ELABNEXT
DATA PROCESSING AGREEMENT (DPA)

THE UNDERSIGNED:

_____ with its registered office and principal place of business _____, registered with the Chamber of Commerce under number _____, herin legally represented by _____ (hereinafter: "Controller");

and

eLabNext: a private company with limited liability registered as Bio-ITech B.V., trading as eLabNext, registered at the Chamber of Commerce under number 53765273, with its registered office in Groningen, the Netherlands. (hereinafter: "Processor");

hereinafter jointly referred to as: "the Parties" and individually as "the Party";

WHEREAS:

- the Controller has instructed the Processor to supply services or products or perform activities otherwise, whereby the Processor is involved in processing personal data;
- the Parties wish to set out in this Data Processing Agreement ("DPA") the responsibilities in accordance with the GDPR and other applicable legislation and regulations regarding the Processing of Personal Data;
- this DPA applies to all existing and future agreements concluded between the Parties and to all the services, products or activities supplied by the Processor on behalf of the Controller;
- the Parties wish to deal scrupulously with the Personal Data to be processed in implementation of the DPA;

DECLARE THAT THEY HAVE AGREED THE FOLLOWING:

Article 1. Definitions

In this DPA, the terms written with a capital letter have the meaning defined in this article. Where the definition in this article is given in the singular, the plural is also included and vice versa, unless otherwise is expressly stated or such is clear from the context.

1.1. **GDPR:** General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and 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 and revoking Directive 95/46/EC, including the Implementation Act of this Regulation. The GDPR replaced the Dutch Personal Data Protection Act on 25 May 2018.

1.2. **Security incident:** a security breach that leads or could have led either inadvertently or unlawfully to the destruction, loss, alteration or unauthorised disclosure of or unauthorised access to forwarded, stored or otherwise processed Personal Data.

1.3. **Data Subject(s):** the person who is the subject of the Personal Data;

1.4. **Third Party:** a third party as provided for in Article 4(10) GDPR;

1.5. **Personal Data:** all information concerning an identified or identifiable natural person, within the meaning of Article 4(1) GDPR;

1.6. **Processor:** the person processing Personal Data on behalf of the Controller, as provided for in Article 4(8) GDPR;

1.7. **Controller:** the person responsible for processing Personal Data as provided for in Article 4(7) GDPR;

1.8. **Processing Personal Data:** any operation or set of operations regarding Personal Data, including in any case the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of data; Where terms are used within this DPA that are not defined in this article 1, but are defined in article 4 GDPR, those terms shall have the same meaning as in the GDPR.

Article 2. Effective date, duration and applicability

2.1. This DPA becomes effective as soon as it is signed and continues to be effective for as long as the Processor acts as a Processor of Personal Data under the

agreement(s) concluded between the Parties with regard to Personal Data made available by the Controller, after which this DPA ends by operation of law.

2.2. This DPA applies to all activities performed and to be performed by the Processor on behalf of the Controller and forms an integral part of any other related agreements.

2.3. Where an assignment - or its performance - involves the Processing of Personal Data by the Processor on behalf of the Controller, the provisions in this DPA will apply to this accordingly.

Article 3. Processing activities and purposes

3.1. The Processor offers software products for the purpose of storing research data of customers all over the world. The use of this software is offered as an online service (Software as a Service; SaaS). To supply these services, Personal Data of staff (users) is processed in the software supplied by the Processor. The purpose of such processing is personal identification, so that adding or changing research data becomes traceable in the software. This means personal data is received, organised, structured, stored, adapted or altered, disclosed, combined or destroyed. The categories of Personal Data the Processor may process as instructed by the Controller are included in Appendix 1 of this DPA. The Processor will not process the Personal Data for any purpose other than those laid down by the Controller. The Controller will notify the Processor of the processing purposes insofar as they have not yet been mentioned in this DPA.

3.2. The Controller is responsible for the Personal Data to be processed by the Processor. The Controller ensures to the Processor that the Personal Data will not contain any sensitive Personal Data.

3.3. The Processor undertakes to process Personal Data under the conditions of this DPA as instructed by the Controller. Processing will take place only for the purpose of supplying the service for the Controller, and those purposes that can be held to be related to this within reason or that are determined on the basis of additional consent.

3.4. The Personal Data to be processed as instructed by the Controller remains the property of the Controller and/or the Data Subjects.

Article 4. Obligations of the Parties

4.1. The Processor processes Personal Data as instructed by and on behalf of the Controller. A list of the processed Personal Data and processing activities is included in Appendix 1 of this DPA. Other processing activities will be performed only if instructed to do so directly by the Controller or if a legal obligation exists to that effect.

4.2. Unless otherwise has been determined in this DPA, the Processor will not take any decision about the use of the Personal Data and the disclosure of Personal Data to third parties. The control of the Personal Data provided under this DPA will never rest with the Processor.

4.3. The Processor processes the Personal Data according to the reasonable written instructions of the Controller, in accordance with the purposes and means determined by the Controller and with due regard to the retention periods established by the Controller, as described in Appendix 1. The Controller is responsible for ensuring that its instructions are in accordance with European legislation and regulations.

4.4. The Processor will process the Personal Data properly and carefully and in accordance with its obligations under the agreement(s) concluded between the parties.

4.5. Where the instructions from the Controller involve additional work (and costs) for the Processor, and may have consequences for an agreed time schedule, such instructions will not be observed until the Parties have made further arrangements about the costs and the time schedule.

4.6. The Processor processes the Personal Data solely in the performance of the Controller's instructions, unless there are derogating legal obligations.

4.7. The Processor ensures that any persons working for or on behalf of the Processor and who are involved in processing the Personal Data are aware of and observe the Processor's obligations included in this DPA.

4.8. Where the Processor intends to engage a Third Party for activities involved in the performance of the Controller's assignment, for the purpose of which it needs to process Personal Data, the Processor will specifically inform the Controller in writing of the intended changes to the list of sub-processors as specified in Appendix 1. The Processor shall specifically inform in writing the Controller of any intended changes of the list in Appendix 1, through the addition or replacement of sub-processors at least one month in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

4.9. Where the Processor engages a sub-processor for carrying out specific activities, the Processor concludes a processing agreement with the sub-processor in question similar to the present one, before that sub-processor becomes involved in processing Personal Data for which the Controller is responsible.

4.10. The Processor must report, at the Controller's request, where the Personal Data are stored. The Processor may not store the Personal Data outside the European Economic Area. The Controller agrees that where the Processor engages a sub-processor in accordance with article 4.8 and 4.9 for carrying out specific

processing activities (on behalf of the Controller) and those processing activities involve a transfer of Personal Data outside the European Economic Area, the Processor and the sub-processor can ensure compliance with the GDPR by using standard contractual clauses as adopted by the European Commission, provided the conditions for the use of those standard contractual clauses are met.

Article 5. The Data Subject's right

5.1. The Processor ensures that the Data Subject can exercise all their rights from the regulation mentioned in **Article 1.1**. The Processor will promptly notify the Controller of any request it has received from a Data Subject. It shall not respond to that request itself unless it has been authorised to do so by the Controller.

5.2. Moreover, the Processor will do the following immediately when requested, within a reasonable term and within five working days if possible, after receiving a request to that effect:

a. provide in writing all necessary information the Controller might need within the framework of this DPA;

b. improve, supplement, remove or protect Personal Data, provided that this is technically possible;

c. transfer the Personal Data of the Data Subject to the Controller in a well-structured, standard and machine-readable format.

Article 6. Duty of confidentiality

6.1. The Processor will maintain confidentiality, both during and for an unlimited period of time after the termination of this DPA, with regard to Personal Data that becomes available to it in the context of the agreement(s) and activities performed and to be performed on behalf of the Controller.

6.2. This duty of confidentiality does not apply where the Controller has given express permission to provide the information to Third Parties, if the provision of that information to Third Parties is logically necessary given the nature of the provided assignment and the performance of this DPA, or if there is a legal obligation to provide the information to a Third Party.

Article 7. Security measures

7.1. The Processor takes all appropriate technical and organisational measures to secure and keep secure the Personal Data and the processing thereof against loss or any form of careless, inexpert or unlawful use or processing, bearing in mind the current state of technology. A list of the security measures applied by the Processor is included in **Appendix 2**.

7.2. If the Processor fails to take appropriate technical and organisational security measures and subsequently fails to take appropriate measures within a reasonable term set by the Controller, the Controller will be entitled to terminate the agreement.

Article 8. Notification of security incidents

8.1. The Processor must notify the Controller in writing, without any unnecessary delay, of any Security Incident that could have direct consequences for the processing of Personal Data of Data Subjects that are under the Controller's responsibility.

8.2. The Processor will specify in such notification the nature and scope of the breach, the name and contact details of the person who can give further information about the breach, the likely consequences of the breach and the measures that can or must be taken to limit the consequences of the breach and prevent them in the future.

8.3. The Controller determines - and is responsible for - whether and when it has to notify the Controller's national Data Protection Authority and/or Data Subjects of a Security Incident reported by the Processor to the Controller.
The Processor will cooperate in every possible way in taking the necessary measures to limit the consequences of a Security Incident and prevent new Security Incidents.

8.4. The Parties will keep each other informed about the developments in respect of a Security Incident and the measures they take to limit the consequences of the Security Incident and prevent a repeat thereof.

Article 9. Liability

9.1. If the Processor fails to comply with an obligation under this DPA, the Controller may declare the Processor in default. Notice of default will be served in writing, giving the Processor a reasonable period in which to meet its obligations.

9.2. The Parties are each responsible and liable for their own actions. The liability regulated in this Article 9 applies exclusively with regard to penalties and damages, resulting from of an attributable failure in complying with this DPA.

9.3. The liability of Processor due to an attributable failure with this DPA, shall be limited to a maximum of the annual amount of the main agreement, concluded between the Processor and the Controller. The liability of Processor for indirect damages, consequential damages, lost profits, lost savings, reduced goodwill, damages due to business interruption and damages resulting from claims of third

parties is excluded, unless the damage arises from wilful acts or gross negligence on the part of Processor.

9.4. A Party may not invoke a limitation of liability in respect of any;
   1. A right of recourse issuing from or in relation to Article 82 AVG; or
   2. Action for damages pursuant to the Processing of Personal Data, if and to the extent that the action consists of recovery of a penalty paid by the other Party to the supervisory authority (in Dutch: the "Autoriteit Persoonsgegevens"), to the extent that such penalty is attributable to the former Party.

9.5. The Controller is fully responsible and is therefore fully liable for the defined purpose of processing, the use and content of the Personal Data, their provision to Third Parties, the duration of the storage of the Personal Data, the processing method and the means used for that purpose.

Article 10. Compliance and inspection

10.1. The Parties shall be able to demonstrate compliance with this DPA.

10.2. The Processor shall deal promptly and adequately with inquiries from the Controller about the Processing of Personal Data in accordance with this DPA.

10.3. The Controller is entitled to inspect compliance with the provisions from this DPA once a year at most. The Controller can do so itself after permission from the Processor for that purpose, or it can engage an independent auditor certified for that purpose to do so.

10.4. The Controller bears the costs of the inspection. The Processor may charge a reasonable fee for the costs of its staff involved in this inspection.

10.5. An inspection must not unnecessarily disrupt the Processor's business operations.

10.6. The Controller will announce the inspection to the Processor at least ten working days prior to commencement in writing, while including a description of the elements to be inspected, the inspection process and the time frame within which the inspection will take place.

Article 11. Destruction and backup

11.1. The Processor will make available all Personal Data to the Controller immediately when requested by the Controller, and in any case within a reasonable term after the end of this DPA or the completion of the assignment.

11.2. The Processor must delete all Personal Data completely and permanently immediately when requested by the Controller, unless the storage of Personal Data is a legal obligation. In such a case the Processor will notify the Controller of such a legal obligation and the implications for the retention period arising from this without any unnecessary delay.

11.3. As soon as the Controller is in possession of all the Personal Data, in a technological format accepted in writing by the Controller, the Processor will delete all the Personal Data completely and permanently within fourteen days of establishing that the Controller is in possession of the Personal Data.
11.4. The Processor may derogate from the provisions of the two preceding paragraphs where a statutory retention period applies with regard to the Personal Data, where such is necessary in order to prove its compliance with its commitments to the Controller, or where it is technically impossible to comply with them.
11.5. Personal Data stored in backups will not be stored any longer than the retention period specified in Appendix 1.

Article 12. Final provisions

12.1. Any amendments to this DPA will apply only if they have been agreed between the Parties in writing.
12.2. In the event of a contradiction between this DPA and the provisions of related agreements between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail.
12.3. The Processor may not suspend compliance with its obligations arising from this DPA, offset them or make them dependent on any action or statement on the part of the Controller. Any default on the part of the Controller in terms of the assignment or the nullification of the agreement on the basis of which the assignment is performed cannot lead in any manner to the Processor's non-compliance with its obligations under this DPA.
12.4. All the provisions from this DPA that are expressly or implicitly intended to remain in force after the termination of this DPA , including Articles 7 (confidentiality), 9(2) (reporting a security incident), 10 (liability) and 12 (destruction and backup) remain in full force.

Article 13. Choice of law and forum

13.1. Any disputes arising from this DPA are subject to Dutch law, with the exception of the international choice-of-law rules enshrined in Dutch law.
13.2. The Dutch court in the Groningen district has exclusive jurisdiction with regard to any disputes arising from this DPA.

	eLabNext (Bio-ITech B.V.)
	W. de Jong
	Managing Director

Place: _____

Date: _____

Place: Groningen, The Netherlands

Date:

Appendix 1: Specification of Personal Data, Processing Purposes, Sub processors and Retention Periods

This Appendix forms part of the DPA.

Processed personal data

- First name
- Last name
- Organisation's email address
- Group
- Organisation
- IP address
- Password *

* Only if Single Sign-On (SSO) or Active Directory (AD) is not used

Purposes of Processing

The email address is used to identify users and send system messages for updates and notifications. The first and last name are displayed after login ("logged in as"), in the user admin panels, in the Group members lists and where the person is mentioned as owner or collaborator. Finally, all displays of logs are based on (first and) last name. Group and Organisation are used to classify persons in the system and on the basis of this give them access or options to obtain access. The IP address is used for different security functionalities (such as occurrence, brute force hacking and 2FA). The password is used for authentication.

Subprocessors

Amazon Web Services (AWS): The eLabJournal Cloud (https://www.elabjournal.com) and eLabInventory Cloud (https://www.elabinventory.com are hosted at AWS data centres within the European Union (Frankfurt, Germany). For customers in North and South America, the eLABJournal Cloud (https://us.elabjournal.com/) and eLABInventory Cloud (https://us.elabinventory.com) are hosted at AWS in the United States (Ohio). Private Cloud installations are hosted at AWS at the following locations unless agreed otherwise: for customers within the European Union, systems are hosted in Dublin, Ireland, for customers in North and South America, systems are hosted in the United states (Ohio),

for customers in the United Kingdom systems are hosted in the United Kingdom (London), for customers in Asia/Pacific, systems are hosted in Australia (Sydney). Amazon Web Services is ISO27001:2013 certified globally. For more information, see https://aws.amazon.com/compliance/.

Retention Period

The Processor will not keep Personal Data any longer than is necessary for the purposes for which it is used, in compliance with the legal obligations and in accordance with the guidelines implemented by the organisation (GxP, FDA 21 CFR part 11) in order to guarantee traceability and at least according to the following guidelines:

- For the period of the licence: unlimited.
- A request to delete specified Personal Data will be carried out within two months. This excludes Personal Data in log tables and backups.
- The Processor reserves the right to delete Personal Data permanently at its own initiative after termination of this DPA.
- Backups will be stored for a maximum of six months.

Appendix 2: Technical and organizational security measures

eLabNext has been ISO 27001:2013 certified since December 2016 (see https://www.elabnext.com/iso-certified/ to download certificate and the statement of applicability) and has taken data protection measures in accordance ISO27001 appendix, which includes (among others):

- Secured connections by means of SSL encryption
- Data security by means of username and password, optional 2nd factor
- Protection and security of server architecture, including encryption, firewall, etc.
- Additional physical protection of backup servers. Database, datafile and log file backups are encrypted and stored by means of AES-256
- Monitoring and logging via Zabbix
- After a period of user inactivity, to be set by administrators, access to the solution will be blocked. This blockade can be lifted by the user through reauthentication.
- Security updates to the platform used by the solution are supported by the provider without reservation
- Screening of and confidentiality statements from staff