DATA PROCESSING ADDENDUM

Last updated: December 2025

This Data Processing Addendum (this "**DPA**") forms part of the Terms and Conditions for LabSVIFT Web Service ("**Agreement**") between PHC Europe B.V. ("**Company**") and Customer and reflects the parties' agreement with regard to the Processing of Personal Data (as each term is defined below). Any capitalized terms not otherwise defined herein shall have their meaning as set forth in the Agreement.

1. DEFINITIONS

1.1. **"Customer Personal Data"** means any Personal Data Processed by Company, or any Company Sub-processor, on behalf of Customer as part of providing the Service.

1.2. **"Controller"** means the entity that determines the purposes and means of the Processing of Personal Data.

1.3. **"Data Protection Laws"** means any applicable laws governing the Processing of Personal Data, such as the Swiss Federal Data Protection Act ("FDPA") and its Ordinance and other related laws and any applicable data protection laws relating to the protection of individuals with regards to the processing of personal data including but not limited, to (i) the General Data Protection Regulation (EU) 2016/679 ("GDPR"); (ii) the GDPR as transposed into the national laws of the United Kingdom ("UK GDPR"); (iii) the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data Protection of the UAE ("PDPL");as well as (iv) any other applicable data protection or privacy laws in the EMEA Region, in each case as amended, replaced, or supplemented from time to time; and (v) any artificial intelligence laws, regulations and binding guidance that apply to the processing of Personal Data in connection with the respective party's performance under this Agreement, or to the privacy of electronic communications, to the extent applicable.

1.4. "**Data Subject**" means a natural person who is the subject of the Personal Data being Processed.

1.5. "**EMEA Region**": refers to the countries of Europe, the Middle East, and Africa, including the EEA Member States, the United Kingdom, Switzerland, and other jurisdictions within these territories that maintain applicable data protection laws.

1.6. **"Personal Data"** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household. This definition includes "Personal Data," "Personal Information," or "Personally Identifiable Information," as defined by any applicable Data Protection Laws.

1.7. **"Processor"** means the entity which Processes Personal Data on behalf of the Controller.

1.8. **"Process," "Processes," or "Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means.

1.9. **"Personal Data Breach"** means any unauthorized disclosure, access, or acquisition of Customer Personal Data that compromises the security, confidentiality, or integrity of such data.

1.10. **"Sub-Processor"** means any third party (including any Company affiliate) that is appointed by Company to Process Personal

Data on behalf of Customer.

1.11. "**International Transfers**" means the Company transferring or otherwise processing Customer Personal Data outside its country of origin within the EMEA region, including outside Switzerland, the United Kingdom, the European Economic Area, and/or any country that has not been identified by a regulator under the Data Protection Laws as a country that provides an adequate level of protection, either directly or via onward transfer;

1.12. "**SCCs**" means (i) the standard contractual clauses set out in Commission Implementing Decision (EU)2021/914 for the transfer of personal data to third countries pursuant to GDPR, as updated, amended, replaced and superseded from time to time ("EU SCCs"); (as recognised by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") in an official communication (The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contract) dated 27 August 2021) (ii) any corresponding or equivalent international data transfer agreement ("IDTA") adopted by the supervisory authority in the United Kingdom, (iii) or any equivalent or legally recognized standard data transfer clauses or instruments issued, adopted, or approved under the applicable data protection laws of any other jurisdiction in the EMEA Region in which the parties process or transfer personal data ("Regional SCCs").

1.13. The terms "supervisory authority" and "transfer" shall have the same meanings ascribed to them under the Data Protection Laws.

2. PROCESSING OF PERSONAL DATA

2.1. The parties acknowledge and agree that with regard to the Processing of Customer Personal Data, Customer is the Controller and Company is the Processor as further specified in the Details of the Processing (Schedule 1) and that Company will engage Sub-Processors pursuant to the requirements set forth in Clause 6 "Sub-processors" below.

2.2. Customer shall, in its use of the Service, at all times be in compliance with all Data Protection Laws. Customer hereby represents and warrants that it has any and all consents, authorizations, rights, and authority necessary to transfer or disclose, and permit Company to Process, any and all Customer Personal Data in connection with the Agreement. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws.

2.3. Company shall treat Personal Data as confidential information and shall only process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Company's users in their use of the Service; and (iii) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

2.4. The subject-matter of Processing of Personal Data by Company is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

Company shall notify Customer without undue delay if Company receives a request from a Data Subject to exercise the Data Subject's right under the Data Protection Laws (“**Data Subject Request**”), which may include right of access, right to rectification, right to erasure, right to data portability, right to object to the Processing, right not to be subject to an automated individual decision making and right to restriction of processing. Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request.

4. COMPANY PERSONNEL

Company shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are subject to obligations of confidentiality with respect to such data. Company shall ensure that access to Personal Data is limited to those personnel performing Services in accordance with the Agreement and obligations under this DPA.

5. PERSONAL DATA BREACH

5.1 Company shall notify Customer promptly upon becoming aware of any personal data breach involving Customer Personal Data. Company will provide: (i) a description of the nature of the Personal Data Breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) a description of the likely consequences of the Personal Data Breach; (iii) and a description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

5.2 Company agrees to assist and cooperate with Customer concerning any disclosures to affected parties, government or regulatory agencies and with any other remedial measures required under any law. Company will take such mutually agreeable steps to prevent the continuation or repetition of such personal data breach.

5.3 The obligations herein shall not apply to Personal Data Breaches that are caused by Customer. Company will not contact any Data Subject directly, unless Customer is unable to do so itself, requests Company’s assistance in notifying the data subject, and Company has the reasonable means to make a notification on Customer’s behalf.

6 SUB-PROCESSORS

6.1 Customer acknowledges and agrees that (a) Company’s affiliates and related entities (collectively, “**Affiliates**”) may be retained as Sub-Processors; and (b) Company and Company’s Affiliates, respectively, may engage third-party Sub-Processors in connection with the provision of the Service.

Company and Company’s Affiliates can engage another processor based on this DPA. Both Company and its Affiliates have in the past engaged and continue to engage Sub-Processors.

6.2 Company receives prior general written authorization of Customer to involve core Sub-Processors as listed in SCHEDULE 1.

Company shall inform Customer of any intended changes concerning the addition or replacement of other Sub-Processors. If the Customer does not raise written objection to such changes on data protection grounds within 20 days following receipt of the notice, the new Sub-Processor shall be deemed to have been accepted by Customer. If an objection is made in time and the Customer has reasonable grounds to believe that the use of the Sub-Processor in question would conflict against Data Protection Laws, and the parties are unable to reach a mutually agreeable solution, the Customer shall have the right to terminate the agreement.

6.3 Company or a Company Affiliate have entered into a written agreement with each Sub-Processor containing the same data protection obligations as set out in this in this DPA with respect to the protection of Customer Personal Data to the extent applicable to the nature of the services provided by such Sub-Processor. Company shall be liable for the acts and omissions of its Sub-Processors to the same extent Company would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7 TRANSFERS

7.1 Company can perform any International Transfers, where an Affiliate, agent or approved subcontractor is covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, and in each case will remain so for the duration of any such processing. Where Company seeks to otherwise transfer Customer Personal Data to any other country or location, it receives Customer's prior written consent, and such consent shall be conditioned upon Company and/or other Data Importer complying with a binding agreement to ensure adequate protection of the Customer Personal Data, such as the SCCs.

7.2 To the extent SCCs are required where the data exporter(s) is Customer (as Controller) and the data importer(s) is the Company (as Processor), they are incorporated into this Agreement by reference as follows:

a. For the purpose of the EU SCCs (Module II): Clause 7 and the optional language in clause 11(a) shall not apply, option 2 of clause 9(a) shall apply, the supervisory authority for the purposes of clause 13(a) shall be determined by the place of establishment of the data exporter, the governing law and choice of forum and jurisdiction shall be those of Switzerland. The frequency of the transfer shall be continuous, as necessary to deliver the services, and retention shall be determined by the Company's corporate record retention schedules and policies.

b. For the purposes of Annex II of the EU SCCs and/or any IDTA the technical and organizational measures shall be as set out at clause 8 of this DPA.

c. For the purposes of Annex I of the EU SCCs and/or any IDTA:

i. The data subjects shall be as set out in SCHEDULE 1 below.

ii. The categories of personal data shall be as set out in SCHEDULE 1 below.

iii. The purposes of the transfer are as described in SCHEDULE 1 below;

iv. The recipients are the recipients to whom it is necessary to disclose data to achieve the purposes described in clause 2.1 of this DPA; and

v. The contact points for data protection enquiries are as set out in clause 10 of this DPA.

7.3 With respect to International Transfers subject to the FADP, the EU SCCs as set out under clause 7.2 of this DPA above shall be amended as follows:

a. The Swiss FDPIC shall act as the competent supervisory authority;

b. The governing law and choice of forum and jurisdiction set out in the Agreement shall apply;

c. The term "Member State" shall not be interpreted to exclude data subjects in Switzerland from pursuing their rights at their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs. Accordingly, data subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland; and

d. References to the GDPR should be read as references to the FADP.

7.4 For the avoidance of doubt (and without prejudice to third party rights for data subjects under the SCCs) the Parties submit to the limitations set out in the Agreement with respect to their respective liability towards one another under the SCCs.

8 SECURITY

Customer and Company shall each maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of Customer Personal Data. Company will not materially decrease the overall security of the Service during a Contract Period and follow the measures listed in Schedule 2.

9 AUDITS

To the extent permitted under the Data Protection Laws, Company shall make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, to the extent commercially reasonable, and not more than once per year. The costs of the audit provided for in this Clause shall be borne by Customer. Customer shall be informed promptly of any inspections, investigations and measures notified by the supervisory authority to the Company, insofar as they relate to the processing of Customer Personal Data.

10 OTHER DUTIES

10.1 Where a Data Protection Impact Assessment ("DPIA") is required under applicable Data Protection Laws for the Processing of Personal Data, Company shall provide, upon request, to Customer any information and assistance reasonably required for the DPIA.

10.2 The contacts for data protection matters are:

Company: dp_office@phchd.com
Customer: [Customer to insert]

11. RETURN AND DELETION OF CUSTOMER PERSONAL DATA

Upon termination of the Agreement, Company shall at Customer’s option, return Customer Personal Data to Customer or delete Customer Personal Data without undue delay to the extent allowed by Data Protection Laws.

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Company will Process Personal Data as necessary to (i) manage the Service; and (ii) perform the Service pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Service.

Duration of Processing

Except as otherwise provided for in the DPA or Agreement, Company will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Contact persons of Customer
- Employees, agents, officers (who are natural persons) authorized by Customer to use the Service as Authorized Users

Type of Personal Data

Customer may submit Personal Data to the Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Contact information (company, email, phone, physical business address)
- Employee ID data
- System user ID
- Logs on the use of the Service

Sub-Processors

Sub-processor	Location of processing	Description	Data Categories Processed
Microsoft (MS Azure)	Northern Europe	Provides the cloud service infrastructure.	Account information, authentication data

Twilio Inc.	Unites States	Provides telephony and SMS delivery services. For SMS distribution and outbound calls, Twilio uses customers’ phone numbers and email addresses as destinations. As a result, these details are retained in SMS delivery logs and call logs.	Name, Phone number
Persol Communication Services (CSL)	Japan	Handles call center operations, including email communication with customers.	Name, Phone number, Mail address

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

The Company has measures in place to:

1. Ensure that Agreement Personal Data can be accessed only by authorized personnel for the purposes set forth in the Distribution Agreement.

2. Take all reasonable measures to prevent unauthorized access to Agreement Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities.

3. Use secure passwords encryption and authentication technology, secure logon procedures and virus protection. Azure Entra ID multi-factor authentication is adopted to prevent unauthorized access to privileged accounts, proactively blocking attackers from infiltrating the system.

4. Account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, alteration, temporary or permanent inability to access, unauthorized or unlawful storage, processing, access or disclosure of Agreement Personal Data.

5. Ensure pseudonymization and/or encryption of Agreement Personal Data, where appropriate.

6. Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience processing systems and services.

7. Maintain the ability to restore the availability and access to Agreement Personal Data in a timely manner in the event of a physical or technical incident.

8. Implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Agreement Personal Data.

9. Implement measures to identify vulnerabilities with regard to the processing of Agreement Personal Data in systems used to provide services to ADC.

10. Provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in policy.