

## Section 1: Purpose

This Supplier Privacy Standard (this “SPS”) is subject to the applicable written or electronic agreement executed by and between Eli Lilly and Company and/or one or more of its Affiliates (“Lilly” or “Buyer”) and the entity entering into such agreement as “Supplier” or “Seller” (including all applicable amendments, purchase orders, work orders, order forms, service orders, schedules, exhibits, statements of work), to which this SPS may be attached. This SPS sets forth privacy and confidentiality requirements with respect to Personal Information Processed by the Parties to ensure that the Processing is compliant with applicable global privacy and data protection laws.

## Section 2: Definitions

The definitions below are for the purposes of this SPS. Any capitalized terms not defined shall take the meaning ascribed to them in the Agreement.

- (a) **“Affiliate”** means, with respect to any individual or a partnership, corporation, association, limited liability company, or other form of organization (“Person”), any entity that, at the relevant time (whether as of the effective date of the Agreement or thereafter), directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with such Person, for so long as such control exists.
- (b) **“Agreement”** means the applicable written or electronic agreement executed by and between Lilly and Supplier including all applicable amendments, purchase orders, work orders, order forms, service orders, schedules, or statements of work.
- (c) **“Applicable Privacy Laws”** means any statute, law, treaty, rule, code, ordinance, regulation, permit, judgment, decree, injunction, writ, order, or like action of a Governmental Authority that may apply to the processing of Personal Information, as the context requires for the performance of the obligations or activities related to the Agreement and this SPS, by a Party, a Party’s Affiliates (if any), a Party’s Subprocessors (if any), or to any of their representatives and any implementing rules or regulations associated with such laws, in each case, as may be amended or replaced from time to time.
- (d) **“Consent”** means any freely given, specific and informed indication of the individual's wishes by which he/she, by a statement or a clear affirmative action, signifies agreement to the Processing of his/her Personal Information in accordance with Applicable Privacy Laws.
- (e) **“Controller”** means the natural or legal person which, alone or jointly with others, determines the purposes and means of Processing of Personal Information, and includes equivalent terms under Applicable Privacy Laws.
- (f) **“Data Subject”** means the individual to whom the Personal Information relates and includes equivalent terms under Applicable Privacy Laws.
- (g) **“Data Privacy Framework”** means, collectively, the EU-US data privacy framework developed by the U.S. Department of Commerce and the European Commission, the UK Government’s UK Extension to the EU-US data privacy framework, and the Swiss Federal Administration’s Swiss-US data privacy framework, all designed to provide reliable mechanisms to lawfully transfer Personal Information to the United States from the European Union, United Kingdom, and Switzerland.
- (h) **“Deidentified Data”** means data that is not linked or reasonably linkable to, and cannot reasonably be used to infer information about, a particular individual, household or device as well as other information defined as “anonymous” or an equivalent term under Applicable Law.
- (i) **“Governmental Authority”** means any nation or government, any state or other political subdivision thereof and any entity exercising executive, legislative, judicial, regulatory or administrative functions of or pertaining to government.

- (j) **“Party” or “Parties”** shall have the meaning given in the Agreement, or, if no such definition exists, shall mean Lilly and Supplier, and any of each Party’s Affiliates that are bound by the Agreement or this SPS.
- (k) **“Personal Information”** means any information relating to an identified or identifiable natural person, as well as other information defined as “personal data,” “personal information” or an equivalent term under Applicable Law. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files. To the extent any other information, such as but not limited to, case report form information, clinical trial identification codes, personal profile information, other unique identifiers, or biometric information is Processed then such information will also be considered Personal Information. For the avoidance of doubt, Personal Information that has been pseudonymized, meaning that the information may not be attributed to a natural person without the use of additional information, will also be considered Personal Information to the extent required by Applicable Privacy Laws.
- (l) **“Process” “Processing” or “Processed”** means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, including but not limited to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, structuring, restriction, or otherwise making available, alignment or combination, blocking or erasure, or destruction.
- (m) **“Processor”** means the natural or legal Person which Processes Personal Information on behalf of a Controller, and includes equivalent terms under Applicable Privacy Laws, including but not limited to “subcontractor,” or “service provider.”
- (n) **“Personal Data Breach”** means any unauthorized, accidental, or unlawful destruction, loss, alteration, disclosure of, or access to, or any breach in the security of, or inability to account for Personal Information transmitted, stored or otherwise Processed or any “personal data breach,” “security incident,” or an equivalent term as defined under Applicable Privacy Laws.
- (o) **“Privacy Communication”** means any request regarding Personal Information received by Supplier from any individual or entity not otherwise a party to the Agreement between Lilly and Supplier.
- (p) **“Restricted Transfer”** means a transfer of Personal Information to a Party or a Subprocessor; or an onward transfer of Personal Information by a Party or Subprocessor, or between two establishments of Party or Subprocessor, in each case, where such transfer would be conditioned or prohibited by Applicable Privacy Laws in the absence of the Standard Contractual Clauses, the Data Privacy Framework, or other data transfer agreements required by Applicable Privacy Laws.
- (q) **“Sensitive Personal Information”** means a subset of Personal Information, which due to its nature has been classified by Applicable Privacy Law as deserving additional privacy and security protections.
- (r) **“Services”** means the particular products, goods, services, tasks, or activities that Supplier provides or performs for Lilly, as may be further detailed in the Agreement.
- (s) **“Standard Contractual Clauses” or “SCCs”** means (i) where the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the Processing of Personal Information and on the free movement of such data, and repealing Directive 95/46/EC (the “General Data Protection Regulation” or “GDPR”) applies, the relevant clauses annexed to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Information to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“SCC Decision”); (ii) where the version of GDPR retained by the United Kingdom (“UK”) by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) and the UK

Data Protection Act 2018 (“UK GDPR”) applies, the International Data Transfer Agreement adopted under section 119A(1) of the Data Protection Act 2018 on 21 March 2022 or the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses adopted under section 119A(1) of the Data Protection Act 2018 on 21 March 2022; (iii) where the Federal Data Protection Act of 19 June 1992 (Switzerland) (“Swiss FDPA”) applies, the relevant clauses annexed to the SCC Decision, as amended by the Swiss Federal Data Protection and Information Commissioner (“FDPIC”) to cover transfers of Personal Information from Switzerland; (iv) where the Brazilian Lei Geral de Proteção de Dados (LGPD) applies, the relevant clauses set out in Annex II of the Brazilian Regulation on International Transfer of Personal Data of the Brazilian National Data Protection Authority; (v) where the Saudi Personal Data Protection Law (PDPL) applies, the relevant clauses set out in the Standard Contractual Clauses for Personal Data Transfer issued by the Saudi Data and Artificial Intelligence Authority; and (v) where the Turkish Kişisel Verileri Koruma Kanunu (KVKK) applies, the relevant clauses set out in the Standard Contract For The Transfer Of Personal Data Abroad issued by the Turkish Personal Data Protection Authority.

- (t) “**Subprocessor**” means any Person (including any third party and any Affiliate of a Party but excluding an employee of such Party) appointed by or on behalf of a Party that Processes Personal Information and includes equivalent terms under Applicable Privacy Laws.

## Part I

### General Obligations

The following obligations shall apply whether Supplier is acting as a Controller or a Processor of Personal Information.

#### Section 1: Description of the Parties’ Personal Information Processing Activities

- (a) Attachment A to this SPS sets out a description of the Processing of Personal Information, including the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Information Processed, and the categories of Data Subjects subject to such Processing. The Parties may make administrative amendments to Attachment A as necessary to reflect current Processing obligations of the Parties by sending an updated Attachment A to the other Party, or the other Party may request an amendment to Attachment A, in each case, solely to reflect those certain processing obligations and not to revise the scope of Services or make other material changes.

#### Section 2: Confidentiality of Personal Information

- (a) A Party’s obligations under this SPS are in addition to the requirements of the Agreement.
- (b) Personal Information is considered confidential and each Party agrees to maintain all Personal Information Processed for the performance of the Agreement in strict confidence pursuant to the Agreement terms. Each Party shall make the Personal Information available only to its employees, contractors, and Subprocessors who have a need to access the Personal Information in order to perform the Services or otherwise comply with its obligations under the Agreement and only to such employees, contractors, and Subprocessors that are subject to binding obligations to keep the Personal Information confidential.

#### Section 3: Compliance with Applicable Privacy Laws

- (a) Each Party must stay informed of the legal and regulatory requirements for its Processing of Personal Information. In addition to being limited to satisfaction of the Services, each Party’s Processing shall comply with all Applicable Privacy Laws.

- (b) Each Party shall promptly assist and cooperate with the other Party to allow the other Party to comply with all Applicable Privacy Laws, including in respect of cooperation with government, regulatory and supervisory authorities, data protection impact assessments, and assessments of the laws and practices of a country that is not deemed to provide an adequate level of data protection by the applicable Governmental Authority (as applicable based on the location from which the data is transferred) required under the SCCs.
- (c) Where required by Applicable Privacy Law, each Party shall appoint a data protection officer, and shall inform, and keep the other Party updated in respect of the name and contact details of its data protection officer.
- (d) To the extent that Supplier receives or otherwise Processes Deidentified Data associated with, derived from, or otherwise related to Personal Information, Supplier will: (i) take reasonable measures to ensure that the Deidentified Data cannot be associated with an individual, household or device; (ii) publicly commit to maintain and use the information in deidentified form and not attempt to reidentify the information; (iii) otherwise comply with applicable requirements for retention and Processing of Deidentified Data under Applicable Privacy Laws; and (iv) contractually obligate any further recipient to comply with all provisions of this Section 3(d) of Part I of this SPS.
- (e) Supplier shall secure all necessary authorizations from its employees and approved Subprocessors to allow Lilly to Process the Personal Information of these individuals, if necessary for Lilly's performance pursuant to the Agreement, including information required to access Lilly systems or facilities, the maintenance of individual performance metrics and similar information.
- (f) Each Party grants the other Party the right to take reasonable and appropriate steps to: (i) help ensure that the Receiving Party (and any Subprocessor) uses Personal Information transferred in a manner consistent with the Disclosing Party's obligations under Applicable Privacy Laws; and (ii) upon notice, stop and remediate any unauthorized use and Processing of Personal Information.

## Section 4: Restricted Transfers

- (a) If, as part of the Agreement, either Party is to receive (directly or indirectly) Personal Information pursuant to a Restricted Transfer Supplier and Lilly agree as follows:
  - (i) By executing the Agreement, they also execute the SCC, which are hereby expressly incorporated by reference and form an integral part of this SPS. The Parties' agree to fill out Attachments A and B to this SPS. For Personal Information of Data Subjects in the Brazil, Turkey, the Kingdom of Saudi Arabia, UK, Switzerland, or another country specified in Attachment A, the Parties adopt the modifications to the SCCs listed in Attachment A to adapt the SCCs to local law, as applicable.
  - (ii) If a Party determines, for whatever reason and acting reasonably, that it cannot provide the same level of protection as is required by the SCCs, it shall give the other Party immediate written notification of such determination and such notifying Party shall promptly remediate such Processing, which may include the application of supplementary organizational or technical measures to the Personal Information, or, if it is unable to do so, cease any and all Processing of such Personal Information until such notifying Party has remediated such Processing;
  - (iii) If Supplier has certified under the Data Privacy Framework, Supplier hereby warrants that: (a) the certification in question covers the Services, and the intended Processing of the Personal Information, by Supplier as set forth in this SPS; (b) Supplier will remain certified under the Data Privacy Framework for as long as Supplier Processes the Personal Information; and
  - (iv) If the Supplier cannot comply with either Section 4(a)(i) or (ii) of Part I of this SPS above for any reason, Supplier agrees to immediately notify Lilly. The Parties shall cooperate to promptly determine and implement appropriate alternative transfer and compliance measures.

- (b) In all cases, each Party shall bear its own costs incurred in relation to establishing and maintaining such transfer and compliance measures. Lilly and Supplier may, by mutual written agreement, terminate or modify data transfer agreements or other compliance measures.
- (c) Access to U.S. Sensitive Personal Information
  - (i) Supplier represents and warrants that it is not a “Covered Person,” as defined in 28 C.F.R. § 202.211.
  - (ii) Supplier shall ensure that none of its employees, Affiliates, contractors, service providers, or Subprocessors with logical or physical access to Personal Information or Sensitive Personal Information of U.S. persons are “Covered Persons.”
  - (iii) Notwithstanding Section 1(g) or 1(i) of Part III of this SPS, Supplier shall not transfer Personal Information or Sensitive Personal Information of U.S. persons to, or permit remote access to such Information from, a “Country of Concern,” as listed in 28 C.F.R. § 202.601.
  - (iv) Supplier shall notify Lilly via email at [privacy@Lilly.com](mailto:privacy@Lilly.com), without undue delay (but no later than 72 hours) upon discovery of any actual or suspected (1) logical or physical access to Personal Information or Sensitive Personal Information of U.S. persons by any “Covered Person”; or (2) transfer of Personal Information or Sensitive Personal Information of U.S. persons to, or remote access to such Information from a “Country of Concern.” In either event, Lilly shall have the right to immediately, upon written notice, terminate the Agreement.

## Section 5: Security

- (a) Each Party shall have documented and implemented appropriate operational, technical and organizational measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access and the Parties will abide by Lilly’s Information Security Standard (ISS) located at <https://www.lilly.com/suppliers/supplier-resources>, which is incorporated as part of the Agreement. These measures shall be commensurate with the sensitivity of the Personal Information. Supplier will regularly test or otherwise monitor the effectiveness and resilience of the safeguards’ controls, systems and procedures. Supplier will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality, availability, and integrity of the Personal Information, and ensure that there are safeguards in place to control those risks (including, pseudonymisation and encryption of data). Subject to Applicable Privacy Laws, Supplier shall monitor its employees and Subprocessors for compliance with its security program requirements.
- (b) Each Party shall maintain all necessary documentation to show compliance with this SPS and with any applicable SCCs, and shall maintain any documentation as may be required by Applicable Privacy Laws in respect of such Party’s Processing of Personal Information under this SPS.

## Section 6: Personal Data Breach

- (a) Supplier will promptly and thoroughly investigate allegations of any Personal Data Breach or any use or disclosure of Personal Information that is in violation of this SPS. Supplier will notify Lilly via email at [privacy@lilly.com](mailto:privacy@lilly.com), without undue delay (but no later than 72 hours) upon discovery of any Personal Data Breach or material violation of this SPS and provide Lilly with sufficient information to allow Lilly to meet any obligations to report or inform Data Subjects of such Personal Data Breach under Applicable Privacy Laws. Additionally, in connection with the foregoing, Supplier take reasonable steps to mitigate any potential damage, conduct a root cause analysis, and upon request, share the results of the analysis and its remediation plan with Lilly. To the extent permitted by Applicable Law, Supplier shall reasonably co-operate with Lilly in resolving and remediating such Personal Data Breach. Except



to the extent that Supplier demonstrates that a Personal Data Breach was solely caused by Lilly, Supplier shall bear all costs associated with resolving a Personal Data Breach or violation of this SPS by Supplier, which may include but are not limited to the need to conduct an investigation, notify Data Subjects and others as required by Applicable Privacy Law or by other applicable regulations, guidelines or standards, provide consumers with one year of credit monitoring, and respond to consumer, regulator and media inquiries. Unless required by Applicable Privacy Laws, Supplier will not inform any third party, Governmental Authority, or make any public statements regarding a Personal Data Breach impacting Lilly Personal Information without the prior written consent of Lilly. Notwithstanding the foregoing sentence, Supplier shall not be restricted from notifying its other customers that may be impacted by the same Personal Data Breach or from consulting its own suppliers in the event of a breach (i.e. counsel, forensic investigators, insurance), provided Supplier does not disclose or make reference to Lilly, its Affiliates, its Data Subjects, or any of Lilly's Personal Information in such notice.

## **Section 7: Severance**

- (a) Should any provision of this SPS be invalid or unenforceable, then the remainder of this SPS will remain valid and in force. The invalid or unenforceable provision will be either (i) amended as to the slightest degree necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

## **Part II**

### **Supplier's Obligations as Independent Controller**

#### **Section 1: General Controller Obligations**

- (a) To the extent each Party Processes the Personal Information as a separate Controller, in addition to Supplier's other obligations under the Agreement, including those set forth in Part I above, Supplier will comply with its obligations under this Part II.
- (b) Supplier and any third party acting for or on its behalf will comply with all Applicable Privacy Laws, with respect to the receipt, collection, compilation, use, storage, processing, sharing, safeguarding, security (technical, physical and administrative), disposal, destruction, disclosure, or transfer (including cross-border) of Personal Information, including providing any notice, obtaining any Consent or prior authorization, and conducting any assessment required under Applicable Privacy Laws.
- (c) Supplier will not "share" or "sell" (as those terms are defined under Applicable Privacy Laws), or otherwise use or disclose for the purposes of cross-context behavioral advertising, any Personal Information.

#### **Section 2: Consent and Authorization**

- (a) Supplier shall comply with the general principles of protection of Personal Information, inform data subjects of the processing carried out concerning their data, establish the necessary measures to ensure security and confidentiality of data, and respect the rights of individuals, such as, their rights of access and rectification. Without limiting the generality of the foregoing, Supplier agrees to: (a) obtain and store all authorizations or lawful bases necessary to process and share Personal Information (identified and de-identified derivatives of such Personal Information), (b) timely enter into legally required agreements with third parties regarding the processing of Personal Information, and (c) provide end-users with a mechanism to withdraw their consent for or otherwise object to/opt-out of processing for Personal Information that it controls or possesses.

## Part III

### Supplier's Obligations as Processor

#### Section 1: General Processor Obligations

- (a) To the extent Supplier Processes the Personal Information as a Processor on behalf of Lilly, in addition to Supplier's other obligations under the Agreement, including those set forth in Part I above, Supplier will comply with its obligations under this Part III.
- (b) Supplier will not Process, retain, disclose or otherwise use any Personal Information for any purpose other than performing the Services for Lilly and in accordance with this SPS and the documented instructions from Lilly, including with regard to transfers of Personal Information to a third country or an international organization, unless approved by Lilly in advance or unless required to do so by Applicable Privacy Law to which Supplier is subject; in such a case, Supplier shall inform Lilly of that legal requirement before Processing, unless that law prohibits disclosing such information on important grounds of public interest. Except as otherwise expressly set forth in the Agreement, Supplier shall not disclose, transmit, or make available the Personal Information to third parties (including Subprocessor), unless explicitly authorized by Lilly. In the event Supplier believes that it cannot satisfy its other obligations under the Agreement while complying fully with the requirements of this SPS, or upon determination Supplier will be unable to comply with the terms of this SPS, Supplier shall notify Lilly without undue delay pursuant to the notice provision in the Agreement and shall not proceed with any act that would violate this SPS until the conflict and/or inability to comply is resolved. Supplier will not:
  - (i) retain Personal Information upon the expiration or termination of the Agreement, except as expressly permitted under the Agreement;
  - (ii) Process Personal Information outside of the direct business relationship between Lilly and Supplier or for Supplier's own commercial purposes;
  - (iii) "share" or "sell" (as those terms are defined under Applicable Privacy Laws), or otherwise use or disclose for the purposes of cross-context behavioral advertising, any Personal Information; or
  - (iv) combine Personal Information that Supplier receives from or on behalf of Lilly with personal information that it receives from or on behalf of another person or collects from its own interaction with an individual, unless expressly permitted by Applicable Privacy Laws.
- (c) Supplier shall without undue delay (but no later than 72 hours) inform Lilly, to the extent not prohibited by Applicable Law, of any Privacy Communication, in writing via email at [privacy@lilly.com](mailto:privacy@lilly.com), including any:
  - (i) request from a Data Subject exercising their rights under Applicable Privacy Law, including but not limited to, any request for access to any Personal Information received by Supplier from an individual who is (or claims to be) a Data Subject, or a request from such Data Subject to cease Processing, or to rectify, block, restrict, erase or destroy any such Personal Information;
  - (ii) request for access to any Personal Information received by Supplier from any government official (including any data protection agency or law enforcement agency), or a request from such government official to cease or not begin Processing, or to rectify, block, erase or destroy any such Personal Information; or
  - (iii) inquiry, claim or complaint regarding the Processing of the Personal Information received by Supplier.
- (d) Supplier is not authorized to respond to a Privacy Communication, unless explicitly authorized by the

Agreement or by Lilly in writing, except for a request received from a Governmental Authority or any third party with a subpoena or similar legal document, made under Applicable Privacy Laws, compelling disclosure by Supplier. In the event that Lilly receives a Privacy Communication, upon Lilly's request, Supplier shall promptly provide Lilly with all information reasonably available to Supplier and assistance as Lilly may reasonably request and comply with Lilly's reasonable instructions in respect of such Privacy Communication.

- (e) Supplier shall limit the extent of Processing to that which is necessary to fulfill the intended Services or business purpose as set out in the Agreement. Supplier shall only store the data for the amount of time necessary to fulfill the intended Services or business purpose or to fulfill a legal requirement. Each Party shall take reasonable steps to assure the integrity and currency of the Personal Information in accordance with the Services to be performed pursuant to the Agreement.
- (f) If the Services involve the Supplier's collection of Personal Information directly from Data Subjects, such as through a registration process or a webpage, Supplier will provide Data Subjects with a clear and conspicuous, concise, transparent, intelligible, and easily accessible notice regarding the uses of the Personal Information, which notice shall be consistent with the provisions of the Agreement, this SPS, and Applicable Privacy Laws, and direction from Lilly. Additionally, if the Supplier's collection of Personal Information directly from Data Subjects includes the collection of Sensitive Personal Information, Supplier will obtain Consent from Data Subjects where required by and consistent with Applicable Privacy Law. However, no terms of use, privacy statement or other provisions presented to Data Subjects via a webpage or in any other manner shall alter the Supplier's obligations or rights under this SPS (including Supplier's role as a Processor) or the manner in which the Supplier may use Personal Information.
- (g) Supplier shall not transfer the Personal Information across any national borders to, or permit remote access to the Personal Information by any employee, Affiliate, contractor, service provider, Subprocessor, or other third party unless such transfer or remote access is specifically permitted in Processing instructions provided to it by Lilly or it has the prior written consent of Lilly for such transfer or access. For clarification, Supplier shall be permitted to transfer Personal Information to or permit access by any approved Subprocessor location for the purposes as further detailed in Attachment A. Supplier may not transfer or permit access across a national border for any other purpose, without Lilly's prior written consent for such transfer or access. Supplier shall provide Lilly with all information reasonably requested by Lilly to allow Lilly to assess whether the laws and practices of the country to which it will transfer Personal Information and which are applicable to the Processing of the Personal Information by Supplier, including any requirements to disclose Personal Information or measures authorising access by public authorities, prevent Supplier from fulfilling its obligations under this SPS or any applicable compliance mechanism. Supplier agrees to execute and undertake such compliance mechanisms as may be required by Applicable Privacy Laws in order for Supplier to transfer Personal Information to such countries or permit remote access in such countries.
- (h) If Supplier receives legal process requiring disclosure of Personal Information that was the subject of a Restricted Transfer to a public authority in a third country that does not benefit from an adequacy decision, Supplier shall promptly, and as applicable: (i) inform the relevant public authority of the incompatibility of the legal process with the safeguards provided under this SPS, and the resulting conflict of obligations for Supplier; (ii) promptly notify Lilly of the legal process and provide a copy, unless legally prohibited from doing so; (iii) assess the lawfulness of the legal process; (iv) respond to the legal process by using reasonable efforts to challenge the validity of the legal process where there are grounds to do so; (v) seek interim measures to suspend the effects of the legal process until the relevant court or authority has decided on the merits; (vi) refrain from disclosing the Personal Information until required to do so under the applicable procedural rules; and (vii) provide the minimum amount of Personal Information permissible when responding to the legal process, based on a reasonable interpretation thereof.



- (i) Lilly generally authorizes Supplier to engage Subprocessors, including those listed in Attachment A, to Process Personal Information, provided that Supplier shall inform Lilly at least thirty (30) days in advance of any intended changes concerning the addition or replacement of Subprocessors listed in Attachment A and Lilly will have the right to reasonably object to such change within such thirty (30) day period and/or terminate the Agreement if the Parties cannot align on a Subprocessor. Subprocessors will be permitted to Process Personal Information only to deliver the Services Supplier has retained them to provide under the Agreement as specified in Attachment A and will be prohibited from Processing Personal Information for any other purpose. Prior to giving any Subprocessor access to Personal Information, Supplier shall ensure that such Subprocessor has entered into a written agreement requiring that the Subprocessor abide by terms no less protective than those provided in this SPS. To the extent a Restricted Transfer is involved, Supplier shall ensure the Standard Contractual Clauses are at all relevant times incorporated into the agreement with Subprocessor, or the parties use another method deemed adequate by an applicable Governmental Authority, before the Subprocessor first Processes Personal Information. Supplier shall remain fully liable for the acts and omissions of any Subprocessor to the same extent as if the acts or omissions were performed by Supplier.
- (j) Without prejudice to any of the Supplier's obligations in the Agreement, Supplier shall reasonably cooperate with Lilly in responding to inquiries, claims, complaints and requests regarding the Processing of the Personal Information.
- (k) When the Supplier ceases to perform Services for Lilly, at the choice of Lilly, Supplier shall, within 30 days, return all Personal Information (along with all copies and all media containing the Personal Information) to Lilly or shall securely destroy all Personal Information in accordance with Section 9 of the Information Security Standard and so certify to Lilly. For clarification, Supplier shall be permitted to make and retain one (1) copy as required pursuant to applicable law for use in its legal archives provided that any such Personal Information retained (i) shall remain subject to the obligations of this SPS; and (ii) not be readily accessible to users, in each case, for so long as the Personal Information is retained.

## **Section 2: Audit**

- (a) At Lilly's reasonable request, Supplier shall submit to an audit, which shall be carried out by Lilly (or by an independent inspection company selected by Lilly) at Lilly's expense during Supplier's reasonable business hours. Such audits may occur only once per year, provided however, that Lilly may audit at any time in the event of a security breach or suspected material violation by Supplier of its obligations under this SPS, or in situations where an audit is necessary or desirable to respond to a Governmental Authority inquiry or request. Supplier shall reasonably co-operate with any such audit. In the event that any such audit reveals material gaps or weaknesses in Supplier's security program or any breach of this SPS, without prejudice to Lilly's other rights, Lilly shall be entitled to suspend transmission of Personal Information to Supplier and Supplier's Processing of such Personal Information, until such issues are resolved. Additionally, Supplier shall, at its own cost and expense, promptly implement such changes as are necessary to address any gaps in the Supplier's security program or rectify any breach and prevent recurrence of the same.

## Attachment A to the Supplier Privacy Standard

### **Data Processing Information Form to the Supplier Privacy Standard** (To be completed by Supplier and returned to Lilly)

#### **A. LIST OF PARTIES**

##### **Data exporter(s):**

1)	Name:	[LILLY ENTITY ENTERING AGREEMENT]
	Address:	As provided in the Agreement
	Contact person's name, position, and contact details:	As provided in the Agreement

##### **Data importer(s):**

1)	Name:	[SUPPLIER ENTITY ENTERING THE AGREEMENT]
	Address:	As provided in the Agreement
	Contact person's name, position, and contact details:	As provided in the Agreement

#### **B. DESCRIPTION OF PROCESSING**

Processing Activity	Status of the Parties	Categories of Data Subjects	Categories of Personal Information that may be Processed	Categories of Sensitive Personal Information that may be Processed and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:	Applicable SCC Module
Supplier Processes to provide the Services as described in the Agreement	Lilly is a Controller and Supplier is a Processor	<input type="checkbox"/> Employees <input type="checkbox"/> End-Users <input type="checkbox"/> Healthcare Providers <input type="checkbox"/> Animal Healthcare Providers <input type="checkbox"/> Clinical Trial Subjects <input type="checkbox"/> Clinical Investigators <input type="checkbox"/> Supplier and other Contractor Employees <input type="checkbox"/> Other (please list): <span style="background-color: cyan;">[INSERT]</span>	<input type="checkbox"/> Employee Data <input type="checkbox"/> Consumer Data <input type="checkbox"/> Healthcare Provider Data <input type="checkbox"/> Animal Healthcare Provider Data <input type="checkbox"/> Clinical Trial Subject Data <input type="checkbox"/> Clinical Investigator Data <input type="checkbox"/> Supplier and other Contractor Employee Data		Module 2 for Restricted Transfers from the EEA, UK and Switzerland.

# Supplier Privacy Standard

			<input type="checkbox"/> Other Personal Information Processed (please list): <b>[INSERT]</b>		
The Parties Process Personal Information of their employees (e.g., to administer and provide the Services, manage invoices, manage the Agreement and resolve any disputes relating to it, respond to or raise general queries, comply with their respective regulatory obligations)	Lilly is a Controller and Supplier is a Processor	Employees	Employee Data	None	Module 2 for Restricted Transfers from the EEA, UK and Switzerland  Template 2 (Controller to Processor) for Restricted Transfers from the Kingdom of Saudi Arabia  Module Two for Restricted Transfers from Turkey
Supplier collects or receives Personal Information as a Controller	Lilly is a Controller and Supplier is a Controller	<input type="checkbox"/> Employees <input type="checkbox"/> End-Users <input type="checkbox"/> Healthcare Providers <input type="checkbox"/> Animal Healthcare Providers <input type="checkbox"/> Clinical Trial Subjects <input type="checkbox"/> Clinical Investigators <input type="checkbox"/> Supplier and other Contractor Employees <input type="checkbox"/> Other (please list): <b>[INSERT]</b>	<input type="checkbox"/> Employee Data <input type="checkbox"/> Consumer Data <input type="checkbox"/> Healthcare Provider Data <input type="checkbox"/> Animal Healthcare Provider Data <input type="checkbox"/> Clinical Trial Subject Data <input type="checkbox"/> Clinical Investigator Data <input type="checkbox"/> Supplier and other Contractor Employee Data <input type="checkbox"/> Other Personal Information Processed (please list): <b>[INSERT]</b>		Module 1 for Restricted Transfers from the EEA, UK and Switzerland  Template 1 (Controller to Controller) for Restricted Transfers from the Kingdom of Saudi Arabia

1. For transfers to Supplier Subprocessors, also specify subject matter, nature, and duration of the Processing.

## TO BE COMPLETED BY SUPPLIER

2. Supplier approved Subprocessors.

Company name of Authorized Subprocessors (including any Supplier Affiliate)	Details of the Point of Contact	Details of the Processing (subject matter, nature, and duration of subprocessing)	Service location	Safeguards
<i>[Include full legal name of each Subprocessor]</i>	<i>[Include contact person's name, position and contact details]</i>	<i>[Include details of the processing to be undertaken by the Subprocessors]</i>	<i>[Include the location of where the services will be provided/data is stored]</i>	<i>[If the data recipient is located outside the EEA/UK, specify the additional safeguards that are implemented, e.g., signed SCCs]</i>

3. Duration of the Processing; The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period.

As Controllers, the Parties retain Personal Information for as long as they have a business purpose for it or for the longest time allowable by Applicable Privacy Law.

As Processor, Supplier retains Personal Information for the duration of the Agreement, after which point Supplier will delete the Personal Information unless otherwise required under Applicable Privacy law.

## C. INFORMATION FOR INTERNATIONAL TRANSFERS

1. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers will be made on (select one):

☐ Continuous basis

☒ A one-off basis commencing on **DATE** and terminating on **DATE**.

2. For purpose of the GDPR SCC:

- a. Optional Clause 7 (*Docking clause*) shall apply;
- b. Clause 9(a), Module 2, (*Use of Subprocessors*): Option 2 shall apply in accordance with the Subprocessor Section in the SPS and the "time period" shall be the same as in Section 1(i) of Part III of the SPS;

- c. Optional Clause 11(a) (*Redress*) shall not apply;
  - d. The following shall apply to Clause 13(a) (*Supervision*): The supervisory authority of one of the Member States in which the data subjects whose Personal Information is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Section C.2.e of this Attachment A shall act as competent supervisory authority.
  - e. Clause 17 (*Governing Law*): Option 1 shall apply, and the specified member state shall be the Member State, the Netherlands;
  - f. Clause 18 (*Choice of Forum and Jurisdiction*): shall specify one of the following Member States as agreed by the parties to serve as the choice of forum and jurisdiction: the Netherlands;
  - g. Annexes I and II of the EU Standard Contractual Clauses are completed with references provided in this Attachment A (Data Processing Information Form to the Supplier Privacy Standard) and Attachment B (Technical and Organizational Measures) of the SPS.
3. With respect to any Restricted Transfer subject to the UK GDPR, the SCCs (as incorporated by reference) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK International Data Transfer Agreement (“UK IDTA”), and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set out below:
- a. Table 1 - the Parties are Supplier and Lilly, with contact details as set forth above in this Attachment A.
  - b. Table 2 - the Approved EU Standard Contractual Clauses with optional provisions as set forth in this Attachment A.
  - c. Table 3 - the Annexes are deemed completed with the relevant information contained in Attachments A and B to the SPS.
  - d. Table 4 - neither Party has the right of termination set forth in Section 19 of the UK IDTA.
4. The Parties agree that, with respect to Personal Information subject to the Swiss FDPA, the SCCs will apply amended and adapted as follows:
- a. the Swiss Federal Data Protection and Information Commissioner is the exclusive supervisory authority;
  - b. the term “member state” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18; and
  - c. references to the GDPR in the EU SCCs shall also include the reference to the equivalent provisions of the Swiss Federal Act on Data Protection (as amended or replaced).
5. Restricted Transfers from Brazil. Without prejudice to the above, if as part of the Agreement, Supplier is acting as a Processor and is to receive (directly or indirectly) Personal Information pursuant to a Restricted Transfer (which may include, without limitation, Personal Information that Lilly transfers from Brazil to a country that is not deemed to provide an adequate level of data protection by the Brazilian National Data Protection Authority,) Supplier and Lilly agree as follows:
- a. Clause 1 (Identification of the Parties) of the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - b. Clause 2 (Object) of the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - c. Clause 3 (Onward Transfers) of the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - d. Clause 4 (Responsibilities of the Parties) of the SCCs: option A shall apply, and the exporter shall be responsible for complying with the obligations set out in Section 4 of Part I of the SPS;



- e. Section III (Security Measures) of the SCCs shall be deemed completed with the information set out in Attachment B of this SPS.
6. Restricted Transfers from the Kingdom of Saudi Arabia. Without prejudice to the above, if as part of the Agreement, Supplier is to receive (directly or indirectly) Personal Information pursuant to a Restricted Transfer (which may include, without limitation, Personal Information that Lilly transfers from the Kingdom of Saudi Arabia to a country that is not deemed to provide an adequate level of data protection by the Saudi Data and Artificial Intelligence Authority,) Supplier and Lilly agree as follows:
- a. Appendix 1 to the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - b. Appendix 2 to the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - c. Appendix 3 to the SCCs shall be deemed completed with the information set out in Attachment B of this SPS.
7. Restricted Transfers from Turkey. Without prejudice to the above, if as part of the Agreement, Supplier is acting as a Processor and is to receive (directly or indirectly) Personal Information pursuant to a Restricted Transfer (which may include, without limitation, Personal Information that Lilly transfers from Turkey to a country that is not deemed to provide an adequate level of data protection by the Turkish Personal Data Protection Authority,) Supplier and Lilly agree as follows:
- a. Module Two (Controller to Processor) shall apply;
  - b. Clause 8 (*Sub-Processors*) Option 2 will apply in accordance with the Subprocessor Section in this SPS and the “time period” shall be the same as in Section 1(i) of Part III of the SPS;
  - c. Clause 10 (*Redress*) the optional language will not apply;
  - d. Clause 16 (*Notification of Contract to Authority*), [data exporter / data importer], agrees to satisfy the obligation to notify the Turkish Personal Data Protection Authority;
  - e. Annex I of the SCCs shall be deemed completed with the information set out in Attachment A of this SPS;
  - f. Legal basis for the transfer field of Annex I of the SCCs shall be: [“Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract”, or such other legal basis as permitted by the Turkish KVKK];
  - g. Annex II of the SCCs shall be deemed completed with the information set out in Attachment B of this SPS.
  - h. Annex III of the SCCs shall be deemed completed with the information set out in Attachment A of this SPS.

## **Attachment B to the Supplier Privacy Standard Technical and Organizational Measures**

The dated version of the Lilly Information Security Standard as published on <https://www.lilly.com/suppliers/supplier-resources> that was in effect as of the date of the Agreement or subsequent amendments, shall prevail, along with any additional Processor measures noted below.