SWISS BIOBANKING PLATFORM
SBP NEXT

PROCESSING TERMS

1. INTRODUCTION

1.1 **Scope and purpose.** These processing terms (**Processing Terms**) automatically apply whenever Biobank Users provide us with datasets containing personal data as part of our NExT Platform (**Shared Personal Data**). They reflect the agreement between you (the Biobank providing us with the Shared Personal Data and any User acting on its behalf) and us (SBP) regarding the processing and security of Shared Personal Data, in order to ensure compliance with applicable data protection laws. These Processing Terms are incorporated into and form an integral part of our terms of use (ToU). Acceptance of the ToU by one Biobank User is deemed acceptance of these Processing Terms by such Biobank.

1.2 **Definitions**. All capitalized terms not defined in this document have the meaning given to them in the ToU. The terms "data subject", "processing", "controller" respectively "controller of the data file" and "processor" used in these Processing Terms shall have the meanings specified in the Swiss Data Protection Legislation or the GDPR, depending on their respective scope of application.

1.3 **Duration**. These Processing Terms apply for as long as we process Shared Personal Data on your behalf (the Term).

2. DATA PROTECTION LEGISLATIONS

2.1 **Applicable legislations**. The following data protection legislations (together the **Applicable Data Protection Legislation**) may, depending on the circumstances, apply to the processing of the Shared Personal Data:

(a) the Swiss Federal Data Protection Act and its implementing ordinances, as may be amended from time to time during the Term (the **Swiss Data Protection Legislation**);

(b) the General Data Protection Regulation (EU) 2016/679 of the European Parliament (the **GDPR**); and/or

(c) If any other data protection legislation applies to the processing of the Shared Personal Data, you undertake to comply with the obligations applicable to you and to inform us in writing of any provisions contained in such legislation that could have an impact on the processing of the Shared Personal Data by us as a processor for you.

2.2 **Applicability of these Processing Terms**. Unless otherwise stated in these Processing Terms, the provisions of these Processing Terms, apply regardless of the legislation applicable to the processing of Shared Personal Data.

3. DATA PROCESSING

3.1 **Roles and compliance.** With regard to the processing of the Shared Personal Data:

(a) we act as data processor, processing such data on your behalf and for your account;

(b) you act as data controller (respectively, controller of the data file), or a processor for a third party, as the case may be; and

(c) each Party must comply with its obligations under the Applicable Data Protection Legislation.

If you are a processor for a third party, you warrant to us that you have obtained the express prior authorization of the applicable controller to your instructions and actions regarding the Shared Personal Data, including our designation as another processor.

3.2 **Scope of processing and instructions**. We will process the Shared Personal Data in accordance with the ToU and these Processing Terms for the purpose of providing the NExT Platform and Services to you. You instruct us to process the Shared Personal Data only in strict compliance with any Applicable Data Protection Legislation and furthermore:

(a) only to provide the Services , as documented in the

ToU, the Processing Terms, and the NExT Platform's documentation; and

(b) only with regard to processing operations that you would be entitled to carry out yourself and provided that no legal or contractual obligation to keep the information secret prohibits our involvement.

We undertake to comply with those instructions unless a legislation applicable to us requires us otherwise, in which case we will inform you of that legal requirement before processing (subject to any legal provisions to the contrary).

3.3 **Categories of personal data and data subjects; pseudonymization**. The categories of personal data and data subjects are described in the NExT Platform's documentation, as may be updated from time to time. In particular the Shared Personal Data you provide must be coded (pseudonymized); you are responsible for ensuring this and for retaining the key permitting to re-identify the individuals. For clarity, these Processing terms also apply to personal data which we receive in a coded form.

3.4 **No Re-identification**. We undertake not to attempt to identify the data subjects to whom the Shared Personal Data relates and in particular not to use such Shared Personal Data (by itself or in conjunction with other tools or datasets) in any other manner which the view of partially or wholly rebuilding the data subjects' records. Although we impose an equivalent restriction on all users of our NExT Platform, we are not responsible for actions of others.

3.5 **Your Obligations**. You are responsible, namely, for the quality, lawfulness, and accuracy of your Shared Personal Data processed and are liable to third parties affected by the processing and to the competent data protection authorities. In particular, you undertake to:

(a) provide sufficient information to the data subjects about the collection and processing of their personal data;

(b) obtain the valid consent of the data subjects to the processing of their personal data, if such consent is required under Applicable Data Protection Legislation; and

(c) ensure compliance with all rights of the data subjects (e.g. right of access and rectification, right to object etc.) as well as all obligations towards the competent data protection authorities (e.g. declaration of files) under the Applicable Data Protection Legislation.

3.6 **Deletion**. You can request us to delete your Shared Personal Data by accessing your Account (for Accounts with admin authorization). In addition, you irrevocably require us to delete all Shared Personal Data from our systems if you terminate your Account (and where a Biobank has several Users, upon the termination of all associated Accounts). We will comply with this instruction as soon as possible, unless we are required to retain all or part of Shared Personal Data for technical or legal reasons. You acknowledge and accept that it is your sole responsibility to transfer and/or safeguard Shared Personal Data that you wish to keep thereafter.

4. DATA SECURITY

4.1 **Security measures**. We will implement and maintain appropriate technical and organizational measures to protect the Shared Personal Data against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access (each a **Security Incident**). These measures include in particular:

(a) the use of firewalls;

(b) the use of personal data in a coded form;

(c) the means to ensure the ongoing confidentiality, integrity, availability and resiliency of processing systems and services;

(d) the means to limit access to the Shared Personal Data to personnel who need to access it in the course of providing the Services;

(e) the means to restore the availability of and access to the Shared Personal Data within an appropriate time frame in the event of a Security Incident; and

(f) a procedure to regularly test, analyze and evaluate the effectiveness of technical and organizational measures to ensure the security of the processing.

4.2 **Security compliance by your personnel**. We will take appropriate measures to ensure compliance with the above-mentioned security measures by our employees and subcontractors, in particular by ensuring that all persons authorized to handle Shared Personal Data are committed to process Shared Personal Data are contractually bound to maintain confidentiality or are subject to an appropriate legal obligation of confidentiality.

4.3 **Appropriateness of security measures**. You warrant that you have verified, and undertakes to continuously verify, that the technical and organizational measures specified in this Section 4 are sufficient to adequately protect the Shared Personal Data in accordance with the requirements set forth in any Applicable Data Protection Law.

4.4 **Security Incidents**. We undertake to inform you as soon as possible by any useful means (in particular via your Account) if we become aware of a Security Incident. We will, to the extent possible, describe the nature of the Security Incident, as well as any measures taken by us to mitigate potential risks and the measures that we recommend you take. Our actions in connection with this Section 4.4 shall not constitute, and shall not be construed as, an admission by us of any fault or liability in connection with the Security Incident that has occurred.

You are solely responsible for carrying out any analysis of the Shared Personal Data and for complying with the legal provisions applicable to it, in particular any obligations to provide a notification of the Security Incident to any competent authority and/or the data subjects. In this context, we will provide you with any assistance reasonably required by you in order to comply with your obligations.

5. INFORMATION ON AND AUDITS OF THE SECURITY MEASURES

5.1 **In General**. If the GDPR applies to the processing of the Shared Personal Data, to the extent reasonably necessary to verify our compliance with our obligations under these Processing Terms, we will make available to you the documents and information, and allow you or an independent auditor appointed by you to conduct audits (including inspections). We will provide reasonable assistance with respect to the audits described in this Section 5.1. Upon conclusion of the audit, you must forward the complete audit report to us, free of charge.

5.2 **Request**. Any request under Section 5.1 must be communicated to us in writing and indicate (i) the Shared Personal Data concerned, (ii) the reasons why the conditions referred to in Section 5.1 apply to such data, (iii) the specific documents to be reviewed, respectively our specific obligations to be audited, and (iv) that you expressly undertake to use the information collected only to ensure that we are in compliance with our obligations with regard to the Shared Personal Data and in particular that the information collected will not be used in connection with any legal or administrative proceedings against us. Unless there are exceptional circumstances, you may not make more than one request per year.

5.3 **Exercise of rights**. Upon receiving a request in accordance with Section 5.2, and provided that all conditions are met, we will comply with the request as follows:

(a) we will inform you, with regard to the review of documents, of the period during which you may consult the documents at our offices. Unless otherwise expressly agreed by us, you are not authorized to make copies of the documents consulted. Alternatively, we may decide to provide the documents by any other useful means, in particular by sending them electronically;

(b) we will inform you with regard to audits of (i) the date or dates on which the audits may take place and (ii) the scope of the audit, in particular the inspections that may be carried out, in order to check our compliance with our obligations under these Processing Terms. You are responsible for the payment of all your internal and external costs (including of the independent auditor appointed by you) in this context. We may invoice you for our own costs associated with the preparation for and execution of the audit based on the costs incurred by us. We may object to any independent auditor appointed by your if, in our opinion, the auditor is not sufficiently qualified, is a competitor of us, or in any other way would not be able to perform its duties properly. In this case, you may either carry out the audit itself or propose another auditor to us.

5.3.2 **Confidential information**. The provisions contained in this Section 5 shall not be interpreted as requiring us to provide you with (i) any information relating to our trade secrets or any information of a confidential nature or (ii) any information concerning our customers or users (except you). We may make the review of documents or the conduct of an audit subject to the conclusion of a specific confidentiality agreement.

6. ASSISTANCE

6.1 **In General**. We will, if so requested by you, provide you with the assistance reasonably necessary for you to meet your obligations under the Applicable Data Protection Legislation, as further specified in Sections 6.2 to 6.3 below. We reserve the right to charge fees for our activities under this Section 6 if we incur internal or external costs in this context. You also undertake to provide us with all necessary information to enable us to demonstrate compliance with our obligations under the Applicable Data Protection Legislation.

6.2 **Requests from data subjects**. If we receive a request from a data subject regarding Shared Personal Data, we will direct the data subject to submit its request to you (provided we can link the data subject to you), and you are responsible for responding to all such requests. We will assist you in complying with your legal obligations to the data subjects, to the extent reasonable. The measures shall cover all rights of the data subjects under any Applicable Data Protection Legislation, in particular access, rectification, limitation, objection, erasure and portability of their Shared Personal Data.

6.3 **Impact assessments and prior consultation**. If the GDPR applies to the processing of the Shared Personal Data, we undertake, to the extent it can reasonably be expected to do so in light of the nature of the processing and the information available to us, to assist you in ensuring your compliance with its impact assessment and prior consultation obligations pursuant to Articles 35 and 36 GDPR.

7. DATA TRANSFERS

7.1 **Transborder transfers**. You agree that we will retain and process Shared Personal Data in Switzerland. We will inform you (unless we are under a legal obligation not to disclose) prior to any transfer of the Shared Personal Data to any other country. You undertake to authorize such transfer provided we can guarantee by any useful means an adequate level of protection for the Shared Personal Data.

7.2 **Sub-processors**. You authorize us to use sub-processors provided we ensure in writing that:

(a) the sub-processor will only access and process Shared Personal Data to the extent necessary to perform its obligations;

(b) the sub-processor has contractual obligations to us that are at least equivalent to ours to you arising from these Processing Terms and the ToU; and

(c) if the GDPR applies, the obligations set forth in Article 28(3) of the GDPR have been imposed on the sub-processor.
The current list of sub-processors is available at [URL link; annex, etc.]. If the GDPR applies, we undertake to inform you at least 30 days in advance and in writing of any planned changes with respect to the addition or replacement of sub-processors, in order to permit you to raise objections. If we confirm the appointment of the sub-processor, you may terminate your agreement with us with immediate effect by deleting your Account (and all associated Accounts). This termination right is your sole and exclusive remedy in the event of an objection to a new sub-processor. If you do not react within the 30 days deadlines specified above, you will be deemed to accept the new sub-processor.

7.3 **Data Available Online**. You further acknowledge and agree that the NExT Platform enables you to make the Shared Personal Data available online to other users or visitors of the NExT Platform (registered or not). Such users and visitors may be located anywhere in the world, where the Shared Personal Data will be available. As further specified in the ToU, you are responsible for ensuring that your use of our Service in this context conforms to Applicable Data Protection Laws.

8. MISCELLANEOUS

8.1 **Register of processing activities**. You acknowledge that we may be required, in particular by the GDPR, to:

(a) collect and store certain information, including the name and contact details of each processor and/or controller with whom we act and, where applicable, the local representative of the controller and/or the data protection officer, as well as the categories of processing carried out; and

(b) make such information available to any competent authority.
You undertake to provide us with all information reasonably necessary for us to meet our obligations.

8.2 **Severability**. If any provision of these Processing Terms is held to be invalid or unenforceable for any reason, the parties shall replace it by a substitute provision that achieves to the fullest extent possible the same legal and economic purposes as those of the invalid or unenforceable provision. In any event, the remainder of these Processing Terms shall remain in full force and effect between the parties hereto. Without limiting the foregoing, if the provisions on governing law in the ToU may not apply in relation to all or part of these Processing Terms due to a mandatory provision of an Applicable Data Protection Law, the parties hereto agree to apply the law of the State imposing such restriction (and where the law of several countries may apply, those with which SBP has the closest connection).

8.3 **Contact us**. All communications to us relating to these Processing Terms and/or data protection must be addressed to sbpnext@swissbiobanking.ch.

8.4 **Amendments**. These Processing Terms may be amended from time to time, in which case you will be notified by any appropriate mean (including via e-mail, or via the NExT Platform, e.g. through banners, pop-ups or other notification mechanisms). Any use of the NExT Platform subsequent to this notification shall constitute acceptance of the Processing Terms as amended.