# Supplier Privacy Standard

## 1. Purpose

This Supplier Privacy Standard (or “Standard") sets forth confidentiality and privacy requirements with respect to Personal Information Processed by Supplier on behalf of Lilly to ensure that the Processing by Supplier is compliant with applicable privacy and data protection laws globally and the requirements of Eli Lilly’s Global Privacy Program.

## 2. Definitions.

For the purposes of this Standard:

(a) “Agreement” means the entire agreement between the Supplier and Lilly under which the Supplier performs services including the Processing of Personal Information on behalf of Lilly.

(b) “Applicable Laws” means any statute, law, treaty, rule, code, ordinance, regulation, permit, interpretation, certificate, judgment, decree, injunction, writ, order, subpoena, or like action of a governmental authority that applies, as the context requires to: (i) the Agreement and this Standard; (ii) the performance of obligations or other activities related to the Agreement; and (iii) a party, a party's Affiliates (if any), a party's subcontractors (if any), or to any of their representatives. Applicable Laws, includes A) the Health Insurance Portability and Accountability Act of 1996, B) The Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Privacy and Security Rule regulations of HIPAA and the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act (the “Omnibus Final Rule”) and all amendments to and further regulations of the HIPAA and HITECH Acts (collectively, “HIPAA”), C) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and any implementing, derivative or related national legislation, rule, or regulation enacted thereunder by any EU Member State subject to its jurisdiction.

(c) “Consent” means any freely given, specific and informed indication of the individual's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the Processing of his/her Personal Information.

(d) “Data Transfer Program” means EU-US Privacy Shield, Swiss-US Privacy Shield, or any other framework for lawfully transferring Personal Information from the European Economic Area (“EEA”) or Switzerland to the U.S.

(e) “EU-US Privacy Shield” means the EU-US framework of privacy principles agreed on February 2, 2016 and formally adopted by the European Commission implementing decision C(2016) 4176 final of July 12, 2016.

# Supplier Privacy Standard

(f) "Personal Information" means any information provided by Lilly and/or its Affiliates or collected by Supplier for Lilly and/or its Affiliates relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files. Personal Information includes: (i) a first or last name or initials; (ii) a home or other physical address, including street name and name of city or town; (iii) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (iv) a telephone number; (v) a social security number, tax ID number, identification number, individual number or other government-issued identifier (such as a driver's license); (vi) an Internet Protocol ("IP") address or host name that identifies an individual; (vii) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (viii) birth dates or treatment dates; or (ix) coded data that is derived from Personal Information. Additionally, to the extent any other information (such as, but not necessarily limited to, case report form information, clinical trial identification codes, personal profile information, other unique identifier, or biometric information) is associated or combined with Personal Information, then such information also will 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.

(g) "Processing of Personal Information" (or "Processing") means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as 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.

(h) "Personal Data Breach" means:

(i) A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed; and

(ii) Any substantially similar term to the above as defined by Applicable Law.

(i) "Sensitive Personal Information" is a subset of Personal Information, which due to its nature has been classified by law or by Lilly policy as deserving additional privacy and security protections. Sensitive Personal Information consists of:

(i) All government-issued identification numbers (including US Social Security numbers, EU Social Security numbers, Canadian Social Insurance numbers, Japanese My Number Social Security/Tax numbers, driver's license numbers, and passport numbers);

(ii) All financial account numbers (bank account numbers, credit card numbers, and other information if that information would permit access to a financial account);
(iii) Individual medical records and biometric information, including any information on any worker or consumer's health, disability, disease or product interests, as well as all data relating to an individual person's health;
(iv) medical, health or genetic information derived from biological samples, such as tissue, blood, urine or other samples, which can directly or indirectly be attributed to an identified or identifiable individual;
(v) Reports of individual background checks and all other data obtained from a U.S. consumer reporting agency and subject to the Fair Credit Reporting Act;
(vi) Data elements revealing race, ethnicity, national origin, religion, philosophical beliefs, trade union membership, political orientation, sex life or sexual orientation, criminal records, histories of prosecutions or convictions, or allegations of crimes; and
(vii) Any other Personal Information designated by Lilly as Sensitive Personal Information (for example (but not limited to), "special care-required personal information" as defined and stipulated in Japan's Personal Information Protection Act shall be included as part of Sensitive Personal Information).

(j) "Services" means the particular services that Supplier performs for Lilly under this Agreement.

(k) "Swiss-US Privacy Shield" means the Swiss-US framework of privacy principles approved by the Swiss Federal Council on January 11, 2017, as providing for adequate protection for personal data transferred from Switzerland to the U.S.

## 3. General Obligations.

(a) All Supplier's obligations under the Agreement are in addition to the requirements of this Standard, including those that are similar in nature. Supplier will not Process or otherwise use any Personal Information for any purpose other than performing the Services for Lilly and in accordance with the documented instructions of Lilly; including with regard to transfers of Personal Information to a third country or an international organization, unless required to do so by Applicable Law to which Supplier is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. In the event Supplier believes that it cannot satisfy its other obligations under the Agreement while complying fully with the requirements of this Standard, Supplier shall notify Lilly immediately and shall not proceed with any act that would violate this Standard until the conflict is resolved.

(b) At appropriate intervals or as otherwise requested by Lilly, Supplier will provide a copy of its written privacy policies and procedures to Lilly.

(c) Supplier shall immediately (no later than 24 hours) inform Lilly, in writing:

(i) of any request for access to any Personal Information received by Supplier from an individual who is (or claims to be) the a Data Subject, or a request from such Data Subject to cease or not begin Processing, or to rectify, block, restrict, erase or destroy any such Personal Information;

(ii) of any request to receive Personal Information in a structured, commonly used and machine readable format and/or transmit the data to another controller received by Supplier from an individual who is the subject of the data;

(iii) of any other request by a Data Subject exercising their rights under Applicable Law;

(iv) of any 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;

(v) of any inquiry, claim or complaint regarding the Processing of the Personal Information received by Supplier;

(vi) of any other requests with respect to Personal Information received from Lilly's employees or other third parties, other than those set forth in the Agreement or a request to cease or not begin Processing, or to rectify, block, erase or destroy any such Personal Information, (each a "Privacy Communication").

Upon receipt of a Privacy Communication from an individual claiming to be a Data Subject, Supplier shall use reasonable endeavors to confirm if the individual is the Data Subject. Supplier understands that it is not authorized to respond to a Privacy Communication, unless explicitly authorized by the Agreement or by Lilly in writing, except for the request received from a governmental agency or any third party with a subpoena or similar legal document, made under Applicable Laws, compelling disclosure by Supplier. To the maximum extent permitted by Applicable Laws, Supplier shall, at its own cost and expense, promptly disclose such Privacy Communication to Lilly, provide Lilly with all assistance it may reasonably request, and comply with the directions of Lilly in responding to Privacy Communication. In the event that Lilly receives a Privacy Communication, upon Lilly's request, Supplier shall promptly provide Lilly with all information and assistance as Lilly may reasonably request and comply with Lilly's reasonable directions in respect of such Privacy Communication.

(d) Supplier will promptly and thoroughly investigate allegations of any Personal Data Breach or use or disclosure of Personal Information of which Supplier is aware that is in violation of this Standard. Supplier will notify Lilly, at privacy@lilly.com, immediately (no later than 24 hours) upon discovery of any suspected Personal Data Breach or material violation of this Standard. Additionally in connection with the foregoing, Supplier will reasonably assist Lilly in mitigating any potential damage, conduct a root cause analysis, and upon request, will share the results of the analysis and its remediation plan with Lilly. Supplier shall bear all costs associated with resolving a Personal Data Breach or violation of this Standard, including conducting an

 

investigation, notifying consumers and others as required by law or the Payment Card Industry Data Security Standard, providing consumers with one year of credit monitoring, and responding to consumer, regulator and media inquiries.

(e) Any Personal Information collected or accessed by Supplier in the performance of the Services contracted shall be limited to that which is necessary to perform such Services or to fulfill any legal requirements. Supplier shall limit the extent of Processing to that which is necessary to fulfill the intended purpose as set out in the Agreement and/or Work Order. Supplier shall only store the data for the amount of time necessary to fulfill the intended purpose. Supplier shall take reasonable steps to assure the integrity and currency of the Personal Information in accordance with document management provisions in the Agreement.

(f) If the Services involve the collection of Personal Information directly from individuals, such as through a registration process or a webpage, Supplier will provide individuals 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. For the collection of Sensitive Personal Information, Supplier will obtain Consent from individuals where required by Applicable Law. However, no terms of use, privacy statement or other provisions presented to individuals via a webpage or in any other manner shall alter the Supplier's obligations or rights under this Standard 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 or other third party unless such transfer or remote access is specifically permitted in the Processing instructions provided to it by Lilly or it has the prior written consent of Lilly for such transfer or access. Supplier agrees to execute and undertake such compliance mechanisms as may be required by Applicable Laws that apply to Lilly or its Affiliates (including data protection laws in any of the members of the EEA and Switzerland) in order for Supplier to receive Personal Information from or send Personal Information to such countries.

Without prejudice to the above, before Supplier receives Personal Information directly from a member state of the EEA or Switzerland in a country that is not deemed to provide an adequate level of data protection by the EU Commission, Supplier must:

(i) Promptly cooperate with Lilly or its Affiliates to duly complete, execute and comply with the Standard Contractual Clauses as provided by the EU Commission (set forth on Lilly's Procurement Portal as "EU Standard Contractual Clauses for Data Transfer") with respect to all transfers of or remote access to Personal Information from the EEA and/or Switzerland to or by Supplier, as the case may be; or

(ii) Notwithstanding the above, in the event that Supplier receives Personal Information from a member state of the EEA or Switzerland in the USA and Supplier is certified under a Data Transfer Program, 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 the Agreement; (b) Supplier will remain certified under such Data Transfer Program during such time as Supplier Processes the Personal Information; and (c) if at any time during such time as Supplier Processes the Personal Information, Supplier de-certifies or otherwise loses the certification in question or for some reason the Data Transfer Program becomes invalid, Supplier will comply with subsection (i) above; or

(iii) If the Supplier cannot comply with either subsection (i) or (ii) above for any reason, the Parties shall cooperate to promptly settle on and execute appropriate alternative compliance measures.

In all cases, each Party shall bear its own costs incurred in relation to such establishing and maintaining such compliance measures. In respect of data transfers from the EEA or Switzerland, Lilly and Supplier may, by mutual written agreement, terminate or modify data transfer agreements or other compliance measures should they become unnecessary following any European Commission positive adequacy decision under Article 45 of the General Data Protection Regulation being issued in relation to the country in question (or relevant sector thereof), or if the General Data Protection Regulation becomes directly applicable in such country, provided that Supplier shall first self-certify or take any other necessary steps as may be necessary to benefit from that adequacy determination.

If Supplier receives Personal Information originating in the EEA or Switzerland from Lilly or its USA Affiliated entities that are certified to a Data Transfer Program, Supplier shall Process such Personal Information in a manner consistent with, and providing the same level of protection as, the Data Transfer Programs. If Supplier determines, for whatever reason and acting reasonably, that it cannot provide the same level of protection as is required by the Data Transfer Programs, it shall give Lilly immediate written notification of such determination and Supplier shall immediately remediate such Processing or, if it is unable to do so, cease any and all Processing of such Personal Information.

(h) Lilly generally authorizes Supplier to engage subcontractors to Process Personal Data provided that Supplier shall inform Lilly of any intended changes concerning the addition or replacement of other subcontractor and Lilly will have the right to object to such change and terminate the Agreement. Any subcontractors will be permitted to Process Personal Data only to deliver the Services Supplier has retained them to provide under this Agreement, and will be prohibited from Processing Personal Data for any other purpose. Prior to giving any Subcontractor access to Personal Data, Supplier shall ensure that such Subcontractor has entered into a written agreement requiring that the subcontractors abide by terms no less protective than those provided in this Agreement. Supplier shall be fully liable for the acts and omissions of any Subcontractor to the same extent as if the acts or omissions were performed by Supplier.

Any breach of the above provisions 3(g) and/or 3(h) by the Supplier shall be considered a material breach of the Agreement by Supplier and shall allow Lilly to immediately terminate the Agreement between the parties, by law, and if Lilly elects to terminate this Agreement, Lilly shall

 

provide notice to Supplier as set forth in the notice section of the Agreement.

(i) Without prejudice to any of the Supplier's obligations in this Agreement, Supplier shall cooperate with Lilly and with Lilly's Affiliates and representatives in responding to inquiries, claims and complaints regarding the Processing of the Personal Information.

(j) Supplier shall secure all necessary authorizations from its employees and approved subcontractors to allow Lilly to Process the Personal Information of these individuals as necessary for the performance of the Agreement by Lilly, including information required to access Lilly systems or facilities, the maintenance of individual performance metrics and similar information.

(k) Notwithstanding anything in this Agreement to the contrary: (a) No action by Lilly expressly permitted by the Standard is a breach of this Agreement by Lilly, and (b) no such action excuses Supplier's performance under this Agreement.

## 4. Confidentiality of Personal Information

(a) Supplier must maintain all Personal Information in strict confidence. Supplier shall make the Personal Information available only to its employees and onsite contractors who have a need to access the Personal Information in order to perform the Services and are subject to binding obligations to keep the Personal Information confidential. Supplier shall not disclose, transmit, or make available the Personal Information to third parties (including subcontractors), unless such disclosure, transmission, or making available has been explicitly authorized by Lilly in writing. In no event may Supplier provide Personal Information (or any other Lilly information) to a subcontractor or sub-processor unless that entity has agreed in writing to terms no less protective than those contained herein, including the provisions regarding security and Lilly audit rights.

(b) When the Supplier ceases to perform Services for Lilly, at the choice of Lilly, Supplier shall return all Personal Information (along with all copies and all media containing the Personal Information) to Lilly or shall securely destroy all Personal Information and so certify to Lilly.

## 5. Security

(a) Supplier 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. 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 Laws, Supplier shall monitor its employees and contractors for compliance with its security program requirements.

(b) Supplier shall maintain all necessary documentation to show compliance with this Agreement and as may be required by Applicable Laws in respect of Supplier's Processing of Personal Data under this Agreement. At Lilly's request, Supplier shall submit its data Processing facilities for audit, which shall be carried out by Lilly (or by an independent inspection company designated by Lilly). Supplier shall fully co-operate with any such audit at Supplier's cost and expense. In the event that any such audit reveals material gaps or weaknesses in Supplier's security program or any breach of this Agreement, 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.

## 6. Compliance with Laws.

(a) Supplier 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, Supplier's Processing shall comply with all Applicable Laws.

(b) Supplier shall promptly assist and cooperate with Lilly to allow Customer to comply with all Applicable Laws, including in respect of cooperation with government, regulatory and supervisory authorities, and data protection impact assessments.

(c) Where required by Applicable Law, Supplier shall appoint a data protection officer, and shall inform, and keep Lilly updated in respect of, the name and contact details of its data protection officer.

## 7. EEA/Switzerland-Specific Terms.

(a) Unless otherwise notified, if Supplier is Processing Personal Information transferred to it (directly or indirectly) from the EEA or Switzerland on the basis of the Standard Contractual Clauses under provision 3(e)(i), Supplier must comply with the obligations imposed on a 'data importer' (or, as applicable, a 'subprocessor') under the Standard Contractual Clauses as provided by the EU Commission (set forth on Lilly's Procurement Portal as "EU Standard Contractual Clauses for Data Transfer") modified as necessary in respect of such Personal Information. Supplier hereby grants any applicable third party beneficiary rights referred to in the Standard Contractual Clauses.

(b) Where a Data Subject, or entity acting on his/her behalf, is entitled to bring a claim against Lilly or its Affiliate(s) for breach of the Standard Contractual Clauses, and such claim arises from Supplier's Processing operations under this Agreement and Standard, Supplier shall indemnify Lilly or its Affiliate(s) for all liabilities, costs, expenses, damages and losses (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest,

 

penalties and legal costs, calculated on a full indemnity basis, and all other reasonable professional costs and expenses) suffered or incurred by Lilly or its Affiliate(s) arising out of or in connection with such claim, provided that:

i. As soon as reasonably practicable, Supplier is given notice of such claim; and
ii. Lilly or its Affiliate(s) (as the case may be) shall not make any admission of liability, agreement or compromise in relation to such claim without the prior written consent of Supplier (such consent not to be unreasonably conditioned, withheld or delayed), provided that Lilly or such Affiliate(s) may settle such claim (after giving prior written notice of the terms of settlement (to the extent legally possible) to Supplier, but without obtaining Supplier's consent) if Lilly or such Affiliate(s) believes that failure to settle such claim would be prejudicial to Lilly or its Affiliate(s) in any material respect.

(c) Promptly upon request from Lilly or its Affiliates, Supplier shall return to Lilly or a requesting Affiliate (if any) a completed Data Processing Information Form using the template set out in Exhibit A.

# Supplier Privacy Standard

EXHIBIT A
Supplier Privacy Standard Data Processing Information Form
(to be completed by Supplier and returned to Lilly upon request from Lilly or its Affiliates)

Supplier represents that the following is accurate to the best of their knowledge:

1. **Supplier's Registered Name and Address:**

2. **Describe the nature and purpose of the data Processing to be undertaken by Supplier as set forth in the description of Services:**

3. **Select the categories of data related to Data Subjects that will be Processed by Supplier as part of the Services:**

- ☐ Employee Data
- ☐ Consumer Data
- ☐ Healthcare Provider Data
- ☐ Animal Healthcare Provider Data
- ☐ Clinical Trial Subject Data
- ☐ Clinical Investigator Data
- ☐ Supplier and other Contractor Employee Data
- ☐ Other Personal Information Processed (please list):

4. **Select the categories of Lilly data that will be Processed by Supplier as part of the Services:**

- ☐ The following data of customers and business partners as well as contact persons at customers and business partners: name, company, location, address(es), contact person, communication data, preferred/excluded communication channels, desired information/ordered newsletters, dispatch, freight, and payment conditions, account advisers, activities, participation in events, campaigns, customer satisfaction, customer-value-score and data of prospective customers.

- ☐ The following data of health care professionals, including thought leaders: name, institution, location, address(es), contact persons, communication data, CV-data, such as education, areas of expertise, skills and experience, cooperation during clinical trials or observational studies, potential conflicts of interests, participation in events, payment conditions.

# Supplier Privacy Standard

- ☐ The following data of visitors of websites: IP Address, date and time of visit of website, web pages visited, website visitor came from, type of browser visitor is using, type of operating system visitor is using, domain name and address of visitor's internet service provider, and, as the case may be, data manually entered by the visitor.

- ☐ The following data of employees of Lilly (staff, freelancers, managing directors, and members of the executive board): in particular personnel master data, e.g. data derived from CVs, salary accounting data, data in relation to trainings and performance management, data in relation to company pension schemes, vacation times, absent times, travel expenses, data in relation to driver's licenses, accidents at work, system log data, as well as all data potentially collected in the personnel records.

- ☐ The following data of patients: patient master data, including data in relation to state of health, medication, information in relation to patient support programs, information in relation to the notification of adverse events and product complaints, etc.

- ☐ Business communication with contact persons, in particular: traffic data of e-mail, facsimile, telephone and content of emails, facsimile, and postal communication.

- ☐ Data and results deriving from surveys and other market research activities; accounts and sub-accounts (e.g. contact data, contact person/s, activities, dispatch, freight, and payment conditions), person in charge at Processor.

- ☐ Contract master data, offers, prices, special conditions, order and delivery data, invoice data, payment data, bank account data, data in relation to outstanding payments, and in each case the history relating thereto.

- ☐ Business documents and text as well as the related history with respect to individual business partners, customers, potential customers and business partners, contacts, accounts or other data records that are stored in the system.

- ☐ Data accrued within the scope of use of services that are provided by Lilly (e.g. personnel identification derived from input and usage trails).

5. **Supplier will Process the Personal Information in the following geographies (list countries where Processing operations will occur):**