PERSONAL DATA PROTECTION POLICY

Ver. 03 / 01.01.2021

Approved by: ……..

/ Acad. Prof. Lachezar Traykov, MD, D.SC. /

Table of contents

1. Objective and scope

MEDICAL UNIVERSITY – SOFIA, hereinafter referred to as the "Organisation", strives to comply with applicable laws and regulations related to Personal Data protection in countries where the Organisation operates. This Policy sets forth the basic principles by which the Organisation processes the personal data of consumers, trainees, suppliers, partners, employees and other individuals, and indicates the responsibilities of its departments and employees while processing personal data.

This policy applies to MEDICAL UNIVERSITY - SOFIA and its directly or indirectly controlled wholly-owned subsidiaries conducting activities within the European Economic Area (EEA) or processing the personal data of data subjects within EEA.

The users of this document are all employees, permanent or temporary, and all contractors working on behalf of The Organisation.

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)
- Personal data protection law
- Employee Personal Data Protection Policy
- Data Retention Policy
- Data Protection Officer Job Description
- Guidelines for Data Inventory and Processing Activities
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Guidelines
- Cross Border Personal Data Transfer Procedure
- Information security policies
- Breach Notification Procedure

3. Definitions

The following definitions of terms used in this document are drawn from 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.

Sensitive 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.

Data Processor: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

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;

Lead supervisory authority: The supervisory authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data; it is responsible, among others, for receiving the data breach notifications, to be notified on risky processing activity and will have full authority as regards to its duties to ensure compliance with the provisions 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 includes 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;

Group Undertaking: Any holding company together with its subsidiary

4. Basic Principles Regarding Personal Data Processing

The data protection principles outline the basic responsibilities for organisations 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 Organisation 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.

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 Organisation 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 order to demonstrate compliance with the principles of data protection, an organisation should build data protection into its activities.

5.1. Notification to Data Subjects

See the Fair Processing Guidelines section

5.2. Data Subject's Choice and Consent

See the Fair Processing Guidelines section

5.3. Collection

The Organisation must strive to collect the least amount of personal data possible. If personal data is collected from a third party, Data Protection Responsible person 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. The Organisation 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. Data Protection Responsible person is responsible for compliance with the requirements listed in this section.

5.5. Disclosure to Third Parties

Whenever the Organisation uses a third-party supplier or other partner to process personal data on its behalf, Data Protection Responsible person must ensure that this processor will provide security measures to safeguard personal data that are appropriate to the associated risks. For this purpose, the Processor GDPR Compliance Questionnaire must be used.

The Organisation must contractually require the supplier or other partner to provide the same level of data protection. The supplier or other partner must only process personal data to carry out its contractual obligations towards the Organisation or upon the instructions of the Organisation and not for any other purposes. When the Organisation processes personal data jointly with an independent third party, the Organisation 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. Rights of Access by Data Subjects

When acting as a data controller, Data Protection Responsible person is responsible to provide data subjects with a reasonable access mechanism to enable them to 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.

5.7. 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 Responsible person is responsible to ensure that such requests are processed within one month, are not excessive and do not affect the rights to personal data of other individuals.

5.8. Right to be Forgotten

Upon request, Data Subjects have the right to obtain from the Organisation the erasure of its personal data. When the Organisation is acting as a Controller, Data Protection Responsible person must take necessary actions (including technical measures) to inform the third-parties who use or process that data to comply with the request.

6. Fair Processing Guidelines

Personal data must only be processed when explicitly authorised by Data Protection Responsible person. The Organisation 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, Data Protection Responsible person 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 Organisation's security measures to protect personal data. This information is provided through Privacy Notice.

If your Organisation has multiple data processing activities, you will need to develop different notices which will differ depending on the processing activity and the categories of personal data collected – for example, one Notice might be written for mailing purposes, and a different one for shipping purposes.

Where personal data is being shared with a third party, Data Protection Responsible person 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 sensitive personal data is being collected, the Data Protection Responsible person must make sure that the Privacy Notice explicitly states the purpose for which this sensitive personal data is being collected.

6.2. Obtaining Consents

Whenever personal data processing is based on the data subject's consent, or other lawful grounds, Data Protection Responsible person is responsible for retaining a record of such consent. Data Protection Responsible person is responsible 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.

Where collection of personal data relates to a child under the age of 16, Data Protection Responsible person must ensure that parental consent is given prior to the collection using the Parental Consent Form.

When requests to correct, amend or destroy personal data records, Data Protection Responsible person must ensure that these requests are handled within a reasonable time frame. Data Protection Responsible person must also record the requests and keep a log of these.

Personal data must only be processed for the purpose for which they were originally collected. In the event that the Organisation wants to process collected personal data for another purpose, the Organisation must seek the consent of its data subjects in clear and concise writing. 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). The Data Protection Responsible person is responsible for complying with the rules in this paragraph.

Now and in the future, The Data Protection Responsible person must ensure that collection methods are compliant with relevant law, good practices and industry standards.

Data Protection Responsible person is responsible for creating and maintaining a Register of the Privacy Notices.

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

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

The Rector makes decisions about, and approves the Organisation's general strategies on personal data protection.

The Data Protection Responsible person is responsible for managing the personal data protection program and is responsible for the development and promotion of end-to-end personal data protection policies.

The Legal department monitors and analyses personal data laws and changes to regulations, develops compliance requirements, and assists departments in achieving their Personal data goals.

The **IT departments,** are 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 **Administration**, 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 responsible** 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 purposes and necessity.

The **Procurement and Accounting departments** are 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 the Organisation reserves a right to audit suppliers.

7. Response to Personal Data Breach Incidents

When the Organisation learns of a suspected or actual personal data breach, Data Protection Responsible person must perform an internal investigation and take appropriate remedial measures in a timely manner, according to the Data Breach Policy. Where there is any risk to the rights and freedoms of data subjects, the Organisation must notify the relevant data protection authorities without undue delay and, when possible, within 72 hours.

8. Audit and Accountability

The Audit Department or other relevant department is responsible for auditing how well 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.

9. 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 the Organisation operates. In the event of any conflict between this Policy and applicable laws and regulations, the latter shall prevail.

10. 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	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	10 years
Data Subject Consent Withdrawal Form	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	10 years
Parental Consent Form	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	10 years
Parental Consent Withdrawal Form	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	10 years
Supplier Data Processing Agreements	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	5 years after the agreement has expired
Register of Privacy Notices	Protected file server	Data Protection Responsible person	Only authorized persons may access the folder	Permanently

11. Validity and document management

This document is valid as of 01.01.2021.

The owner of this document is the Rector, who must check and, if necessary, update the document at least once a year.