APPENDIX 2

Data Processing Agreement

(I) DATA PROCESSING AGREEMENT

Between

CUSTOMER

the Controller – "COMPANY" –

and

ROCHE

the Processor – "ROCHE" –

1. SUBJECT MATTER AND DURATION

(1) Subject matter

This data processing agreement ("**Data Processing Agreement**") forms as an attachment an integral part of the Service Agreement (hereinafter referred to as "**Service Agreement**"). The subject matter of this Data Processing Agreement results from the Service Agreement.

(2) Duration

The duration of this Data Processing Agreement corresponds to the duration of the Service Agreement.

2. SPECIFICATION

(1) Nature and purpose of the processing of personal data

Nature and purpose of processing of personal data by ROCHE for COMPANY are precisely defined in Section 1 of the Service Agreement.

(2) Geographic scope

The undertaking of the contractually agreed processing of personal data shall be carried out exclusively within a member state of the European Union (EU) or within a member state of the European Economic Area (EEA). Each and every transfer of personal data to a state which is not a member state of either the EU or the EEA requires the prior agreement of COMPANY and shall only occur if the specific conditions of Article 44 et seq. GDPR have been fulfilled.

(3) Type of personal data

The type of personal data used is precisely defined in the Service Agreement in Appendix 3.

(4) Categories of data subjects

The categories of data subjects are precisely defined in the Service Agreement in Appendix 3.

3. TECHNICAL AND ORGANISATIONAL MEASURES

(1) The necessary technical and organisational measures are documented in **Appendix 1** hereto ("**Technical and Organisational Measures**") and are hereby approved by COMPANY. The documented measures form the foundation of the Data Processing Agreement. Insofar as the COMPANY requires amendments, such amendments shall be implemented by mutual agreement.

(2) Based on the agreed Technical and Organisational Measures, ROCHE shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR in accordance with the instructions of the COMPANY. The Technical and Organisational Measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR are taken into account.

(3) COMPANY shall label and appropriately limit the data disclosure to which has been described as the subject matter of the services of ROCHE.

(4) ROCHE shall inform COMPANY if, in ROCHE's opinion, any COMPANY instruction infringes any applicable data privacy law, provided that this requirement shall not create any obligation on ROCHE to independently investigate or provide legal or regulatory advice.

(5) If COMPANY requires that ROCHE follow a processing instruction despite ROCHE's notice that such instruction infringes an applicable data privacy law, COMPANY shall be responsible for all liability, and shall defend, indemnify and hold ROCHE harmless against all claims and damages, arising from any continued processing in accordance with such instructions.

(6) As of the effective date of this Data Processing Agreement, COMPANY hereby acknowledges and agrees that it considers the Technical and Organisational Measures described in **Appendix 1** to be appropriate, taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk to data subjects.

(7) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for ROCHE to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be agreed by the parties and documented in **Appendix 1**.

(8) In the event of any change to (including changes in, or further guidance regarding, interpretation of) an applicable data protection law which requires a change to all or any part of the Technical and Organisational Measures that increases ROCHE's costs and expenses will be subject to mutual agreement on the compensation.

4. RECTIFICATION, RESTRICTION AND ERASURE OF PERSONAL DATA

(1) ROCHE may not on its own authority rectify, erase or restrict the processing of personal data that is being processed on behalf of COMPANY, but only on documented instructions from COMPANY.

Insofar as a data subject contacts ROCHE directly concerning a rectification, erasure, or restriction of processing, ROCHE will forward the data subject's request to COMPANY without undue delay.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by ROCHE in accordance with documented instructions from COMPANY without undue delay.

5. QUALITY ASSURANCE AND OTHER DUTIES OF ROCHE

In addition to complying with the rules set out in this Data Processing Agreement, ROCHE shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, ROCHE ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his duties in compliance with Articles 38 and 39 GDPR. ROCHE has appointed Olivier Convard, Roche Diabetes Care Spain S.L., global.rdc-dpo@roche.com as Data Protection Officer. COMPANY shall be informed immediately of any change of Data Protection Officer.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. ROCHE entrusts only such employees with the data processing outlined in this Data Processing Agreement who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. ROCHE and any person acting under its authority who has access to personal data, shall not process that personal data unless on instructions from COMPANY, which includes the powers granted in this Data Processing Agreement, unless required to do so by applicable law.

c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Data Processing Agreement in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR and as set forth in Section 3 and **Appendix 1**.

d) ROCHE and COMPANY shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) COMPANY shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Data Processing Agreement. This also applies insofar as ROCHE is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the processing of personal data in connection with this Data Processing Agreement.

f) Insofar as COMPANY is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with this Data Processing Agreement data processing by ROCHE, ROCHE shall make every effort to support COMPANY.

g) ROCHE shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organisational Measures conducted by COMPANY as part of COMPANY's supervisory powers referred to in Section 7 of this Data Processing Agreement.

6. SUBCONTRACTING

(1) Subcontracting for the purpose of this Data Processing Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. ROCHE shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of COMPANY's data, even in the case of outsourced ancillary services.

(2) ROCHE may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from COMPANY.

a) COMPANY agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

COMPANY subcontractor	Address/country	Service
Accenture AG	Accenture AG Fraumunsterstr. 16 CH-800 1 Zurich Switzerland	☒ Hosting ☒ Maintenance ☒ Storage ☒ Support ☒ Testing

b) Changing the existing subcontractor

are permissible when:

- ROCHE submits such an outsourcing to a subcontractor to COMPANY in writing or in text form with appropriate advance notice; and
- COMPANY has not objected to the planned outsourcing in writing or in text form within two weeks following ROCHE's submission to COMPANY; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from COMPANY to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, ROCHE shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor requires the express consent of ROCHE (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. SUPERVISORY POWERS OF COMPANY

(1) The COMPANY has the right, after consultation with ROCHE, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this Data Processing Agreement by ROCHE in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) ROCHE undertakes to give COMPANY the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures may be provided by

- Compliance with approved Codes of Conduct pursuant to Article 40 GDPR; and/or
- Certification according to an approved certification procedure in accordance with Article 42 GDPR; and/or
- Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); and/or
- A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) ROCHE may claim remuneration for enabling COMPANY inspections.

8. COMMUNICATION IN THE CASE OF INFRINGEMENTS BY ROCHE

(1) ROCHE will assist COMPANY in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach without undue delay to COMPANY.

c) The duty to assist COMPANY with regard to COMPANY's obligation to provide information to the Data Subject concerned and to immediately provide COMPANY with all relevant information in this regard.

d) Supporting COMPANY with its data protection impact assessment.

e) Supporting COMPANY with regard to prior consultation of the supervisory authority.

(2) ROCHE may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of ROCHE.

9. AUTHORITY OF COMPANY TO ISSUE INSTRUCTIONS

(1) COMPANY shall immediately confirm oral instructions (at the minimum in text form).

(2) ROCHE shall inform COMPANY immediately if he considers that an instruction violates data protection regulations. ROCHE shall then be entitled to suspend the execution of the relevant instructions until COMPANY confirms or changes them.

10. DELETION AND RETURN OF PERSONAL DATA

(1) Copies or duplicates of the data shall never be created without the knowledge of COMPANY, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by COMPANY, at the latest upon termination of the Service Agreement, ROCHE shall hand over to COMPANY or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Data Processing Agreement shall be stored beyond the contract duration by ROCHE in accordance with the respective retention periods. It may hand such documentation over to COMPANY at the end of the contract duration to relieve ROCHE of this contractual obligation.

- **Appendix 1**
- **Technical and Organisational Measures**

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control

  No unauthorised access to data processing facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems.

  Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

  The infrastructure is on Amazon Web Services Cloud ("AWS Cloud") in ISO 27001 certified data centers in Germany.

  Security measures for the AWS Cloud:

  - Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means.
  - Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.

  Security Measures for ROCHE premises:

  - Assets and facilities are protected using the appropriate means based on the ROCHE Security Standards
  - All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, access control mechanisms and other measures to prevent equipment and data center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the data center facilities. To protect proper functionality, physical security equipment undergo maintenance on a regular basis.
  - In general, buildings are secured through access control systems (e.g., smart card access system).
  - Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures.

- Access rights are granted to authorized persons on an individual basis according to the system and data access control measures.
- Guests and visitors to ROCHE buildings must register their names at reception and must be accompanied by authorized ROCHE personnel.
- ROCHE employees and external personnel must wear their ID cards at all ROCHE locations.
- ROCHE and all third-party data center providers log the names and times of authorized personnel entering ROCHE's private areas within the data centers.
- Secure rooms are in place from where personal and sensitive personal data can only be accessed by authorized personnel.

- Electronic Access Control

  No unauthorised use of the Data Processing and Data Storage Systems: (secure) passwords, automatic blocking/locking mechanisms, encryption of data carriers/storage/storage media.

  ROCHE only allows authorized personnel to access Personal Data as required in the course of their duty.

  Data processing systems used to provide the service must be prevented from being used without authorization.

  Measures:

  - Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the ROCHE Security Policy.
  - All personnel access ROCHE's systems with a unique identifier (user ID).
  - ROCHE has procedures in place to so that requested authorization changes are implemented only in accordance with the ROCHE Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
  - ROCHE has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form.
  - The ROCHE network is protected from the public network by firewalls.
  - Security patch management is implemented to provide regular and periodic deployment of relevant security updates.

- Access to personal and sensitive personal by authorized personnel is done through VPN. All VPN logins are monitored.

- Internal Access Control (permissions for user rights of access to and amendment of data)

  No unauthorised reading, copying, changes or deletions of data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events.

  A ROCHE ID and appropriate access rights are requested for each system. Only authorized personnel that require access to the system to perform their work (need to know basis) duties is allowed. A logging system is in place to ensure traceability of the actions performed and audit trails are kept.

2. Pseudonymization and Encryption of Data (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)

The processing of personal data in this release is in such a method that clinical medical data is in a different database from specific Data Subject identifiable data. Thus, information is stored separate and is subject to appropriate technical and organisational measures.

Clinical and non-clinical data bases are related by IDs assigned to each user that are generated without involving Data Subject's personal data.

Application processing in the solution occurs using tokens in such a way that do not involve personal data and are not able to identify the Data Subject.

3. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control

  No unauthorised reading, copying, changes or deletions of data with electronic transfer or transport, e.g.: encryption, virtual private networks (VPN), electronic signature.

  SSL layer over HTTP protocol to secure the communication through untrusted network Internet is used in this solution.

  Access to back-end systems is done via VPN. ROCHE credentials (unique Roche ID) and access rights are required to be able to connect.
- Data Entry Control

  Verification, whether and by whom personal data is entered into a data processing system, is changed or deleted, e.g.: logging, document management.

  ROCHE has implemented a logging system for input, modification and deletion of data. This traceability logs include user access, type of access and file/register accessed, among other details.

  ROCHE has implemented validation of data entry in information fields accepting input information from users, including security controls on top of business logic validations of information.

Business logic validations include among others: no mandatory fields are missing, format and control length of the fields accepting input.

Authorization controls are also in place, so that validation verifies that each logged in user is entitled to perform an action in the system.

4. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control

  Personal Data will be protected against accidental or unauthorized destruction or loss.

  General Measures:
  - ROCHE implements regular backup processes to provide restoration of business-critical according to backup strategy,
  - ROCHE uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the data centers.
  - ROCHE has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical services.

  Specific Measures for Operations:
  - Application is protected with specific security architecture following the defence in depth principle
    - Perimeter firewall in high availability configuration. Only allowing access on allowed ports for the application
    - External web application firewall (WAF) in high availability configuration
    - Application design allows high availability and elasticity
    - Segregation of traffic at different layers: Firewall, AWS Security Groups, dockers / kubernetes policies to segregate front-end and back-end pods
    - Antivirus is installed in every EC2 instances and centrally managed. Antivirus is updated periodically
    - Infrastructure is monitored in terms of availability and performance
    - Specific security monitoring and incident management process in place
    - ROCHE employs regular backup processes to provide restoration of business-critical systems as and when necessary. All production infrastructure is backed up on daily basis (via AWS snapshots) and snapshots are retained for 7 days.

- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

  ROCHE executes regular disaster recovery exercises, at least once a year.

5. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;

  ROCHE has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, ROCHE uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Encryption of data in transit and at rest

The DPO is given the required independence to perform his tasks. The DPO and the corporate Data Privacy Office, in a timely manner, in all issues relating to the protection of

personal data.

- Incident Response Management;

ROCHE applications and underlaying infrastructure is monitored in a 24x7 window to detect security events or potential incidents. A security incident management process is in place to ensure that:

- Incident response is activated, and right steps are taken, communications launched, etc.
- Helping to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Initiate corrective actions (lowers repeat rate) and preventive actions to prevent this to happen.

In case of a personal data is involved in the security incident, the ROCHE Personal Data Breach Process is activated, and the Data Protection Officer notified in order to activate activities required by current legislations i.e. communication to authorities or Data Subjects when needed.

- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);

According to the sensitivity of health data, ROCHE designed the Platform in line with data-protection principles, such as data minimisation, encryption of data, and is committed to continuously maintain and enhance the security and privacy levels with appropriate technical and organisational measures, designed in an effective manner and in order to meet the requirements of GDPR and protect the rights of Data Subjects.

By default, only personal data which are necessary for each specific purpose of the processing are processed, involving the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

- Order or Contract Control

No third party data processing as per Article 28 GDPR without corresponding instructions from ROCHE.

ROCHE ensures proper contractual arrangements, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.