1. Purpose, Scope and Users

SOFMEDICA Group includes SofMedica SRL, SofMedica Hellas Medical Technologies S.A., SofMedica Cyprus Ltd., SofMedica Bulgaria EOOD, SofMedica Hungary Kft. and other companies: SofTehnica SRL, Inter Health Systems, ISLE Academy S.S.A., hereinafter referred to as the "Group", strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Group operates. This Policy sets forth the basic principles by which the Group processes the personal data of consumers, customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

This Policy applies to the Group and its directly or indirectly controlled wholly-owned subsidiaries conducting business within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document, bound by this policy, are all employees, permanent or temporary, and all contractors working on behalf of the Group (for example labor medicine services provider, meal tickets providers, payroll services, tourism agencies).

2. Reference Documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Relevant national law or regulation for GDPR implementation for each company in SOFMEDICA Group
- Other local laws and regulations whenever the case.

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation:

Personal Data: Any information relating to an identified or identifiable natural person ("**Data Subject**") 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.

Special Personal Data: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data (examples when Group companies act as a data controller – when receives sponsorship request for doctors' personal data communicated to the congress organizer; for the personal data of its employees).

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller (for example whenever receives medical data of the patients from the hospitals).

Processing: An 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, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

Anonymization: Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by any other person to identify that individual. The personal data processing principles do not apply to anonymized data as it is no longer personal data.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymization reduces, but does not completely eliminate, the ability to link personal data to a data subject. Because pseudonymized data is still personal data, the processing of pseudonymized data should comply with the Personal Data Processing principles.

Cross-border processing of personal data: Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Supervisory Authority: An independent public authority which is established by a Member State pursuant to Article 51 of the EU GDPR;
Each "**local supervisory authority**" will still maintain in its own territory, and will monitor any local data processing that affects data subjects or that is carried out by an EU or non-EU controller or processor when their processing targets data subjects residing on its territory. Their tasks and powers include conducting investigations and applying administrative measures and fines, promoting public awareness of the risks, rules, security, and rights in relation to the processing of personal data, as well as obtaining access to any premises of the controller and the processor, including any data processing equipment and means.

"Main establishment as regards a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

"Main establishment as regards a processor" with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
Company: Any individual company in SOFMEDICA Group.

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organizations handling personal data. Article 5(2) of the GDPR stipulates that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*."

4.1. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.2. Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3. Data Minimization

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The Group must apply anonymization or pseudonymization to personal data, if possible, to reduce the risks to the data subjects concerned.

4.4. Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified in a timely manner.

4.5. Storage Period Limitation

Personal data must be kept for no longer than is necessary for the purposes for which the personal data are processed according to the local legal/contractual obligations.

4.6. Integrity and confidentiality

Taking into account the state of technology and other available security measures, the implementation cost, and likelihood and severity of personal data risks, the Group must use appropriate technical or organizational measures to process Personal Data in a manner that

ensures appropriate security of personal data, including protection against accidental or unlawful destruction, loss, alternation, unauthorized access to, or disclosure.

4.7. Accountability

Data controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

5. Building Data Protection in Business Activities

In order to demonstrate compliance with the principles of data protection, SOFMEDICA Group should build data protection into its business activities.

5.1. Notification to Data Subjects

(See the Fair Processing Guidelines – section 6 below.)

5.2. Data Subject's Choice and Consent

(See the Fair Processing Guidelines section– section 6 below.)

5.3. Collection

SOFMEDICA Group must strive to collect the least amount of personal data possible. If personal data is collected from a third party, each employee must ensure that the personal data is collected lawfully.

5.4. Use, Retention, and Disposal

The purposes, methods, storage limitation and retention period of personal data must be consistent with the information contained in the Privacy Notice. SOFMEDICA Group must maintain the accuracy, integrity, confidentiality and relevance of personal data based on the processing purpose. Adequate security mechanisms designed to protect personal data must be used to prevent personal data from being stolen, misused, or abused, and prevent personal data breaches. Each company is responsible for compliance with the requirements listed in this section.

5.5. Disclosure to Third Parties

Whenever the Group uses a third-party supplier or business partner to process personal data on its behalf, the responsible employee for the relationship/related activities must ensure that this processor will sign an agreement which will provide security measures adopted to safeguard personal data that are appropriate to the associated risks (such as misuse of personal data, an authorized disclosure of personal data, data breaches, etc).

The Group must contractually require the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to carry out its contractual obligations towards the Group or upon the instructions of the Group and not for any other purposes. When the Group processes personal data jointly with an independent third party, the Group must explicitly specify its respective responsibilities of and the third party in the relevant contract or any other legal binding document, such as the Supplier Data Processing Agreement.

5.6. Cross-border Transfer of Personal Data

Before transferring personal data out of the European Economic Area (EEA) adequate safeguards must be used including the signing of a Data Transfer Agreement, as required by the European Union and, if required, authorization from the relevant Data Protection Authority must be obtained. The entity receiving the personal data must comply with the principles of personal data processing set forth in Cross Border Data Transfer Procedure.

5.7. Rights of Access by Data Subjects

When acting as a data controller, each company of the Group is responsible to provide data subjects with access their personal data, and must allow them to update, rectify, erase, or transmit their Personal Data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure Chapter.
When acting as a data processor, each company of the Group is responsible to notify the controller of the data.

5.8. Data Portability

Data Subjects have the right to receive, upon request, a copy of the data they provided to us in a structured format and to transmit those data to another controller, for free. Data Protection Officer is responsible to ensure that such requests are processed within one month, are not excessive (i.e., requests sent daily) and do not affect the rights to personal data of other individuals (other person's rights to privacy).

5.9. Right to be Forgotten

Upon request, Data Subjects have the right to obtain from each company of the Group the erasure of its personal data. When the companies from the Group are acting as a Controller, Group Compliance Director must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

6. Processing Rules

Personal data must be processed fair and transparent only when required by the nature of the activities and/or by the law.
Each company of the Group must decide whether to perform the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

6.1. Notices to Data Subjects

At the time of collection or before collecting personal data for any kind of processing activities including but not limited to selling products, services, or marketing activities, each company of the Group is responsible to properly inform data subjects of the following: the types of personal data collected, the purposes of the processing, processing methods, the data subjects' rights with respect to their personal data, the retention period, potential international data transfers, if data will be shared with third parties and the Group's security measures to protect personal data.

This information is provided through Privacy Notice. Each company of the Group develops different notices which will differ depending on the processing activity and the categories of

personal data collected – for example for employees, for job candidates, for visitors when video cameras are installed, for the website when data is collected etc.

Where personal data is being shared with a third party, each company must ensure that data subjects have been notified of this through a Privacy Notice.

Where personal data is being transferred to a third country according to Cross Border Data Transfer Policy, the Privacy Notice should reflect this and clearly state to where, and to which entity personal data is being transferred.

Where special personal data is being collected the Privacy Notice explicitly states the purpose for which this special personal data is being collected.

6.2. Obtaining Consents

Whenever personal data processing is based on the data subject's consent each company will be responsible for retaining a record of such consent, for providing data subjects with options to provide the consent and must inform and ensure that their consent (whenever consent is used as the lawful ground for processing) can be withdrawn at any time. Examples of situations when consent is required: for retaining CV-s of the candidates which are not hired, for employees which participate at company events etc.

Where collection of personal data relates to a child under the age of 16, each Group company must ensure that parental consent is given prior to the collection using the Parental Consent Form. Each Group company shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

When requests to correct, amend or destroy personal data records, each company must ensure that these requests are handled within a reasonable time frame, are recorded and to keep a log of these requests.

Personal data must only be processed for the purpose for which they were originally collected. In the event that the SOFMEDICA Group wants to process collected personal data for another purpose, it must seek the consent of its data subjects in clear and concise writing or make an update of the Privacy Notice and inform the data subjects about this update, where no consent is required. Any such request should include the original purpose for which data was collected, and also the new, or additional, purpose(s). The request must also include the reason for the change in purpose(s). Each company is responsible for complying with the rules in this paragraph.

Now and in the future, each company must ensure that collection methods are compliant with relevant law, good practices and industry standards.

Each company is responsible for creating and maintaining a Register of the Privacy Notices.

7. Organization and Responsibilities

The responsibility for ensuring appropriate personal data processing lies with everyone who works for or with SOFMEDICA Group and has access to personal data processed by the Group.

The key areas of responsibilities for processing personal data lie with the following organizational roles:

The Board of Directors or other relevant decision-making body makes decisions about, and approves the Group's general strategies on personal data protection.

The **Legal Affairs Department/Counsel together with the designated person,** monitors and analyses personal data laws and changes to regulations, develops compliance requirements, and assists business departments in achieving their Personal data goals.

The **IT manager** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.

The **Marketing Manager** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with the Data Protection Officer to ensure marketing initiatives abide by data protection principles.

The **Human Resources Manager** is responsible for:

- Improving all employees' awareness of user personal data protection.
- Organizing Personal data protection expertise and awareness training for employees working with personal data.
- End-to-end employee personal data protection. It must ensure that employees' personal data is processed based on the employer's legitimate business purposes and necessity.

The **Procurement Manager** is responsible for passing on personal data protection responsibilities to suppliers and improving suppliers' awareness levels of personal data protection as well as flow down personal data requirements to any third party a supplier they are using. The Procurement Department must ensure that each company reserves a right to audit suppliers.

8. Response to Personal Data Breach Incidents

When a company from SOFMEDICA Group learns of a suspected or actual personal data breach it must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the current section. Where there is any risk to the rights and

freedoms of data subjects, each company must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

9.1 Personal data breach notification: Data controller to supervisory authority

When the personal data breach or suspected data breach affects personal data that is being processed by each company as a data controller, the following actions are performed by the designated person:

1) Each company must establish whether the personal data breach should be reported to the Supervisory Authority.

2) If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. However, the data breach should be recorded into the Data Breach Register.

3) The local National Supervisory Authority must be notified with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.

The company will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Contact person
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

9.2 Personal data breach notification: Data controller to data subject

Each company must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject. If yes, the company must notify with undue delay the affected data subjects.

The Notification to the data subjects must be written in clear and plain language and must contain the same information listed in Section above.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, each company must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

9.3 Personal data breach notification: Data processor to data controller

When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, each company acting as a data processor must report any personal data breach to the respective data controller/controllers without undue delay.

The designated person will send Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

Each company will record the data breach into the Data Breach Register**.**

9. Audit and Accountability

Each company is responsible for auditing how well business departments implement this Policy. Any employee who violates this Policy will be subject to disciplinary action and the employee may also be subject to civil or criminal liabilities if his or her conduct violates laws or regulations.

10. Processing of Employee Personal Data

10.1 Legitimate Purposes for Processing Employee Personal Data – each company may process employee Personal Data for legitimate purposes which include but not limited to:

a) **Human resources management**. This purpose includes human resource management activities carried out during recruitment or the performance of an employment contract, such as interviews, on boarding, termination of employment, attendance, performance management, compensation and benefits, training, employee services, health and occupational safety, and other activities for the purpose of human resource management or protecting the vital interests of employee.
b) **Other business operations.** This purpose includes business activities such as managing travel and expenses, managing company assets, providing IT services, information security, conducting internal audits and investigations, fulfilling the obligations of business contracts, legal or business consulting, and preparing for legal litigation, etc.
c) **Compliance with the law**. The Processing of employee Personal Data in order to comply with a legal obligation, for example the disclosure of employee Personal Data to a tax authority in order to comply with applicable tax laws.

10.2 Requirements for the Processing of Employee Personal Data
Any Processing of employee Personal Data by each company must be for a legitimate purpose, and must comply with the following requirements:

a) **Notification to Employees** - For the purpose of transparency of employee Personal Data Processing, when each company collects the Personal Data of an employee, the employee should be notified of the types of data being collected, the purpose and types of Processing, the employee's rights, and the security measures taken to protect the Personal Data. Notification may take the form of the publication or updating of statements on the protection of employee Personal Data, for example: the insertion of

terms on employee Personal Data protection in employment contracts by the Employee Relationship Department/HR; the insertion of Personal Data Statement to relevant IT systems by the Quality, Business Process & IT Management Department.

b) **Employee Choice and Consent** - In principle, each company may Process employee Personal Data for a legitimate purpose as an employer and generally it may do so without obtaining the consent of the employee, to improve the efficiency of internal operation.
Human resource management activities such as interviews, on boarding, termination of employment, attendance, compensation and benefits, employee services, health and occupational safety may involve the Processing of Special Personal Data. If country specific laws or regulations govern these issues (for example, obtaining the consent of the employee), the company shall take these laws or regulations into account. Each country is responsible for identifying specific compliance requirements and for ensuring compliance.

c) **Collection** - Each company must collect employee Personal Data for legitimate purposes, and must comply with the principle of Data Minimization. If the Personal Data of a job candidate or employee is collected from a third party (e.g., recruitment or background check agencies), each company must make best efforts to ensure that the third party obtained the Personal Data by legitimate means.
No company may collect Personal Data of job candidates or employee in a way which is inconsistent with the law or business ethics.

d) **Use, Retention, and Disposal** - Each company must use, retain, and dispose of employee Personal Data in a manner which is consistent with the notification to the employee. It must also ensure its accuracy, integrity, and relevance. They must take appropriate security measures to protect the employee Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized access, or disclosure according to Information security policy and other documents that describe data security.

Each company must not unlawfully destroy or alter employee Personal Data. They must not access, sell, or provide employee Personal Data to any third party unlawfully or without authorization.

In the course of business operations, the employee Personal Data may be Processed in the following ways to minimize data protection risk: employee Personal Data may be anonymized for the purpose of irreversible de-identification; or data may be aggregated into statistical or survey results. (The Personal Data Processing principles do not apply to anonymized data and aggregate data as they are not Personal Data.)

e) **Disclosure to a Third Party** - When companies need to disclose employee Personal Data to a supplier, business partner, or other third party, they should seek to ensure that the supplier, business partner or other third party will provide security measures to safeguard employee Personal Data that are appropriate to the risks associated. They should also require the third party to provide the same level of data protection as the company by contract or other arrangement.

Besides, when companies disclose employee Personal Data in response to a request from a law enforcement agency or judicial authority, they will seek legal advice in order to handle the request.

f) **Cross-border Transfer of Employee Personal Data** Different countries impose different requirements for the cross-border transfer of Personal Data (such as no limitation, conditional limitation, or a prohibition against transfers of certain types of Personal Data out of the country). Before transferring Personal Data out of a country, each company must seek legal advice in order to determine whether the cross-border transfer is necessary and legal.

When transferring employee Personal Data out of the European Economic Area, the transferor and the transferee must have signed a data transfer agreement in compliance with EU regulations and Cross Border Data Transfer Policy. The transferee must provide adequate protection for the data transferred in accordance with the data transfer agreement.

g) **Employee Access** – Each company must provide reasonable means for employees to access Personal Data held about them and allow employees to update, correct, erase, or transmit their Personal Data if appropriate or required by law. When responding to an employee request for access, the company may not provide any Personal Data until they have verified identity of the employee. The Group needs to make sure that they know the identity of the person making the request before they can send the personal data to the individual.

11. Conflicts of Law

This Policy is intended to comply with the laws and regulations in the place of establishment and of the countries in which SOFMEDICA Group operates, respectively Romania, Greece, Cyprus, Bulgaria and Hungary. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

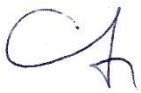
12. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Data Subject Consent Forms	Company server	For employees - human resources department; For patients – reception desk; For other persons – compliance department.	Only authorized persons may access the forms	For employees - 10 years; For patients – 10 years; For other persons – 10 years
Register of Privacy Notices	Company server	Data Protection Officer	Only authorized persons may access the folder	Permanently
Data Breach	Company	Data Protection	Only authorized	Permanently

Register	server	Officer	persons may access the folder	

13. Validity and document management

This document is valid as of 25 May 2018.
The owner of this document is the Compliance Director who must check and, if necessary, update the document at least once a year.

	Name	Function	Signature	
Issued:	Katerina Pappa	Regulatory & Compliance Manager		Date: 20.12.2022
Approved:	Cristina Miroescu	Compliance Director		Date: 20.12.2022