EXINI

Contents

1. Purpose and Scope

1) The purpose of this policy is to describe the basic principles according to which EXINI Diagnostics AB (publ) ("EXINI," "we," "our," or "us") collects, uses, and shares information about employees, clients, suppliers and other relevant individuals. It is to ensure that the collected data in EXINI is treated fairly and in accordance with the legal requirements and international standards.

2) This policy will guide EXINI to strive for compliance with Regulation (EU) 2016/679, the European Union's ('EU') new General Data Protection Regulation ('GDPR'), EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce, Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as national Swedish legal requirements with regards to privacy.

3) This policy provides governing principles to all EXINI agreements and Standard Operating Procedures that entails data collection activities.

2. Relation to other applicable provisions, specific requirements

1) EXINI reserves the right to issue, based on this policy, more specific requirements for handling personal data requirements with respect to individual countries and/or individual business units.

3. Governance of this Policy

Communication and implementation

1) The Policy shall be communicated by Site Manager at EXINI and further implemented by all relevant functional managers.

2) The policy enters into force on the date of EXINI Board approval, as stated on the front page. It is valid until the EXINI Board decides otherwise.

Document owner

3) The Site Manager at EXINI is the owner of the Policy. He/she is responsible for maintaining the accuracy of the policy.

4) The Site Manager at EXINI shall review the policy annually in order to ensure that it remains fit for purpose and complies with all relevant regulations. The policy should be updated and approved annually by the EXINI Board.

Reporting

5) The Site Manager will report on compliance with this policy – data subject rights, security as well as incidents - to the Management and the EXINI Board.

4. General privacy principles

Fair and Lawful processing

1) EXINI shall ensure that processing of personal data will be carried out fairly and lawfully, taking into account the processing conditions of each individual case.

2) EXINI shall always ensure compliance with legal requirements when processing personal data. EXINI's processing of data may be deemed as lawful when:
    a. The data subject has given his/her consent to the processing
    b. The processing is necessary for the performance of a contract with the data subject
    c. The processing is necessary in order to comply with a legal obligation for EXINI
    d. The processing is necessary for the purposes of EXINI's legitimate interest.

3) EXINI as a controller should ensure that personal data are collected directly from the consenting individual. Any data collection from third parties without the knowledge of the data subject should be avoided.
    a. The concerned individual should know what personal data are collected and stored for what purpose, and for how long.
    b. The concerned individual should know the third parties or categories of third parties to which the data may possibly be transferred for further processing.

4) EXINI as a processor should ensure that all personal data collected directly or indirectly, are for explicitly stated and justified purposes.

Sensitive Data

5) EXINI will identify personal data as sensitive data according to article 9 of GDPR. EXINI shall always ensure compliance with legal requirements when processing sensitive data. EXINI's processing of sensitive data may be deemed lawful when:
    a. The data subject has given his/her explicit consent
    b. The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller
    c. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
    d. The processing relates to personal data which are made public by the data subject
    e. Processing is necessary for the establishment, exercise or defence of legal claims

6) Upon EXINI's processing of sensitive data appropriate safeguards must be ensured, as stated in section 11 of this policy. Especially regards to sensitive data EXINI should strive for use of pseudonymized data.

Transparency and data minimization

7) We may only be collecting personal data for explicitly stated and justified purposes and only include information that is adequate, relevant and limited to what is necessary for that purpose. We may not process personal data for any purpose that is incompatible with the purpose for which it was originally collected, unless there is a legal basis for such processing.

8) We may only collect data directly from the data subject. Data collected by us through a third party without the knowledge of the data subject shall be avoided. EXINI is responsible to take appropriate measures to always be transparent in where data was collected from and to who data may be transferred.

9) In consideration of the purpose of processing the data, appropriate measures are to be taken to delete or at least to restrict processing of any data that are no longer required. EXINI shall have routines in place to ensure that no unnecessary personal data are processed by the company.

Data portability

10) When the processing is based on consent and the processing is carried out by automated means, upon request from the data subjects, EXINI must transmit the pertaining data in a structured, commonly used and machine-readable format.

Data quality

11) EXINI shall review and update the data banks, on a regular basis, to delete or to amend data that is not correct or that is no longer necessary for the explicitly stated purposes.

12) To fulfill this requirement EXINI will keep a record of all automatic or structured manual processing of personal data. The record shall contain:
    a. The purpose of each processing,
    b. The categories of data subjects,
    c. The categories of personal data
    d. The categories of recipients,
    e. The transfer to third countries, if applicable

f. The planned time limits for erasure of the different categories of data
g. A general description of the technical and organizational security measures

5. Rights of the person concerned

Information to data subjects

1) The following are the requirements on EXINI to comply with the data subject's rights, both where EXINI acts as a controller or as aprocessor.

2) We will inform the data subjects according to our legal obligations, regarding GDPR. We will strive to inform the data subject in a concise and easy accessible form, using clear and plain language. For the products and systems developed by EXINI the applicable information notice to data subjects will also always be available on each system.

Right of Access, rectification, deletion and restriction of use of data

2) Upon a request from the data subject EXINI will provide more and specific information. Such information should be provided in text form (by letter or email) within reasonable time.

3) The data subject's right of access will be fulfilled according to legal obligations. Should EXINI be limited to fulfill the right of access due to an overriding interest of EXINI or of a third party, e.g. protecting a company secret or protecting the identity of a third party, we will inform the data subject of here.

4) A fee may be charged for the information, insofar as this is admissible under the respective national laws.

5) The data subject has the right to rectification and/or completion should his/her personal data be inaccurate or incomplete. The data subject may demand deleting of his/her data if its storage is unlawful or if the data are no longer necessary for the purpose of processing the data. The data subject may, under certain circumstances, demand that the use of his/her data is restricted. The data subject may object to use of his/her data for direct marketing purposes.

Complaints

If the data subject has any objections against EXINI's processing of his or her data, the individual has a right to lodge a complaint with a supervisory authority (in Sweden Datainspektionen).

6. Use of further data processor

Agreement on privacy

1) EXINI may commission other entities to further process personal data. In such circumstances, EXINI is required to establish an agreement with the data processor documented in a suitable form. This agreement should include the following regulations:
    a. Subject matter of the commission
    b. The processor is bound by the instructions of the commissioning party
    c. The scope of the right to give instructions and the obligations to cooperate
    d. A list of any of the data processor's subcontractors which process personal data
    e. The obligation of the processor to bind its subcontractors by agreements that are equivalent to the agreement with the processor

f. The supervisory obligations of the commissioning party as described in this policy
g. Access rights in order to carry out checks.

7. Data transfer to third parties

1) EXINI may transfer personal data to third parties in compliance with the general privacy principles as set out in this policy and legal requirements.

2) As a subsidiary to Progenics Pharmaceuticals Inc, EXINI may share personal information with its owner. Progenics Pharmaceuticals Inc is certified to participate in the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding personal information collected from the European Union and the European Economic Area (collectively, “EU”), and is thereby in compliance with article 46, 47 or 49 of GDPR. Progenics Pharmaceuticals Inc. adheres to the Privacy Shield Principles of notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access, and recourse, enforcement and liability when it receives or accesses personal information from the EU, in particular, in connection with services provided by its subsidiary EXINI.

3) As a provider of cloud services, EXINI has a business associate agreement with Amazon.com, Inc. to host and process its data in the U.S. Amazon.com, Inc. is certified under the EU-US Privacy Shield and Amazon Web Services (AWS) is covered under this certification, thereby in compliance with article 46, 47 and 49 of GDPR.

8. Information request by public authorities

1) Following information requests, personal data may be disclosed to public authorities insofar as legal provisions expressly allow the disclosure of such data. This applies in particular if such provisions exist for the protection of state security, national defense, maintaining public security, the prevention, investigation or prosecution of criminal offences, for the protection of rights of the person concerned or of rights of third parties.

2) Before disclosing the requested information, EXINI as a responsible entity for processing the data must assess whether and how far the information request is in line with applicable legal provisions. In cases of doubt, the relevant representative from the privacy organization should be consulted.

9. Information and documentation obligations concerning personal data breaches

1) Personal data breaches must be reported to the EXINI Data Privacy Officer (“DPO”). They must be documented and certain minimum information must be obtained in writing using a uniform notification form provided by the DPO. The DPO coordinates with the local management on how to proceed.

2) EXINI will inform the relevant persons and the competent privacy authorities must be as required by law.

10. Data security technical and organizational measures

1) When handling personal data, EXINI will implement appropriate technical and organizational measures with regard to business processes and IT systems. These are to ensure that personal data are protected against accidental or

unlawful destruction, loss, unauthorized alteration or disclosure, unauthorized access, any other form of unlawful processing or unduly long storage periods.

2) Measures applied to ensure security should be aligned with EXINI's IT risk management procedures. Should there be a conflict between IT Controls, applications, process etc. with regards to personal data, it is strongly recommended that the classification of this data be coordinated with the DPO.

3) When developing new instruments of data processing, technology conducive to privacy should be preferred.

11. Review of technical and organizational measures of data processors

1) EXINI should verify the implementation of the technical and organizational measures applied by data processors before they begin with the data processing activities. This verification should also be repeated on a regular basis. The result must be documented in a suitable form.

2) Reviews shall be based on this policy, local public and internal regulations, and country-specific or sector-specific requirements.

3) In carrying out this assessment, EXINI's internal assessment procedures should be used, e.g. privacy audits.

4) EXINI may delegate reviewing to the DPO.

12. Data secrecy

1) EXINI shall
    a. process personal data only within the scope of their respective activities and tasks
    b. not process personal data for other purposes, in particular private purposes
    c. not transfer or otherwise disclose personal data to unauthorized persons. “Unauthorized persons” in this sense can also include colleagues or other employees in the event that they do not need this personal data for their respective activities and tasks.

2) Data secrecy obligations exist independently and irrespective of other existing employee confidentiality obligations, in particular with regard to the company’s business secrets or expertise.

13. Roles and responsibilities

Data Privacy Officer

1) EXINI’s DPO tasks include the strategic planning and coordination of company privacy by establishing a risk-based privacy management system and formulating privacy goals. This includes privacy checks in the form of internal audits. In the event of severe personal data breaches, the DPO can be provided with a direct mandate for an ad-hoc audit.

The EXINI Board

2) The EXINI Board is ultimately responsible to ensure that EXINI handles personal data in accordance with external regulations.

The Site Manager

3) By delegation from the EXINI Board, the Site Manager is given the mandate to develop and implement more detailed guidelines in the area of personal data protection.

Management of the owners of EXINI

4) Management is responsible for implementing and complying with this policy and for communicating it to employees.
    a. This task may be delegated to other persons, such as the DPO.
    b. A direct reporting line to the EXINI Board/Management must be ensured.