2. EU/UK PRIVACY POLICY

We are very delighted that you have shown interest in our enterprise. Data protection is of a particularly high priority for the management of Bioniks. This privacy policy outlines what personal data that is being collected and how it is used in the operations of the Kinetigram platform, either obtained from the evaluator (user) or data subject (patient). We collect only the data that is necessary either for authentication (login to the application) or motion assessment.

The processing of personal data shall always be in line with the General Data Protection Regulation (GDPR), and in accordance with the country-specific data protection regulations applicable to Bioniks. By means of this data protection declaration, our enterprise would like to inform the general public of the nature, scope, and purpose of the personal data we collect, use and process. Furthermore, data subjects are informed, by means of this data protection declaration, of the rights to which they are entitled.

As the controller, Bioniks has implemented numerous technical and organizational measures to ensure the most complete protection of personal data processed through the Kinetigram application and cloud infrastructure.

1. Data Protection Officer and EU Representative

Our data protection officer ("DPO") for the European Union is:
DP Dock DPO Services GmbH, Attn: Bioniks, Grüffkamp 10, 24159 Kiel, Germany (bioniks@dp-officer.com)

The EU Representative pursuant to Art. 27 of the GDPR is:
Rivacy GmbH, Mexikoring 33, 20079 Hamburg, Germany (info@rivacy.eu)

The UK Representative pursuant to UK GDPR is:
Rivacy Ltd., St James' Hall, Mill Road, Lancing, West Sussex, England, BN15 0PT, United Kingdom (info@rivacy.co.uk)

2. Definitions

Our privacy policy is intended to be simple and understandable for everyone. As a rule, the official terms of the GDPR are used in this privacy policy. The official definitions are explained in Article 4 of the GDPR.

3. Collection of General Data and Information

The personal data collected for operations of Kinetigram platform include two types of data: (1) user data and (2) subject/patient data.

User data pertains to data needed to identify and authenticate a user for access to Kinetigram application, including:

- First and last name*
- Job title (optional)
- Email address
- Username*
- Institution affiliation (site/tenant identifier) *

These data are managed by Bioniks via Microsoft Azure B2C Identity Service. Azure B2C is an identity management service that enables signing up, signing in, and managing login profiles (More information is available at: https://docs.microsoft.com/en-us/azure/active-directory-b2c/).

Data marked (*) are also retained in the tenant database for the customer collected data.

Subject/patient data collected by the Kinetigram include the following information:

- Subject alpha-numerical identifier (pseudonymized)
- Affiliation to a site/tenant identifier
- Gender
- Height
- Weight
- Hand dominance
- Arm measurements (body segment lengths)
- Login session information (logged user, date and time of login/logout)
- Measurement session data (date, time, user performing assessment, parameters of assessment, notes etc.)
- Kinect frame data (timestamp, 25 tracked joint positions in three dimensions: x, y, z, visibility flag etc.) and other motion data
- Processed motion data (reachable workspace parameters, functional workspace information, range of motion etc.).

This data is stored in our cloud servers. Although Kinetigram uses Kinect sensor consisting of color and infrared cameras, the Kinetigram does not store or transmit any audio or video information to Bioniks. To obtain the raw motion data, the infrared camera data are processed locally by the Microsoft Kinect Runtime and provided as 3D joint positions to Kinetigram application.

Note: When using the Kinetigram with a Kinect for Windows v2 sensor, Microsoft will collect telemetry data (e.g., operating system, number of processors, graphic chipset, memory, device type, locale, time) in order to improve Microsoft products and services. The data will not be used to identify specific individuals.

Additional data on the application activities are collected in various cloud and local log files that provide operational support for the Kinetigram infrastructure. The log files do not contain personal information. Examples of such information may include: (1) clinical site identifier, (2) database identifiers, (3) Internet protocol address (IP address), (4) time and type of API calls, and other operational metadata. When using these general data and information, Bioniks does not draw any

conclusions about the data subject. Rather, this information is needed to (1) deliver the content correctly, (2) optimize the content, (3) ensure the long-term viability of our information technology systems and cloud technology, and (4) cooperate with law enforcement or similar investigations by responding to subpoenas, search warrants, or other lawful requests for information that we receive. Therefore, Bioniks may analyze anonymously collected data and information statistically, with the aim of increasing the data protection and data security of our enterprise. The anonymous data of the server log files are stored separately from all personal data provided by a data subject. The operational logging data are typically preserved up to 30 days.

4. **Log files**

As a medical device manufacturer and software company, Bioniks is required by FDA 21 CFR Part 11 to implement additional audit trails that track user-initiated changes in the database. Where appropriate, Bioniks maintains the audit table until final data transfer to the clinical trial sponsor. With consideration for the data minimization principle of Art. 5 (1) c GDPR, Bioniks only retains a minimum amount of data in the audit logs. In terms of patient/subject data, the audit logs retain primarily the data fields that are entered directly through the client application (e.g. subject ID, height, weight, gender, session metadata) and processed functional scores. The raw motion data and graphical results are not retained as part of the audit table. In terms of user data, Bioniks removes user's account information and email addresses from the Microsoft server, yet retains name/username in the audit logs since patient data is associated with who collected or made changes to the data.
Maintaining these records in the audit trail is in accordance with Art. 17(3) e and Art. 6(1) c of GDPR, in which it is stated that the right to deletion of the data subject does not apply in cases of establishment, exercise or defense of legal claims. Bioniks, as a Data Controller, also has a legitimate interest in storing data in the audit logs, according to Art. 6(1) f GDPR. With consideration to a necessary balance of interests, Bioniks' legitimate interest in storing data in the audit logs outweighs the data subject's individual right of erasure. Data subjects are hereby informed that, in this case, their data cannot be erased.

5. **Children's Information**

Children may be data subjects in a clinical study conducted by the trial sponsor. In such case, Bioniks may collect health data of children according to the study protocol. Unless children are part of the study, Bioniks does not knowingly collect information on people under the age of 18. If you think that your child provided this kind of information, we strongly encourage you to contact us immediately and we will do our best efforts to promptly remove such information from our records. We encourage parents and guardians to observe, participate in, and/or monitor and guide their online activity.

6. **Rights of the Data Subject**

a) Right of Access (Art. 15 GDPR)
Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this

information. Furthermore, the European directives and regulations grant the data subject access to the following information:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- The existence of the right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may, at any time, contact any employee of the controller.

b) Right to Rectification (Art. 16 GDPR)
Each data subject shall have the right granted by the European legislator 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.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact any employee of the controller.

c) Right to Erasure (Right to be forgotten) (Art. 17 GDPR)
Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.
- If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by Bioniks, he or she may, at any time, contact any employee of the controller. An employee of Bioniks shall promptly ensure that the erasure request is complied with immediately.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) GDPR to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. An employee of Bioniks will arrange the necessary measures in individual cases.

d) Right of restriction of processing (Art. 18 GDPR)
Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
- The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by Bioniks, he or she may at any time contact any employee of the controller. The employee of Bioniks will arrange the restriction of the processing.

e) Right to data portability (Art. 20 GDPR)
Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact any employee of Bioniks.

f) Right to object (Art. 21 GDPR)
Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

Bioniks shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.

If Bioniks processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to Bioniks to the processing for direct marketing purposes, Bioniks will no longer process the personal data for these purposes.

In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by Bioniks for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact any employee of Bioniks. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

g) Automated individual decision-making, including profiling (Art. 22 GDPR)
Each data subject shall have the right granted by the European legislator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision (1) is not is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is not based on the data subject's explicit consent.

If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject's explicit consent, Bioniks shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any employee of Bioniks.

h) Right to withdraw data protection consent (Art. 7(3) GDPR)
Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at any time, contact any employee of Bioniks.

If Bioniks serves as the data processor for the clinical study, all requests should be directed to the study sponsor which will direct Bioniks to remove the data.

7. **Legal Obligations**

The provision of personal data for the decision on the conclusion of a contract, the fulfilment of a contract or for the implementation of pre-contractual measures is voluntary. However, we can only make the decision in the context of contractual measures if you provide such personal data that is required for the conclusion of the contract, the performance of the contract or pre-contractual measures. For example, we work with our clinical study partners to ensure security and to track who collects data. Hence, accurate login information is necessary.

8. **Third Party Sharing**

We may be contractually obligated to share personal data with our third-party clinical study partners.

9. **Preventing Re-identification of Data**

Data is only collected for the intended purposes of clinical studies, and is not sold to third parties. Bioniks follows Microsoft Azure's B2C policies: https://docs.microsoft.com/en-us/azure/active-directory-b2c/

10. **Subject to Change**

We reserve the right to adapt or update this data protection declaration, if necessary, in compliance with the applicable data protection regulations. In this way, we can adapt it to the current legal requirements and take into account changes to our services, e.g., when introducing new services. The current version applies to your visit.

11. **Contact Us**

If you have any questions about our privacy practices or this Privacy Policy, please contact us at:

Bioniks
2156 Central Avenue
Alameda, CA 94501
United States of America
Tel: +1-510.747.1947
Email: info@bioniks.net

If you have further questions or concerns, please contact our Data Protection Officer (DPO) at DP Dock DPO Services GmbH, Attn: Bioniks, Grüffkamp 10, 24159 Kiel, Germany and/or our EU Representative at Rivacy GmbH, Mexikoring 33, 20079 Hamburg, Germany or for UK: Rivacy Ltd., 87, Warriner Gardens, Unit G1/G2, London, SW11 4DX, United Kingdom.

Last review of this Privacy Policy: Nov 3, 2026