ARENSIA Privacy & Data Protection Policy

I. Data Protection Policy

As part of our operations, ARENSIA Exploratory Medicine assures the necessary compliance with the high level of protection of personal data and multifaceted requirements of the General Data Protection Regulation (GDPR). This policy refers to all parties – employees, vendors, patients and sponsors - who provide any amount of information to our company.

The Data Protection Policy applies worldwide to the ARENSIA Exploratory Medicine Company and is based on globally accepted, basic principles on data protection. For cross-border data transmission among the companies units, the policy provides one of the necessary framework conditions ensuring the adequate level of data protection prescribed by the General Data Protection Regulation[1] .

II. Application of National Laws

The GDPR not only applies to organizations located within the EU but it also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

III. Data Protection Policy Definitions

'Personal data' means 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;

'Processing' means 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, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Controller' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

[1] The Regulation (EU) 2016/679 (General Data Protection Regulation) -

'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'Cross-border processing' 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.

'Data Protection Officer' (DPO) is a designate assigned by the controller and processor of personal data to fulfil the tasks and responsibilities as defined by the Union. He/she does not receive any instructions regarding his/her exercise of tasks, shall not be penalized for performing his/her tasks, reports directly into highest level of management and is bound by secrecy or confidentiality concerning the performance of his/her tasks. The tasks of the DPO are listed in section XII.

IV. Principles for Processing Personal Data

1. Lawfulness, fairness and transparency

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

2. Purpose limitation

The personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1)[2], not be considered to be incompatible with the initial purposes.

3. Data Minimization and Accuracy

The personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The data must be accurate and, where necessary, kept up to date; every reasonable step 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 without delay.

[2] Art.89 GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes - https://gdpr-info.eu/art-89-gdpr/

4. Storage Limitation

The personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)[3] subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

5. Integrity and Confidentiality

The collected data must be processed 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.

V. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases of the GDPR. The privacy and security of the personal data collected is a priority to ARENSIA Exploratory Medicine and it is equally important to ARENSIA that everybody understand how we handle this data:

1. Patient Data

To conduct a clinical trial in line with the Declaration of Helsinki and International Committee of Harmonization (ICH) guideline for Good Clinical Practice (GCP) we collect data to the extent as described in the approved and favourable voted trial protocol. Such data may include health related and other sensitive information.

2. Employee Data

To conduct business globally and comply with government regulations (employment, tax, insurance, etc.), we collect various personal and other data depending on your employment responsibilities, citizenship, location of employment, and other factors.

Such data may include:

- Name;
- ID;
- Phone Number;
- E-mail address;
- Banking and other financial data;
- Government identification numbers - social security numbers, tax payer ID's, driver's license;
- Family-related data

[3] Art.89 GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes - https://gdpr-info.eu/art-89-gdpr/

We may use the data as follows:

- to identify somebody personally;
- to communicate with somebody;
- to comply with human resource requirements;
- to comply with government regulations;
- to provide employee benefits (compensation, health insurance, expense reimbursements, etc.)

3. Customer and Third Party data

To conduct business and fulfil contractual obligations we collect data of contractual partners, such as sponsors, subcontractors and vendors. Such data may include name, business email address, business phone number, banking and other financial details of the company. ARENSIA takes precautions not disclose Personal Data to third parties, other than in accordance with instructions and limited to disclosures to agents and subcontractors of vendor and where ARENSIA has received prior written consent from customer or third party or where such disclosure is required by law.

VI. Contract data processing

Data processing on Behalf means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Protection on Behalf must be concluded with external providers and among affiliates within ARENSIA. The client retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the client. Such services might be used for payroll accounting locally.

VII. Rights of the data subject

1. Right of access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

2. Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right to be forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being

relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

4. Right to restriction of processing

The conditions for consent are strengthened, as the request for consent is given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent is clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language in every document provided by ARENSIA: employment contracts, customers and vendors contracts, including documents provided by Sponsors via ARENSIA. i.e. Inform Consent Form (ICF). It is as easy to withdraw consent as it is given.

5. Right to data portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

6. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

VIII. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employee is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

IX. Processing security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal

data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data.

In particular, the responsible department can consult with its IT and DPO. The technical and organizational measures for protecting personal data are part of Data Protection Officer and must be adjusted continuously to the technical developments and organizational changes.

X. Data protection control;

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the DPO and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the DPO. ARENSIA Exploratory Medicine management must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

XI. Data protection incident, responsibilities and sanctions

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals (e.g. unauthorized reveal of bank account number or details on health insurance) must be notified to the respective Data Protection Agency within 72 hours and to affected individuals without undue delay.

XII. Data Protection Officer (DPO)

A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

DPO responsibilities:

- Educating the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information.

XIII. Data Protection at ARENSIA

The principles as described in this policy and as required by the GPDR are implemented within ARENSIA systems by respective Working Instructions, covering the mentioned topics.