DATA PROCESSING ADDENDUM

This Data Processing Addendum (“DPA”) is incorporated into and forms part of the Master Licence and Services Agreement or Supply and License Agreement ("MLSA") between the respective Lunit (“Vendor”) and Customer entities which are party to the MLSA. This DPA sets out the requirements for Vendor’s processing of Personal Data as a processor on behalf of Customer for the purposes of providing the Services. To the extent there is any conflict between the terms of this DPA and the terms of an MLSA, then the terms of this DPA shall control with respect to Vendor’s processing of Customer Personal Data.

1 Definitions

1.1 The following defined terms apply to this DPA:

Adequate Country	means a country or territory recognised as providing an adequate level of protection for Personal Data under an adequacy decision or regulations made, from time to time, by (as applicable) (i) the UK Secretary of State under applicable UK law (including the UK GDPR), or (ii) the European Commission under the EU GDPR, or (iii) the Swiss Federal Council under Swiss Data Protection Law.
Data Protection Laws	means as applicable: (a) in the European Union, the General Data Protection Regulation 2016/679 (the “GDPR”) and other European local data protection and privacy laws that apply to the Customer on a local country basis, (b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the “UK GDPR”) and the Data Protection Act 2018, (c) Swiss Data Protection Law, (d) in Brazil, Law No. 13,709 of August 14, 2018, on the processing of personal data, including in digital media, by a natural person or a legal entity under public or private law, with the objective of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person (“Brazilian General Data Protection Law”), (e) any Mexican law related to the protection of Personal Data applicable to where the Vendor or Customer are established,

	(f) any Canadian federal or provincial law related to the protection of Personal Data applicable to where the Vendor or Customer is established, or (g) the Australia Privacy Act 1988.
Data Subject Request	means a request from or on behalf of a data subject to exercise any rights in relation to their Personal Data under Data Protection Laws.
EEA	means the European Economic Area.
Group One Product	means one or more of the following products: Analytics, Volpara Live, Volpara Scorecard.
Group Two Product	means one or more of the following products: Lunit INSIGHT CXR, Lunit INSIGHT MMG, Lunit INSIGHT DBT.
Personal Data	means all personal data which is Customer Data or is otherwise provided by the Customer as part of receiving the Vendor Services and is accessed, stored or otherwise processed by Vendor as a processor on behalf of Customer.
Security Breach	means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data by any of Vendor's staff or sub-processors, or any other identified or unidentified third party.
Vendor Services	means the provision of the Products and Services by Vendor as described in the MLSA and in the applicable Quotation and Statement of Work.
Supervisory Authority	means in the UK, the Information Commissioner's Office ("ICO"), in the EEA, an independent public authority established pursuant to the GDPR, and other regulatory authorities in applicable countries which are designated with enforcement of Data Protection Laws.
Swiss Data Protection Law	means the Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances as amended, superseded or replaced from time to time.
UK	means the United Kingdom.

1.2 "controller", "data subject", "personal data" (or “personal information”) and "processor", have the meanings ascribed to them in the Data Protection Laws (where applicable).

1.3 Any defined terms which are not defined in this DPA are as defined in the MLSA.

1.4 Additional requirements for certain jurisdictions are set out in Schedule 5.

2 Roles and compliance with Data Protection Laws.

2.1 Customer is the controller of Personal Data, and Vendor is the processor of Personal Data. Each party will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with Data Protection Laws applicable to such party in the processing of Personal Data. As between the parties, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Personal Data was acquired.

3 Description of Processing

3.1 The Subject matter, nature and purposes of the processing, duration, types of Personal Data and categories of Data Subject are set out in Schedule 1.

3.2 *Processing by Vendor.* As a processor, Vendor will only process Personal Data (i) in order to provide the Vendor Services to Customer or (ii) per Customer’s reasonable instructions in writing or via the Vendor Services. Vendor will notify Customer (unless prohibited by applicable law) if it is required under applicable law to process Personal Data other than pursuant to Customer’s instructions or to provide the Vendor Services. As soon as reasonably practicable upon becoming aware, Vendor shall inform the Customer if, in Vendor’s opinion, any instructions provided by the Customer under this clause 3 infringes applicable Data Protection Laws. Upon termination of the Agreement and upon written request of the Customer, Vendor shall return or securely delete the Personal Data, unless required by law to continue to store a copy of the Personal Data.

3.3 *Customer Instructions.* Vendor shall Process Customer Personal Data to provide the Vendor Services in accordance with the MLSA, this DPA, any applicable Quotation and Statement of Work, and any instructions agreed upon by the Parties in writing.

4 Technical and Organisational Security Measures

4.1 Vendor will implement, as a minimum, the technical and organizational security measures set out in Schedule 2 that are appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

4.2 Vendor will take reasonable steps to ensure that only authorised personnel have access to Personal Data and that any persons whom it authorizes to access Personal Data are under obligations of confidentiality.

5 Security Breaches, Data Subject Requests & Further Assistance

5.1 *Security Breaches*. Vendor will notify Customer of any Security Breach without undue delay.

5.2 *Data Subject Requests.* To the extent legally permitted, Vendor will promptly notify Customer if it receives a Data Subject Request. Vendor will not respond to a Data Subject Request without Customer's agreement, provided that Customer agrees Vendor may at its discretion respond to the data subject to confirm that such request relates to Customer. Customer acknowledges and agrees that the Vendor Services may include features which will allow Customer to manage Data Subject Requests directly through the Vendor Services without

additional assistance from Vendor. If Customer does not have the ability to independently respond to a Data Subject Request, Vendor will, upon Customer's written request, provide reasonable assistance to facilitate Customer's response to the Data Subject Request to the extent such assistance is consistent with applicable law; provided that Customer will be responsible for paying for any costs incurred or fees charged by Vendor for providing such assistance.

5.3 *Further Assistance.* Taking into account the nature of processing and the information available to Vendor, Vendor will provide such assistance as Customer reasonably requests in relation to Customer's obligations under Data Protection Laws with respect to (i) data protection impact assessments including consultation with the Supervisory Authority, (ii) notifications to the Supervisory Authority under Data Protection Laws and/or communications to data subjects by the Customer in response to a Security Breach, or (iii) Customer's compliance with its obligations under applicable Data Protection Laws with respect to the security of processing. Customer will pay any costs or fees charged by Vendor for providing the assistance in this Section 5.3.

6 Sub-processing

6.1 Customer grants a general authorisation to Vendor to appoint its Affiliates or third parties as sub-processors to support the performance of the Vendor Services, including data centre operators, cloud-based software providers, and other outsourced support and service providers. Vendor will maintain a list of sub-processors and will communicate to the Customer any intended changes to the sub-processor list at least thirty (30) days before such change takes effect. If Customer has a reasonable objection to any new or replacement sub-processor, it shall notify Vendor of such objections in writing within fifteen (15) days of receipt of the notification and the parties will seek to resolve the matter in good faith. If Customer, acting reasonably, is not reasonably satisfied that the sub-processor meets the security and privacy protections of applicable Data Protection Law then Customer, as its sole remedy may, within such 15-day period, terminate that part of the Agreement which relates to the impacted Products only.

6.2 Vendor will enter into a written contract with each sub-processor which imposes on such sub-processor terms no less protective of Personal Data than those imposed on Vendor in this DPA (the "Relevant Terms"). Vendor shall be liable to Customer for any breach by such sub-processor of any of the Relevant Terms to the extent required under Data Protection Law.

7 International Transfers and Processing

7.1 Customer agrees that its use of the Vendor Services will involve the transfer of Personal Data to, and processing of Personal Data by Vendor and its sub-processors in, locations outside of the country from which the Personal Data originates, for the purposes of providing the Vendor Services and support to Customer.

7.2 To the extent Personal Data is transferred by Vendor for further processing to a sub-processor outside the EEA, UK or Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited by applicable Data Protection Laws in the absence of an approved transfer mechanism, Vendor will enter into the appropriate terms with the sub-processor to legitimise the transfer in accordance with applicable Data Protection Laws.

8 Audit and Records

8.1 Vendor shall make available to the Customer such information in Vendor's possession or control as Customer may reasonably request with a view to demonstrating Vendor's compliance with the obligations of Vendor under this DPA in relation to its processing of Personal Data.

9 General

9.1 *Conflicts.* This DPA is without prejudice to the rights and obligations of the parties under the MLSA which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the MLSA, the terms (including definitions) of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data by Vendor as a processor. The English language version of this DPA shall be the governing version used when interpreting or construing this DPA. This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA.

9.2 *Limitation of Liability.* Vendor's maximum aggregate liability to Customer under or in connection with this DPA shall not under any circumstances exceed the maximum aggregate liability of Vendor to the Customer as set out in the MLSA. Nothing in this DPA will limit Vendor's liability for any liability or loss which may not be limited by agreement under applicable law.

9.3 *Governing Law; Venue.* Without prejudice to the provisions of the EU Clauses, Swiss Addendum and the UK Approved Addendum addressing the law which governs them, this DPA shall be governed by and construed in accordance with the laws which govern the MLSA and the venue(s) for disputes and claims under the MLSA shall also apply to disputes and claims under this DPA.

SCHEDULE 1

Data Processing Details

For the purposes of clause 3 of the DPA and any other applicable Schedules the parties set out below a description of the Personal Data being processed under the MLSA and further details required pursuant to the Data Protection Laws

Subject Matter of the Processing	Vendor's provision of the Vendor Services to Customer as set out in the MLSA, Quotation and Statement of Work.
Nature and purpose of Processing	The storage and processing of Personal Data pursuant to providing the Vendor Services to Customer.
Types of Personal Data	Personal Data including but not limited to: • Customer's employees' Personal Data such as name, email address, role, Vendor username and other relevant employee Personal Data required to deliver the Vendor Services to the Customer and related device information used to administer the Vendor Services by Customer's employee such as device serial number and IP address and other relevant device data required to deliver the Vendor Services to the Customer. • Customer's patient Personal Data such as name, address, relevant medical history, telephone, appointment location, date and time, age, gender, medical record number, Customer's patient Personal Data generated by the Vendor Services, and other relevant patient Personal Data required to deliver the Vendor Services to the Customer.
Categories of Data Subject	Data Subjects may include any end users (including without limitation employees, and patients of Customer) about whom Personal Data is provided to Vendor via the Vendor Services by, or at the direction of, Customer.
Duration of Processing	For the duration of the Agreement, or until the processing is no longer necessary for the purposes.

SCHEDULE 2

Security Measures

A current copy of Vendor's Security Measures is available at https://www.lunit.io/en/legal-terms.

SCHEDULE 3

Sub-processors: Group One Products

Name	Address and Contact Information	Description of the Processing
8x8, Inc.	675 Creekside Way Campbell, CA 95008 United States dpo@8x8.com Data centre: United States. Please note that 8x8 is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Receive and record customer phone calls
Absorb Software Inc.	Absorb LMS Software 685 Centre St S, Suite 2500 Calgary, Alberta Canada T2G 1S5 privacyofficer@absorblms.com Data centre: Canada	Collect customer employee personal data in order to register users for training curriculum
Microsoft Corporation (Azure)	Microsoft Corporation One Microsoft Place South County Business Park Leopardstown, Dublin 18, D18 P521, Ireland https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure?view=o365-worldwide https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-officer Data centre: United States; Canada; France Central; Ireland; Netherlands; Australia; New Zealand; Singapore.	Temporary storage of PHI images for the purposes of investigating customer issues/complaints
ServiceNow, Inc.	ServiceNow, Inc. Attn: Privacy 2225 Lawson Lane Santa Clara, CA 95054 U.S.A. privacy@servicenow.com Data centre: the United States. Please note that ServiceNow is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Storage of customer support requests, which may have personal information
Smartsheet Inc.	Smartsheet Inc. Attn: Legal - Privacy Office 500 108th Ave NE, Suite 200 Bellevue WA 98004 U.S.A.	Storage of customer project deliverables, which may have customer names and email addresses

	privacy@smartsheet.com Data centre: Germany; backup in Ireland	
Twilio Inc.	Twilio Inc. 101 Spear Street, 5th Floor, San Francisco, California, 94105, United States of America privacy@twilio.com Data Centre: the United States. Please note that Twilio is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Send and receive communication with customers on product questions and issues for customers based in Central and South America
WhatsApp LLC (Meta)	WhatsApp LLC 1601 Willow Road Menlo Park, California 94025 U.S.A. https://www.whatsapp.com/contact/forms/503092477794354/ Data Centre: United States. Please note that WhatsApp is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Send and receive communication with customers on product questions and issues for customers based in Central and South America

Sub-processors: Group Two Products

Name	**Address and Contact Information**	**Description of the Processing**
Microsoft Corporation (Azure)	Microsoft Corporation, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure?view=o365-worldwide https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-officer Data centre: Republic of Korea; United States; Germany; Netherlands; Australia; Singapore.	Cloud hosting of the Group Two Products and storage of Personal Data processed through them
Twilio Inc.	Twilio Inc. 101 Spear Street, 5th Floor, San Francisco, California, 94105, United States of America privacy@twilio.com Data Centre: the United States. Please note that Twilio is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Send and receive communication with customers on product questions and issues for customers based in Central and South America

Zendesk, Inc.	Zendesk, Inc. Attn: Associate General Counsel, Global Commercial 181 Fremont St. San Francisco, CA USA 94105 privacy@zendesk.com Data centre: United States. Please note that Zendesk is registered on the EU-US Data Privacy Framework (with Swiss and UK extensions)	Storage of customer support requests, which may have personal information

Affiliates: Group One Products

Name	Address and Contact Information	Description of the Processing
Lunit UK Ltd	Mynshull House Warr & Co Limited Stockport, SK1 1YJ United Kingdom	Provides deployment services, product training, and Tier 1 support to EU/UK customers
Lunit Denmark ApS	Rosenørns Alle 31, 2. 1970 Frederiksberg C Denmark	Provides administrative and operational support to customers
Lunit Americas, Inc.	3500 188th Street SW, Suite 335 Lynnwood, WA 98037	Provides project management services for customer deployment projects
Lunit International Limited	Level 4, 1 Victoria Street Wellington Central Wellington 6011	Provides Tier 2/3 support to customers for Group One Products

Affiliates: Group Two Products

Name	Address and Contact Information	Description of the Processing
Lunit Inc.	4-9F, 374 Gangnam-daero, Gangnam-gu, Seoul, 06241, Republic of Korea	Provides deployment services, product training, and support services
Lunit, USA, Inc.	24 W 35TH ST STE 500#922, New York, NY USA10001-2538	Provides support to U.S. customers
Lunit Europe GmbH	Ludwig-Erhard-Str. 30-34, 65760 Eschborn, Frankfurt, Germany	Provides support to EU/UK customers
Lunit Japan	Hibiya Park Front 19F ,2-1-6 Uchisaiwaicho, Chiyoda-Ku, Tokyo, Japan100-0011	Provides support to Japan customers
Lunit Denmark ApS	Rosenørns Alle 31, 2. 1970 Frederiksberg C Denmark	Provides administrative and operational support to customers

SCHEDULE 4

EEA AND UK DATA TRANSFERS

1. Definitions for this Schedule 4

EU Clauses	means the standard contractual clauses for international transfers of personal data to third countries set out in the European Commission's Decision 2021/914 of 4 June 2021 (at http://data.europa.eu/eli/dec_impl/2021/914/oj) incorporating Module Two for Controller to Processor transfers which forms part of this DPA in accordance with Annex 1 and 2 to this Schedule 4.
Swiss Addendum	means the addendum set out in Annex 3 to this Schedule 4.
UK Approved Addendum	means the template Addendum B.1.0 issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force from 21 March 2022.
UK Mandatory Clauses	means the Mandatory Clauses of the UK Approved Addendum, as updated from time to time and/or replaced by any final version published by the Information Commissioner's Office.

2. EU transfers:

2.1 To the extent Personal Data is transferred by Customer to Vendor and is processed by Vendor outside the EEA (except if in an Adequate Country) in circumstances where such transfer would be prohibited by EU GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses will apply in respect of that processing and are incorporated into this DPA in accordance with Annex 1 and 2 to this Schedule 4.

2.2 Annex 2 to this Schedule 4 contains the information required by the EU Clauses.

3. Swiss transfers:

3.1 To the extent Personal Data is transferred by Customer to Vendor and processed by Vendor outside Switzerland (except if in an Adequate Country) in circumstances where such transfer would be prohibited by Swiss Data Protection Laws in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the Swiss Addendum will apply in respect of that processing. The Swiss Addendum is incorporated into this DPA.

3.2 Annex 2 to this Schedule 4 contains the information required by the Swiss Addendum, including for the purposes of transfers to which this clause 3 applies.

4. UK transfers:

4.1 To the extent Personal Data is transferred by Customer to Vendor and is processed by Vendor outside the UK (except if in an Adequate Country) in circumstances where such transfer would be prohibited by UK GDPR in the absence of a transfer mechanism, the parties agree that the EU Clauses subject to the UK Approved Addendum will apply. The UK Approved Addendum is incorporated into this DPA.

4.4.1 Annex 4 to this Schedule 4 references the information required by Tables 1 to 4 inclusive of the UK Approved Addendum.

4.4.2 To the extent Personal Data is transferred to Vendor and processed by or on behalf of Vendor in the US, the Confirmatory Statement set out in Annex 4 to this Schedule 4 will apply.

5. Vendor may (i) replace the EU Clauses, the Swiss Addendum and/or the UK Approved Addendum generally or in respect of the EEA, Switzerland and/or the UK (as appropriate) with any alternative or replacement transfer mechanism in compliance with applicable Data Protection Laws, including any further or alternative standard contractual clauses formally approved from time to time and (ii) make reasonably necessary changes to this DPA by notifying Customer of the new transfer mechanism or content of the new standard contractual clauses (provided their content is in compliance with the relevant decision or approval), as applicable.

ANNEX 1 TO SCHEDULE 4

EU Clauses

1. For the purposes of this Annex 1 Schedule 4, the EU Clauses (Module Two – Controller to Processor), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN, shall be incorporated by reference to this Schedule 4 and the DPA and shall be considered an integral part thereof, and the Parties' signatures in the MLSA shall be construed as the Parties' signature to the EU Clauses. In the event of an inconsistency between the DPA and the EU Clauses, the latter will prevail.

2. For the purposes of the EU Clauses, the following shall apply:

   - Customer shall be the data exporter and controller and Vendor shall be the data importer and processor. Each Party agrees to be bound by and comply with its obligations in its role as exporter and importer respectively as set out in the EU Clauses.

   - Clause 7 (Docking clause) shall be deemed as included.

   - Clause 9 (Use of sub-processors): OPTION 2 – GENERAL WRITTEN AUTHORISATION shall apply. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors as set out in clause 6 of the DPA.

   - Clause 11 (Redress): optional clause (optional redress mechanism before an independent dispute resolution body) shall be deemed as not included.

   - Clause 13 (a) (Supervision):

     - The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

   - Clause 17 (Governing law):

     These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

   - Clause 18 (b) (Choice of forum and jurisdiction): The Parties agree that any dispute between them arising from the EU Clauses shall be resolved by the courts of Ireland.

3. Any provision in the EU Clauses relating to liability of the parties with respect to each other shall be subject to the limitations and exclusions of the MLSA.

4. Any provision in the EU Clauses relating to the right to audit shall be interpreted in accordance with Clause 5 of the DPA and the MLSA.

ANNEX 2 TO SCHEDULE 4

A. LIST OF PARTIES

Data exporter(s):
Name: Customer entity that is party to the MLSA
Address: As set out in the MLSA
Contact person's name, position and contact details: As set out in the MLSA
Activities relevant to the data transferred under these Clauses: data exporter will transfer Personal Data to the data importer as required for the provision of Services by the data importer under the Agreement and as set out in the DPA.
Signature and date: please refer to signature and date in the MLSA.
Role (controller/processor):
☒ Controller
☐ Processor

Data importer(s):
Name: Vendor entity that is party to the MLSA.
Address: As set out in the MLSA
Contact person's name, position and contact details: As set out in the MLSA
Activities relevant to the data transferred under these Clauses: data importer will process personal data as required for the provision of Services under the Agreement and as set out in the DPA.
Signature and date: signature and date in the MLSA.
Role (controller/processor):
☐ Controller
☒ Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Schedule 1 to the DPA

Categories of personal data transferred
See Schedule 1 to the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards
To the extent data fields set out in Schedule 1 to the DPA are considered special category data under applicable Data Protection Law

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Transfers will occur from time to time as required during the course of the performance of the Services under the Agreement.

Nature of the processing
See Schedule 1 to the DPA

Purpose(s) of the data transfer and further processing
See Schedule 1 to the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
See Schedule 1 to the DPA

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
See Schedule 3 to the DPA

C. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with Clause 13
See Annex 1 to Schedule 4

ANNEX I - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL
See Schedule 2 to the DPA

ANNEX II – LIST OF SUB-PROCESSORS
See Schedule 3 to the DPA

ANNEX 3 TO SCHEDULE 4

Swiss Addendum

In respect of transfers otherwise prohibited by Swiss Data Protection Law:

1. The Federal Data Protection and Information Commissioner ("**FDPIC**") will be the competent supervisory authority;

2. Data subjects in Switzerland may enforce their rights in Switzerland under Clause 18c of the EU Clauses; and

3. References in the EU Clauses to the EU GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

ANNEX 4 TO SCHEDULE 4

UK transfers

For the purposes of the UK Approved Addendum:

1. the information required for Table 1 is contained in Schedule 1 to this DPA and the start date shall be deemed dated the same date as the EU Clauses;
2. in relation to Table 2, the version of the EU Clauses to which the UK Approved Addendum applies is Module Two for Controller to Processor transfers;
3. in relation to Table 3, the list of parties and description of the transfer are as set out in Annex 2 of Schedule 4 of this DPA, Vendor's technical and organisational measures are set out in Schedule 2 of this DPA, and the list of Vendor's sub-processors shall be provided pursuant to section 6.1 of this DPA; and
4. in relation to Table 4, neither party will be entitled to terminate the UK Approved Addendum in accordance with clause 19 of the UK Mandatory Clauses.

To the extent Personal Data is transferred to Vendor and processed by or on behalf of Vendor in the US, the following confirmatory statement (Confirmatory Statement) will apply:

- The Customer has completed a transfer risk assessment (TRA). It has relied on the Department for Science, Innovation and Technology's Analysis of the UK Extension to the EU-US data privacy framework published in September 2023 (the DSIT analysis).

- The Customer is satisfied that the DSIT analysis concludes that US laws and practices provide adequate protections for people whose personal information is transferred to the US for risks to people's rights:

  (i) arising in the US from third parties that are not bound by this DPA accessing the transferred personal information in particular, government and public bodies; and

  (ii) arising from difficulties enforcing the DPA.

- The Customer considers that it is reasonable and proportionate for it to rely on the DSIT analysis, given the scope of this assessment is as required under Article 45 UK GDPR, and the enactment of adequacy regulations under Section 17A DPA 2018 by the Secretary of State and Parliament, on the basis of that assessment.

- The Customer will review this TRA if a new or amended version of the DSIT analysis is published, or the DSIT analysis is withdrawn.

SCHEDULE 5

ADDITIONAL PROVISIONS FOR CERTAIN JURISDICTIONS

To the extent that Data Protection Laws apply to transfers of Personal Data by Customers in any jurisdiction listed in this Schedule 5, the specific jurisdiction provisions of the relevant jurisdiction will also apply.

1. BRAZIL

A. Data Subjects' Requests. If a Brazilian data subject requests access to its personal data or confirmation of the processing, the Controller shall provide it to the data subject in a simplified format, immediately, or by means of a clear and complete declaration that indicates the origin of the data, the non-existence of registration, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy, within a period of fifteen (15) days from the date of the data subject's request.

B. International Transfers and Processing. In so far as the data transfers are subject to the LGPD, references to obligations, rules and rights not provided for in the LGPD and in conflict with Brazilian law, in a broad sense, shall not apply to the extent of the conflict. With regard to the transfer of Personal Data protected by LGPD, outside the Brazilian territory, in light of the absence of adequacy decisions issued by the Brazilian Data Protection Authority ("ANPD"), if the ANPD does not recognize the EU SCCs as providing a sufficient level of protection to allow for the transfer, the Parties shall enter into the Brazilian Standard Contractual Clauses (SCCs) as provided by ANPD's Regulation No. 19/2024, by 1st August, 2025.

C. Supervision. Where the data transfer is governed by the LGPD, the ANPD is the competent supervisory body.

D. Limitation of Liability. Notwithstanding anything to the contrary, either in the MLSA, the DPA or any other documents executed by the Parties, Customer's liability shall not be limited by: (ii) any compensation award or any fine or penalty imposed on Vendor arising from a breach of the Data Protection Laws caused by the action or omission of Customer; or (iii) any and all claims, costs, damages, fines, losses, liabilities, expenses and attorneys' fees related to the occurrence of security incidents suffered by Vendor and involving personal data processed pursuant to the MLSA arising from an action or omission by the Customer.

E. Governing Law; Venue. To the extent that personal data about data subjects located in Brazil will be processed, Brazilian law will apply to this DPA. The parties acknowledge that a data subject in Brazil may bring legal proceedings before the courts of Brazil.

2. MEXICO

A. Regarding Clause 3 of this DPA.

(i) The Vendor acknowledges and agrees that the processing of Personal Data must be conducted in accordance with applicable Mexican legislation, including the Federal Law on Protection of Personal Data Held by Private Parties ("LFPDPPP") and its implementing regulations, confidentially, and exclusively for the purposes necessary for the provision of the Vendor Services.

(ii) The Vendor may only process Personal Data in accordance with the Customers' documented instructions in this DPA, which the Customer shall ensure are aligned with the Customers' privacy notice.

(iii) The Processor shall be considered a Controller and shall assume the corresponding obligations when: (a) it processes or uses the Personal Data for a purpose other than that authorized by the Controller, or (b) it carries out a transfer of Personal Data in breach of the Controller's instructions.

B. Regarding Clause 6 of this DPA.

The Vendor may only transfer Personal Data under the following circumstances:

(i) When expressly authorized by the Customers, including as specified in this DPA.

(ii) When the transfer is to an Affiliate or is necessary for the subcontracting of services, provided that the Vendor ensures that the terms entered into with that Affiliate or subcontractor are no less protective of Personal Data than the data protection obligations established in this DPA and the applicable legislation.

(iii) When required by a competent authority. In such a case, the Vendor shall notify the Customer before making the transfer, to the extent permitted by law.

3. CANADA (INCLUDING QUEBEC)

A. The following "or other such breach of security and/or confidentiality relating to Personal Data as deemed under applicable Data Protection Laws" is added to clause 1.1. of the DPA, at the end of the definition of Security Breach.

B. Regarding clause 2.1 of this DPA, the parties acknowledge and agree that the Customer, in respect of Personal Data, may be a "custodian", "health information custodian", or similar under Data Privacy Laws and that the Customer hereby appoints the Vendor to act as its "agent", "information manager", or similarly regulated service provider in connection with all Personal Data.

C. Adding a Clause 2.2 of this DPA

2.2. If the Customer is located in Quebec, the following provisions of Quebec privacy laws notably apply to this DPA:

(a) For Customer's employees' Personal Data, in particular, sections 53, 53.1, 54, 55, 56, 57, 58, 59, 62, 63.8, 63.9, 63.10, 63.11, 65, 65.0.1, 65.0.2, 67.2, 83, 84, 89, 95 et 159 of the *Act respecting Access to documents held by public bodies and the Protection of personal information.*

(b) For Customer's patient Personal Data, in particular, sections 2, 3, 5, 6, 14, 15, 17, 18, 19, 44, 62, 65, 66, 80, 74, 77, 92, 93, 94, 95, 96, 108, 109, 110, 160 of the *Act respecting health and social services information*.

D. Adding Clauses 3.4 and 3.5 of this DPA

3.4. If the Customer is located in Quebec, the Vendor shall only use technology products or services authorized by the Customer to collect, store, use or disclose Personal Information.

3.5. If the Customer is located in Quebec, the Vendor shall transmit to the Customer, free of charge, upon thirty (30) day prior notice, any health and social services information contained in the Customer's patient Personal Data obtained from the Customer or produced for the Customer in the context of this DPA, provided that this obligation shall not extend to Personal Data that is aggregated with the Vendor's own proprietary data.

E. Adding a Clause 4.3 of this DPA

4.3 If the Customer is located in Quebec, the Customer attests that its privacy officer considers that this is not necessary for every person to whom the information may be disclosed to complete additional confidentiality undertaking.

F. Replacing Clause 5.1 of this DPA

5.1. Security Breaches. Vendor will notify Customer of any Security Breach or attempted Security Breaches at the first reasonable opportunity, and in any event without undue delay. Under no circumstances may the Vendor respond or otherwise communicate with the persons concerned by the Security Breach or with a third party in connection with a Security Breach, without obtaining the Customer's written authorization.

G. Replacing Clause 7.2 of this DPA

7.2. To the extent Personal Data is transferred by Vendor for further processing to a sub-processor outside of the jurisdiction in which Customer is located, Vendor will reasonably assist Customer to comply with its obligations under Data Protection Laws and will enter into reasonable appropriate terms with the sub-processor to legitimise the transfer in accordance with Data Protection Laws.