1 PURPOSE

The purpose of this policy is to establish the requirements for data management relating to the processing of Personal Data by Accelevir Diagnostics (Company).

2 SCOPE

This document applies to all processing and handling of Personal Data in accordance with the principles established by the General Data Protection Regulation (GDPR).

3 DEFINITIONS

Company: Accelevir Diagnostics

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

EU: European Union

GDPR: General Data Protection Regulation

IT: Information Technology

Data Controller: A person who determines the purposes and the means of the processing of Personal Data.

Data Processor: A legal person, a public authority, a service provider, or other body which processes Personal Data on behalf of the Data Controller

Personal Data: Any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identifiable natural person.

Sensitive Personal Data: Sometimes referred to as "Particular Categories of" Personal Data, these categories include health data, biometric and genetic data, criminal convictions, trade union membership, sex life, and ethnic origin. For clarity, the Company does not collect or capture Sensitive Personal Data.

4 RESPONSIBILITIES

The Company is accountable for compliance with the principles described within the Policies and places responsibility on each employee for compliance.

The Company is responsible for training employees in the protection of Personal Data and for creating appropriate awareness.

This policy applies to all Company business processes utilizing professionally reasonable methods for the handling of Personal Data. The Company will also notify our service providers of the Personal Data policy.

5 KEY ROLES

5.1 Data Controller

The Data Controller has the obligation to implement the technical and organizational measures to protect and demonstrate that use of the data is carried out in accordance with Company Data

Privacy Policies with an aim to capture the principles of the GDPR. Company data privacy policies are reviewed and updated as necessary.

5.2 Data Processor

The obligations of the Data Processor include:

- Obtain authorization from the Data Controller before subcontracting any data processing to a sub-processor (see Section 10.1);
- Maintain the confidentiality of the data processed and utilizing commercially reasonable efforts and responsibility for the data protection any sub-processors;
- Maintain a register of processing activities for which the Company has obtained Personal Data which is not widely and independently disclosed by the Interested Party to other 3rd Parties and includes details of the Data Processor and the Data Controller containing a description and/or link to the existing security and data protection measures (see Section 10.1);
- Cooperate as appropriate with federal, state, and/or regulatory authorities;
- Notify the Data Controller of a data breach;
- Utilize the best available professional standards for data retention and notification of any data breach.

6 PRINCIPLES APPLICABLE TO THE PROCESSING OF PERSONAL DATA

Applicable data protection principles outline Company responsibilities in handling Personal Data. These principles, are adopted from the detailed GDPR guidance, state how "the Data Controller is competent for compliance with the principles, and able to prove it."

6.1 Lawfulness, Fairness, and Transparency

Personal Data are processed by the Company in a lawful, correct, and transparent manner in relation to the data subject.

To ensure transparency, the Company has prepared specific privacy information notices, drafted in a concise, transparent, and easily accessible form with simple and clear language. These include the procedures for exercising the rights of the data subject, the purposes of the processing to which Personal Data are intended as well as the legal basis of the processing, and the retention period of Personal Data.

6.2 Purpose Limitation

Personal Data are collected by the Company for specified, explicit, and legitimate purposes, and subsequently processed in a way that is compatible with those purposes.

6.3 Data Minimization

The Personal Data processed by the Company are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

The Company utilizes deidentified Personal Data, whenever possible, to reduce the risk for data subjects.

6.4 Accuracy of Data

Professionally reasonable efforts are taken to update data with respect to the purpose for which they are processed.

6.5 Data Retention

Personal Data are stored by the Company for a period of time as defined by the relevant policies and/or contractual obligations.

In other cases, Accelevir will refer to the policy ACDX-DP007 Data Conservation and Cancellation Management.

6.6 Data Integrity and Confidentiality

Taking into account the technologies and commercially reasonable approaches as well as the costs of implementation and the likelihood and severity of risks to Personal Data, the Company implements technical and organizational measures to ensure an adequate level of security for Personal Data. These measures include protection against accidental or unlawful destruction, loss, modification, and unauthorized disclosure or access.

6.7 Accountability

The Company is responsible for compliance with the principles described above and holds supporting information as allowed under federal, state, and local laws.

6.8 Data Collection

The Company limits itself to collecting as little Personal Data as possible. If Personal Data are collected by a third party, the Data Protection Officer (DPO) ensures that the Personal Data are collected lawfully.

6.9 Use, Storage, and Deletion of Data

The purposes, methods, registration limit, and retention period of Personal Data are consistent with the information contained in the Privacy Policy related to the individual data process.

The Company maintains the accuracy, integrity, confidentiality, and relevance of Personal Data according to the purpose of the treatment, using appropriate security mechanisms to protect Personal Data and mitigate risk of theft and misuse.

6.10 Disclosure to Third Parties

We will notify our suppliers or business partners who have access to Personal Data of our policies and expectations for security measures and use of Personal Data. The supplier or business partner processes Personal Data only to fulfill its contractual obligations for the Company. When we process Personal Data jointly with an independent third party, the Company explicitly specifies its responsibilities and expectations for the third party regarding the protection of Personal Data. We will utilize best efforts (as feasible) to incorporate these policies as an element of contractual agreements (ACDX-DP009 Data Protection Agreement).

6.11 Data Privacy Impact Assessment

We shall make best efforts to complete a Data Protection Impact Assessment (DPIA) for the following conditions if met:

- The data processed is an assessment of personal aspects relating to individuals, based on automated processing; or,
- The data processing, if applicable on a large scale, of Particular Categories of Personal Data; or,
- The data processing is systematic large-scale surveillance of an area accessible to the public.

Details regarding the DPIA can be found in ACDX-DP010 Guide Template for Data Protection Impact Assessment.

7 RIGHTS OF THE INTERESTED PARTIES

7.1 Right of Access by Interested Parties

When the Company acts as a Data Controller, it is responsible for providing data subjects with a reasonable mechanism to allow them to access their Personal Data and must allow them to update, rectify, delete, or transmit their Personal Data, as appropriate or required by law.

7.2 Data Portability

Data subjects have the right to receive, upon request, a copy of the data they have provided in a structured format and to transmit their own Personal Data outside the purview of the Company. When the Company acts as a Data Controller, it is responsible for ensuring that such requests are processed as soon as reasonably possible and within a target of thirty (30) days, unless they are excessive and do not affect other people's Personal Data rights.

7.3 Right to be Forgotten

When the Company acts as Data Controller, it is responsible for taking the necessary actions to provide Notices to third parties on the principles embedded within Company policies.

The mechanism for managing the rights of the interested parties is detailed in ACDX-DP007 Data Conservation and Cancellation Management.

8 THE SECURITY OF PERSONAL DATA PROCESSING

Personal Data are processed by the Company in a way that ensures appropriate security, including protection against unauthorized or illegal processing using professionally reasonable efforts. The Data Controller and Data Processors utilize best professional standards to ensure that a level of security is deemed appropriate according to the risks, including:

- Pseudonymization and encryption of Personal Data,
- Measures to maintain confidentiality, integrity, availability, and resilience of processing systems and services,
- Access to Personal Data in the event of a physical or technical incident,
- Testing and/or obtaining periodic reports from Information Technology (IT) Management service provider reports to reflect their testing, evaluating, and effectiveness of security measures.

9 DATA BREACH NOTIFICATION

The Company is required to report security breaches to the Interested Party and/or designated IT service provider without undue delay, and where possible, no later than 72 hours after becoming aware of them. However, we shall not notify the security breach if it is "unlikely to cause a risk to the rights and freedoms" of data subjects (See ACDX-DP012 Risk Evaluation for more information on determining risk level).

The Company has implemented technical protection measures to limit the risk of access to Personal Data.

10 DETAILED DESCRIPTION OF THE ACCELEVIR DIAGNOSTICS METHODOLOGY

10.1 Data Processing Activities Registry

The Company has created an electronic Data Process Activities Register which allows a single collection point for all the information relating to the single data process (see Section 10.1).

10.2 Privacy Information Notices

The Company has proceeded to define specific privacy information notices for the interested parties involved in the individual processing of Personal Data in accordance with GDPR guidelines.

10.3 Data Protection Impact Assessments

The Company shall analyze the need to conduct an impact assessment as outlined in Section 6.11.