collected. However, personal data collected for a specific purpose may be processed for another purpose, if this purpose is compatible with the original purpose for which the data was collected, if consent from the data subject has been obtained or if the further processing is authorized by Union or Member State law.

Data minimization

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Thus there cannot be any processing of data which is not necessary or proportionate.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. FeMD must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation and deletion

Personal data must be erased or anonymized, when it is no longer necessary to process them in relation to the purpose for which they were originally collected or any other subsequent compatible purposes.

The general data retention policy of FeMD sets out further requirements for when personal data must be deleted.

Protection

Personal data must be processed by FeMD in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Accountability and documentation

FeMD ensures by means of registering, compliance overview, controls and documentation that the organization is compliant with the Data Protection Laws.

Lawfulness of processing

Personal data may only be processed where a legal basis exists in the Data Protection Laws. The legal basis for the respective processing activities is described further within the internal guidelines.

Description of the processing

1) There will be processed personal data in connection with written communication with a data subject. The data is typically; Contact info, name, job position, phone number, address, e-mail address. This information is used to communicate with and identify the data subject. The source of the data is the data subject.

2) There will be processed personal data in connection with FeMD entering into cooperation with a data subject. The data is typically; Contact info, name, job position, phone number, address, e-mail address. This information is used to communicate with and identify the data subject as well as a mean of documentation in terms of proving who have performed certain services. The source of the data is the data subject.

Storage

FeMD stores records containing personal data as long as it is necessary to the purpose which is was collected for. Generally all data will be deleted 12 months after the collection, if there is no lawfulness of processing in GDPR art. 6 or art 9 stipulating a longer retention period. Deletion will partially be carried out by automated processes to ensure consistency.

Transparency and rights of the data subjects

Duty of notification

When personal data is collected about the data subjects, FeMD must provide the data subjects with information about the intended processing. This applies irrespective whether the information is collected directly from the data subject or from a third party. In practice this is done through Privacy Policies which - depending on the circumstances - is communicated directly to the data subject or made available by other means.

Requests from data subjects

The data subjects have certain rights, when FeMD is processing personal information about them, including a right to - when certain requirements are met - access to, rectification of, update or erasure of information, and to have the processing restricted or seized on requrest. FeMD respects these rights, and have established relevant procedures for handling a request from the registered to use these rights.

The Data subject (below here “You”) have the following rights:

- You have the right to request access to and rectification or erasure of your personal data.
- You also have the right to object to the processing of your personal data and have the processing of your personal data restricted.
- In particular, you have an unconditional right to object to the processing of your personal data for direct marketing purposes.
- If processing of your personal information is based on your consent, you have the right to withdraw your consent at any time. Your withdrawal will not affect the lawfulness of the processing carried out before you withdrew your consent. You may withdraw your consent by [insert modality].
- You have the right to receive your personal information in a structured, commonly used and machine-readable format (data portability).
- You may always lodge a complaint with a data protection supervisory authority, e.g. The Danish Data Protection Agency.

There may be conditions or limitations on these rights. It is therefore not certain for example, that you have the right of data portability in the specific case - this depends on the specific circumstances of the processing activity.

Data Protection Impact Assessment

Where processing activities, which are likely to result in a high risk to the rights and freedoms of natural persons, FeMD will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment or "DPIA").
FeMD has assessed and will continuously asses any processing of personal data in RISMA, and FeMD has taken the required precautions.

FeMD must consult with the supervisory authorities before any processing is initiated, if a DPIA indicates that the processing is likely to result in a high risk, which cannot be mitigated by compensatory measures.

Third parties

Data processors

When FeMD make use of data processors for processing of personal data, FeMD must - before the data processor gets access to the personal data - ensure:

- That the data processor can establish appropriate technical and organizational measures to ensure a level of security appropriate to protect the personal data, that the data processor is processing on behalf of FeMD
- Conclude a written data processing agreement that meets the requirements of the Data Protection Laws.

FeMD must therefore ensure through continuous monitoring that the data processor is compliant with the rules and oblige the data processors to perform continuous monitoring of their sub-processors.

FeMD might share records with:

- Business partners within IT support/assistance

- Public authorities

- Customers/distributors

- Consultants

- Suppliers/Sub suppliers

Third country transfers

Transfer of data to countries outside the EEA, which have not been deemed by the Commission of the European Union to have an adequate level of protection of personal data, may only occur when FeMD has provided a legal basis for the transfer. Such circumstances are handled by the Legal department.

IT-security

Security of processing

FeMD shall implement appropriate technical and organizational measures and a level of security appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes as well as the risk of the processing.

Moreover, FeMD's IT-security policy on information security will apply for protection of personal data, including requirements for encryption, access control, logging etc.

Personal data security breach

Plans and procedures

FeMD has procedures in place for handling personal data breaches including examples of data breaches. The procedure involves all relevant staff.

Data breaches

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In case of a personal data breach FeMD should notify the personal data breach to Datatilsynet without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless FeMD is able to demonstrate, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification. If the information cannot be provided at the same time, the information may be provided in phases without undue further delay.

In the event that the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, FeMD shall communicate the personal data breach to the data subject without undue delay, unless the Data Protection Laws authorizes an exemption. Procedures describing how to handle breaches are established in internal procedures.

Awareness-raising and training programs

FeMD have appropriate awareness-raising and training programs modified to FeMD's situation, that ensures that the employees obtains sufficient knowledge of the Data Protection Laws, this policy and FeMD's other internal guidelines and policies.

All employees who process or access records containing personal data for which FeMD is responsible, must acknowledge that they have read and understood this policy.

Responsibility and governance

The executive board has the overall responsibility for complying with this policy in FeMD and actively supporting the implementation of this policy through underlying internal guidelines and procedures regarding processing of personal data.

The legal department has the day-to-day responsibility for ensuring compliance with GDPR and all internal policies and procedures regarding processing of personal data (including this policy). Furthermore they have the responsibility to perform internal controls in relation to this policy and procedures regarding retention periods. The Legal department supervises employees who process personal data on behalf of FeMD, and is the contact-point for public authorities in terms of GDPR related issues.

Reporting

The Legal department shall report annually to the executive board about the follows matters:

- The development of FeMD’s processing and protection of personal data, including suggestions for improvements in the management's risk assessment
- Follow-up on previously identified gaps
- Assessments of whether FeMD's internal guidelines rules and control procedures are sufficient to ensure compliance with Data Protection Laws
- Any suggestions for changes to internal guidelines and control procedures
- Any contact with the supervisory authorities during the year

- 0 -

Last updated: 14. February 2019