SCHEDULE

DATA PROTECTION TERMS – BASIC PERSONAL INFORMATION

Covered Affiliate means: each Affiliate of GSK which has the benefit of the Services as a third party (a list of which will be provided by GSK to Supplier on request). An Affiliate is any entity that, with respect to any other entity, is Controlled by, under common Control, or Controls, such other entity. "Control" and its derivatives means the ownership (directly or indirectly) of a majority of the voting shares of such entity or is the ability (directly or indirectly) to appoint a majority of the directors of such entity or the authority to direct the management or policies of such entity, by contract or otherwise;

Data Protection Laws means: (a) the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and any applicable laws and/or regulations that implement and/or exercise derogations under it and/or replace or supersede it (**GDPR**); and (b) the GDPR as tailored by the UK Data Protection Act 2018; (c) the California Consumer Privacy Act of 2018 (Cal. Civ. Code 1798.100 – 1798.199) (**CCPA**); and (d) all other laws concerning the processing of personal data;

Personal Information means personal data within the following set: first name and/or last name, initials, work contact details, group memberships, network or user identification number, login credentials, work history and skills, gender or title, event attendance of GSK employees and complementary workers using the Services

GSK Personal Information means any Personal Information: (i) supplied by or on behalf of GSK to Supplier (including where Supplier has access to Personal Information held by GSK or on its behalf), or which Supplier collects or generates on behalf of GSK; (ii) that is processed by Supplier under or in connection with this Agreement as; and (iii) in respect of which GSK is a controller or owner (or equivalent);

Security Schedule means *the cybersecurity schedule attached hereto as Appendix 1*.

The terms **controller, data protection impact assessment, data subject, personal data, personal data breach, processor, processing, service provider** and **supervisory authority** shall be as defined under relevant Data Protection Laws. Any reference to GSK shall mean the GSK contracting entity used in the Agreement, as well as Covered Affiliates.

Processor Terms

In the event supplier is acting as a processor of GSK Personal Information under relevant Data Protection Laws, the following terms shall apply:

1. Each party shall comply with its obligations under applicable Data Protection Laws. GSK and Supplier agree that in relation to the GSK Personal Information processed under this Agreement GSK will be the controller and Supplier will be the processor. For purposes of the CCPA, Supplier is a service provider to GSK and the processing of GSK Personal Information by Supplier shall be undertaken only for GSK's purposes in accordance with this Schedule, that no monetary or other valuable consideration is being provided by Supplier to GSK and therefore GSK is not selling GSK Personal Information to Supplier as defined by the CCPA.

2. Supplier shall comply with the following in respect of GSK Personal Information:

a) process GSK Personal Information only on GSK's lawful written instructions and solely for the purposes of the provision of Services by Supplier to GSK under this Agreement for the term of the Agreement or any additional period stated in the Agreement, if applicable;

b) neither Supplier, nor any of its employees, agents, consultants or assigns shall have any right to process GSK Personal Information for their own commercial benefit in any form;

c) implement and maintain appropriate technical and organizational security measures, including without limitation, the measures set out in the Security Schedule. References in the Security Schedule to "GSK Data" shall include GSK Personal Information;

d) keep GSK Personal Information confidential in accordance with the terms of this Schedule and references in this Schedule and the Security Schedule to GSK Confidential Information shall include GSK Personal Information;

e) impose confidentiality obligations equivalent to the obligations set out under the Agreement on relevant personnel having access to GSK Personal Information;

f) not engage another processor ("**sub-processor"**) without the prior written approval of GSK (and for these purposes GSK consents to the following categories of sub-processor: hosting infrastructure service providers, the use of individual contractors, and sub-processors made known to GSK at the time the Agreement is entered into) and transfer GSK Personal Information to such approved sub-processors only under a written contract which imposes obligations consistent with those set out in this Schedule. When Supplier appoints a sub-processor in line with this clause 2(f) it remains liable for the acts and omissions of the sub-processor;

g) provide GSK reasonable assistance with (i) carrying out any legally required data protection impact assessments and/or data transfer impact assessments ; (ii) complying with the rights of data subjects; and (iii) responding to requests from any supervisory authority in respect of GSK Personal Information;

h) notify GSK without delay after becoming aware of a personal data breach in respect of any GSK Personal Information and provide GSK assistance in relation to such breach;

i) notify GSK without delay if it receives a written request from (i) a data subject to exercise any of their rights in relation to GSK Personal Information under Data Protection Laws; or (ii) a supervisory authority in relation to the processing of GSK Personal Information;

j) unless otherwise set out in Agreement, either return or destroy all GSK Personal Information in its possession or under its control (including any GSK Personal Information processed by permitted sub-processors) on termination or expiry of Agreement; and

k) on GSK's written request, provide GSK with reasonable information necessary to demonstrate compliance with this Schedule, which may include any available third-party security audit reports.

Controller Terms

In the event supplier is acting as a controller of GSK Personal Information under relevant Data Protection Laws, the following terms shall apply:

1. Each party acts as an independent controller and shall comply with its obligations under applicable Data Protection Laws. GSK and Supplier agree that, in relation to the personal data processed under this Schedule, for purposes of the CCPA, that no monetary or other valuable consideration is being provided by Supplier to GSK in exchange for the GSK Personal Information and therefore GSK is not selling GSK Personal Information to Supplier as defined by the CCPA.
2. If Supplier receives any communication from a supervisory authority which relates directly or indirectly to a) Supplier's processing of GSK Personal Information; or (b) a potential failure to comply with Data Protection Laws in relation to the processing of GSK Personal Information, Supplier shall, to the extent permitted by applicable laws, promptly forward the communication to GSK and provide reasonable cooperation and assistance to GSK in relation to the same.
3. If a data subject makes a written request to either party to exercise any of their rights under Data Protection Laws in respect of GSK Personal Information, the receiving party shall respond to that request in accordance with Data Protection Laws. To the extent the request concerns processing of GSK Personal Information undertaken by the other party, the receiving party shall: (i) promptly and without undue delay forward the request to the other party; and (ii) cooperate and provide reasonable assistance in relation to that request to enable the other party to respond in accordance with Data Protection Laws.
4. Without limiting any provision of the Security Schedule, upon becoming aware of a personal data breach affecting GSK Personal Information, Supplier shall (a) promptly notify GSK and provide GSK with a reasonable description of the breach; and (b) not publish any communication concerning the breach without first consulting GSK, save that it may notify a breach to a supervisory authority to the extent required by applicable Data Protection Law.

International Data Transfer

Where GSK, acting as a data exporter, transfers GSK Personal Information to Supplier, acting as data importer, in a manner that constitutes a restricted international data transfer under applicable Data Protection Laws, both parties have hereby entered into and will abide by the applicable Model Clauses covering the relationship between the parties:

- The Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**Annex**") along with MODULE ONE: Transfer controller to controller (available **here**) and incorporated herein by reference as updated, amended, replaced or superseded from time to time by the European Commission; and/or (ii) any corresponding or equivalent international data transfer agreement or addendum to the Model Clauses adopted by the supervisory authority in the United Kingdom ("**C2C Model Clauses**");
- The Annex along with MODULE TWO: Transfer controller to processor (available **here**) and incorporated herein by reference as updated, amended, replaced or superseded from time to time by the European Commission; and/or (ii) any corresponding or equivalent international data transfer agreement or addendum to the Model Clauses adopted by the supervisory authority in the United Kingdom ("**C2P Model Clauses**");

"**Model Clauses**" shall mean the Annex together with C2C Model Clauses and C2P Model Clauses.

For the purposes of the Model Clauses the parties agree that:

- The option in square brackets of Clause 11 "Redress" shall not apply
- Option one is selected for Clause 17 "Governing Law" and the law of Ireland shall apply.
- The courts of Ireland will have jurisdiction under Clause 18 "Choice of Forum and Jurisdiction".

For the purposes of the applicable C2P Model Clauses and C2C Model Clauses, please note the following:

- Annex1 (Exporter and Importer): GSK or the relevant GSK service recipients located in the EU and/or the UK under the agreement(s) with Supplier is a Data Exporter in relation to GSK Personal Information. Supplier is a Data Importer in relation to GSK Personal Information
- Annex 1 (Description of the Transfers): please see definition of Personal Information and Services to be provided by Importer. No sensitive data is transferred. The frequency of the transfer is continuous. The nature of processing activities and the purposes of the transfer are set out in the agreement(s) with Supplier. The data will be retained in line with the Data Exporter's data retention policies.
- Annex 1 (Competent Authorities): as set out in clause 13 of the C2C Model Clauses and C2P Model Clauses
- Annex 2 (Technical and Organization Measures): please see Security Measures set out below

The parties agree that option 2 of clause 9 "Use of Sub-Processors" of the C-P Model Clauses shall apply where Supplier engages a sub-processor and Supplier and sub-processor shall agree to abide by the **P-P Model Clauses**, which means i) the Annex along with MODULE THREE: Transfer processor to processor (available **here**) and incorporated herein by reference as updated, amended, replaced or superseded from time to time by the European Commission; and/or (ii) any corresponding or equivalent international data transfer agreement or addendum to the Model Clauses adopted by the supervisory authority in the United Kingdom;

In the event Supplier does not believe it can meet the requirements as reasonably set forth by GSK, Supplier shall notify GSK immediately of its inability and GSK shall have the right to terminate Agreement.

Parties agree that Model Clauses entered into shall have effect in countries outside of the European Economic Area where: (i) their provisions are recognized as an appropriate safeguard in relation to international transfers of Personal Data to non-adequate countries or (ii) the Data Protection Laws require the existence of contractual provisions to protect international transfers of Personal Information. In interpreting the Model Clauses, in those countries, any reference to the term "Member State in which the data exporter is established" will be interpreted to mean the country in which the GSK entity is established; and any reference to Regulation (EU) 2016/679shall be to the law of the country where GSK is established outside the EEA. Any reference to an "Adequate Country" shall mean any country which is held to provide, or which otherwise provides, an equivalent level of protection for the purposes of the applicable Data Protection Laws, in those countries outside of the European Economic Area where the Model Clauses shall cover the transfers of Personal Data.

Security Measures

"GSK Data" means any data or information that is provided by or on behalf of GSK or obtained by Supplier or Supplier Personnel in connection with the negotiation and execution of the Agreement or the performance of Supplier's obligations under the Agreement, including any such data and information that either: (i) is created, generated, collected or processed by Supplier Personnel in the performance of Supplier's obligations under the Agreement, or (ii) resides in or is accessed through GSK's information systems or Supplier information systems, as well as any data and information derived from the foregoing.

"**Processing**" means any operation or set of operations which is performed on any information or data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Supplier Environment" means the combination of hardware, software, operating systems, database systems, tools and network components used by or on behalf of Supplier to receive, maintain, Process, store, access or transmit GSK Data.

"Supplier Personnel" means any and all personnel engaged or employed by Supplier and its Subcontractors to perform any part of the Services.

This Security Schedule forms a part of the Agreement by and between GSK and Supplier. In the event of any conflict with respect to cyber security between the terms of this Security Schedule and the terms of the Agreement, this Security Schedule shall control. Capitalised terms not defined in this Security Schedule will have the meanings ascribed to them in other parts of the Agreement.

1. Responsibilities. Supplier shall: (a) use strong encryption controls to protect all GSK Data from unauthorized disclosure, access or alteration in transit into or out of the Supplier Environment over third-party networks; (b) maintain control processes in line with industry best practice to detect, prevent, and recover from malware, viruses and spyware, including updating antivirus, anti-malware and anti-spyware software at regular intervals; (c) maintain access management policies, procedures, and technical controls in line with industry best practice to ensure all access to GSK Data in its control is appropriately authorised.

2. Security Breach. Supplier will report to GSK by email to cstd@gsk.com any verified accidental, unauthorized or unlawful use, loss, destruction, disclosure, access, corruption, modification, sale, rental or other Processing of any GSK Data (a "**Security Breach**") within twenty-four (24) hours of Supplier's verification. Supplier will ensure that all security incidents involving GSK Data are managed in accordance with appropriate incident response procedures Supplier shall work with GSK in good faith to identify a root cause and remediate the Security Breach.

الجدول

شروط حماية البيانات - المعلومات الشخصية الأساسية

الشركة التابعة المشمولة يُقصد بها: كل شركة تابعة لشركة GSK تستفيد من الخدمات كطرف ثالث (ستقدم شركة GSK قائمة بهم إلى المورد عند الطلب). والشركة التابعة هي، فيما يتعلق بأي كيان آخر، أي كيان يخضع لسيطرة هذا الكيان الآخر أو يخضع لسيطرة مشتركة معه أو يسيطر عليه. وتعني **"السيطرة"** ومشتقاتها ملكية (بشكل مباشر أو غير مباشر) أغلبية الأسهم التي لها حق التصويت في هذا الكيان أو القدرة (بشكل مباشر أو غير مباشر) على تعيين أغلبية أعضاء مجلس الإدارة في هذا الكيان أو سلطة توجيه الإدارة أو السياسات في هذا الكيان، بموجب عقد أو غير ذلك.

قوانين حماية البيانات تعني: (أ) اللائحة العامة لحماية البيانات (الاتحاد الأوروبي) 2016/679 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والحركة الحرة لهذه البيانات وأي قوانين و/أو لوائح سارية تعمل على تطبيقها و/أو ممارسة الاستثناءات بموجبها و/أو استبدالها أو إبطالها (**اللائحة العامة لحماية البيانات**)؛ و(ب) اللائحة العامة لحماية البيانات بما يتفق مع قانون حماية البيانات في المملكة المتحدة لسنة 2018؛ و(ج) قانون خصوصية المستهلك في كاليفورنيا لسنة 2018 (مدونة القوانين المدنية في كاليفورنيا 1798.199 – 1798.100) (**قانون خصوصية المستهلك في كاليفورنيا**)؛ و(د) جميع القوانين الأخرى المتعلقة بمعالجة البيانات الشخصية.

المعلومات الشخصية يُقصد بها البيانات الشخصية ضمن المجموعة التالية: الاسم الأول و/أو الاسم الأخير، والأحرف الأولى من الاسم، وتفاصيل الاتصال الخاصة بالعمل، وعضويات المجموعة، ورقم تعريف الشبكة أو المستخدم، وبيانات اعتماد تسجيل الدخول، وسجل العمل والمهارات، والجنس أو المُسمّى الوظيفي، وحضور الفعاليات لموظفي شركة GSK والعاملين التكميليين الذين يستخدمون الخدمات.

المعلومات الشخصية لشركة GSK يُقصد بها أي معلومات شخصية: (1) تقدمها شركة GSK أو يتم تقديمها نيابة عنها إلى المورد (بما في ذلك حيثما يتمتع المورد بحق الوصول إلى المعلومات الشخصية التي تحتفظ بها شركة GSK أو يتم الاحتفاظ بها نيابة عنها)، أو التي يجمعها المورد أو يُنشئها نيابة عن شركة GSK؛ و(2) يقوم المورد بمعالجتها بموجب هذه الاتفاقية أو فيما يتعلق بها؛ و(3) تتعلق بشركة GSK بصفتها مراقب أو مالك (أو أي صفة معادلة).

جدول الأمن يعني *جدول الأمن السيبراني المرفق بهذه الوثيقة باعتباره الملحق 1.*

تحمل مصطلحات **المراقب وتقييم أثر حماية البيانات والشخص موضوع البيانات والبيانات الشخصية وخرق البيانات الشخصية والمعالج والمعالجة ومقدم الخدمة** و**السلطة الإشرافية** المعنى الوارد لها في قوانين حماية البيانات ذات الصلة. وتتضمن أي إشارة إلى شركة GSK الكيان المتعاقد التابع لشركة GSK الوارد في الاتفاقية، وكذلك الشركات التابعة المشمولة.

شروط معالج البيانات

في حالة تصرف المورد بصفته معالج للمعلومات الشخصية لشركة GSK بموجب قوانين حماية البيانات ذات الصلة، تنطبق الشروط التالية:

1. يمتثل كل طرف لالتزاماته بموجب قوانين حماية البيانات المعمول بها. توافق شركة GSK والمورد على أنه فيما يتعلق بالمعلومات الشخصية لشركة GSK التي تتم معالجتها بموجب هذه الاتفاقية، ستكون شركة GSK هي مراقب البيانات وسيكون المورد هو المعالج. ولأغراض قانون خصوصية المستهلك في كاليفورنيا، يُعد المورد مقدم خدمة لشركة GSK ولا يعالج المورد المعلومات الشخصية لشركة GSK إلا للأغراض التي حددتها الشركة وفقًا لهذا الجدول، على أساس أن المورد لا يقدم أي مقابل نقدي أو مقابل ذي قيمة آخر إلى شركة GSK وبالتالي لا تبيع شركة GSK معلوماتها الشخصية للمورد على النحو المحدد في قانون خصوصية المستهلك في كاليفورنيا.

2. يمتثل المورد لما يلي فيما يتعلق بالمعلومات الشخصية لشركة GSK:

a) عدم معالجة المعلومات الشخصية لشركة GSK إلا بناءً على تعليمات مكتوبة قانونية من الشركة ولأغراض تقديم الخدمات من قبل المورد إلى الشركة بموجب هذه الاتفاقية أثناء مدة الاتفاقية أو أي فترة إضافية منصوص عليها في الاتفاقية، إن وجدت؛

b) لا يمتلك المورد ولا أي من موظفيه أو وكلائه أو مستشاريه أو المتنازل لهم لديه أي حق في معالجة المعلومات الشخصية لشركة GSK لمصلحته التجارية بأي شكل من الأشكال؛

c) تطبيق والحفاظ على التدابير التقنية والتنظيمية الملائمة فيما يتعلق بالأمن، بما في ذلك على سبيل المثال لا الحصر، التدابير المنصوص عليها في جدول الأمن. وتشمل الإشارات الواردة في جدول الأمن إلى "بيانات شركة GSK" المعلومات الشخصية للشركة؛

d) الحفاظ على سرية المعلومات الشخصية لشركة GSK وفقًا لشروط هذا الجدول وتشمل الإشارات الواردة في هذا الجدول وجدول الأمن إلى المعلومات السرية لشركة GSK المعلومات الشخصية لشركة GSK؛

e) فرض التزامات سرية مكافئة للالتزامات المنصوص عليها في الاتفاقية على الموظفين المعنيين الذين يتمتعون بحق الوصول إلى المعلومات الشخصية لشركة GSK؛

f) عدم إشراك معالج آخر (**"المعالج من الباطن"**) دون الحصول على موافقة كتابية مسبقة من شركة GSK (ولهذه الأغراض توافق شركة GSK على الفئات التالية من المعالجين من الباطن: مقدمو خدمات البنية التحتية المضيفة، والمتعاقدين الفرديين، والمعالجين من الباطن الذين تم إبلاغ شركة GSK بهم في وقت إبرام الاتفاقية) وعدم نقل المعلومات الشخصية لشركة GSK إلا إلى هؤلاء المعالجين من الباطن المعتمدين بموجب عقد مكتوب يفرض التزامات تتفق مع تلك المنصوص عليها في هذا الجدول. وفي حالة تعيين المورد لمعالج من الباطن بما يتماشى مع هذا البند 2(و) فإنه يظل مسؤولاً عن الأفعال والإغفالات التي تقع من هذا المعالج من الباطن؛

g) تقديم المساعدة المعقولة لشركة GSK بشأن (1) إجراء أي تقييمات أثر تتعلق بحماية البيانات و/أو نقل البيانات تكون مطلوبة قانونًا؛ و(2) الامتثال لحقوق الأشخاص موضوع البيانات؛ و(3) الاستجابة للطلبات الواردة من أي سلطة إشرافية فيما يتعلق بالمعلومات الشخصية لشركة GSK؛

h) إخطار شركة GSK دون إبطاء لدى العلم بأي خرق للبيانات الشخصية فيما يتعلق بأي من المعلومات الشخصية لشركة GSK وتقديم المساعدة للشركة فيما يتعلق بهذا الخرق؛

i) إخطار شركة GSK دون إبطاء في حالة تلقي طلب كتابي من (1) شخص موضوع بيانات لممارسة أي من حقوقه فيما يتعلق بالمعلومات الشخصية لشركة GSK بموجب قوانين حماية البيانات؛ أو (2) سلطة إشرافية فيما يتعلق بمعالجة المعلومات الشخصية لشركة GSK؛

j) ما لم يُنص على خلاف ذلك في الاتفاقية، إعادة أو إتلاف جميع المعلومات الشخصية لشركة GSK التي تكون في حوزته أو تخضع لسيطرته (بما في ذلك أي معلومات شخصية لشركة GSK يقوم معالجون من الباطن مسموح بهم بمعالجتها) عند إنهاء الاتفاقية أو انتهاء مدتها؛

k) تزويد شركة GSK، بناءً على طلب كتابي منها، بالمعلومات المعقولة اللازمة لإثبات الامتثال لهذا الجدول، والتي قد تتضمن أي تقارير تدقيق أمني من جانب طرف ثالث.

شروط مراقب البيانات

في حالة تصرف المورد بصفته مراقب للمعلومات الشخصية لشركة GSK بموجب قوانين حماية البيانات ذات الصلة، تنطبق الشروط التالية:

1. يتصرف كل طرف بصفته مراقب بيانات مستقل ويمتثل لالتزاماته بموجب قوانين حماية البيانات المعمول بها. وتوافق شركة GSK والمورد على أنه، فيما يتعلق بالبيانات الشخصية التي تتم معالجتها بموجب هذا الجدول، لأغراض قانون خصوصية المستهلك في كاليفورنيا، لا يقدم المورد أي مقابل نقدي أو مقابل ذي قيمة آخر إلى شركة GSK في مقابل المعلومات الشخصية لشركة GSK، وبالتالي لا تبيع شركة GSK المعلومات الشخصية الخاصة بها للمورد على النحو المحدد في قانون خصوصية المستهلك في كاليفورنيا.

2. إذا تلقى المورد أي مراسلة من سلطة إشرافية تتعلق بشكل مباشر أو غير مباشر بما يلي: أ) معالجة المورد للمعلومات الشخصية لشركة GSK؛ أو (ب) الإخفاق المحتمل في الامتثال لقوانين حماية البيانات فيما يتعلق بمعالجة المعلومات الشخصية لشركة GSK، يقوم المورد، إلى الحد الذي تسمح به القوانين المعمول بها، بإعادة توجيه المراسلة على الفور إلى شركة GSK وتقديم التعاون والمساعدة المعقولين إلى شركة GSK فيما يتعلق بذلك.

3. إذا قدم الشخص موضوع البيانات طلبًا كتابيًا إلى أي من الطرفين لممارسة أي من حقوقه بموجب قوانين حماية البيانات فيما يتعلق بالمعلومات الشخصية لشركة GSK، يستجيب الطرف المتلقي لهذا الطلب وفقًا لقوانين حماية البيانات. وإلى الحد الذي يتعلق فيه الطلب بمعالجة المعلومات الشخصية لشركة GSK من جانب الطرف الآخر، يقوم الطرف المتلقي بما يلي: (1) إعادة توجيه الطلب على الفور ودون إبطاء لا مبرر له إلى الطرف الآخر؛ و(2) التعاون وتقديم المساعدة المعقولة فيما يتعلق بهذا الطلب لتمكين الطرف الآخر من الاستجابة وفقًا لقوانين حماية البيانات.

4. دون تقييد أي حكم من أحكام جدول الأمن، يقوم المورد لدى علمه بحدوث أي خرق للبيانات الشخصية من شأنه أن يؤثر على المعلومات الشخصية لشركة GSK، بما يلي: (أ) إخطار شركة GSK على الفور وتزويدها بوصف معقول لهذا الخرق؛ و(ب) عدم نشر أي مراسلة تتعلق بالخرق دون استشارة شركة GSK أولاً، باستثناء أنه يجوز له إخطار سلطة إشرافية بالخرق إلى الحد الذي يقتضيه قانون حماية البيانات المعمول به.

النقل الدولي للبيانات

في حالة قيام شركة GSK، بصفتها جهة تصدير البيانات، بنقل معلوماتها الشخصية إلى المورد، بصفته جهة استيراد البيانات، بطريقة تمثل نقلًا دوليًا مقيدًا للبيانات بموجب قوانين حماية البيانات المعمول بها، يبرم كلا الطرفين بموجب هذه الاتفاقية بنودًا نموذجية تغطي العلاقة بين الطرفين ويلتزمان بها:

- ملحق القرار التنفيذي للمفوضية بشأن البنود التعاقدية القياسية لنقل البيانات الشخصية إلى بلدان ثالثة وفقًا للائحة (الاتحاد الأوروبي) 2016/679 للبرلمان الأوروبي والمجلس (**"الملحق"**) بالإضافة إلى الوحدة الأولى: النقل من مراقب إلى مراقب (متوفرة هنا) والمتضمنة في هذه الاتفاقية عن طريق الإشارة حسبما يتم تحديثها أو تعديلها أو استبدالها أو إلغاؤها من وقت لآخر من قبل المفوضية الأوروبية؛ و/أو (2) أي اتفاقية مقابلة أو معادلة للنقل الدولي للبيانات أو ملحق البنود النموذجية الذي اعتمدته السلطة الإشرافية في المملكة المتحدة (**"البنود النموذجية لنقل البيانات من مراقب إلى مراقب"**)؛

- الملحق بالإضافة إلى الوحدة الثانية: النقل من مراقب إلى معالج (متوفرة هنا) والمتضمنة في هذه الاتفاقية عن طريق الإشارة حسبما يتم تحديثها أو تعديلها أو استبدالها أو إلغاؤها من وقت لآخر من قبل المفوضية الاوروبية؛ و/أو (2) أي اتفاقية مقابلة أو معادلة للنقل الدولي للبيانات أو ملحق البنود النموذجية الذي اعتمدته السلطة الإشرافية في المملكة المتحدة (**"البنود النموذجية لنقل البيانات من مراقب إلى معالج"**)؛

"البنود النموذجية" يُقصد بها الملحق بالإضافة إلى البنود النموذجية للنقل من مراقب إلى مراقب والبنود النموذجية للنقل من مراقب إلى معالج.

لأغراض البنود النموذجية، يوافق الطرفان على ما يلي:

- لا ينطبق الخيار الموجود بين قوسين معقوفين في البند 11 "التعويض"
- يتم تحديد الخيار الأول في البند 17 "القانون الحاكم" ويسري قانون أيرلندا.
- يكون لمحاكم أيرلندا الاختصاص القضائي بموجب البند 18 "اختيار المحكمة والاختصاص القضائي".

لأغراض البنود النموذجية للنقل من مراقب إلى معالج والبنود النموذجية للنقل من مراقب إلى مراقب المعمول بها، يُرجى ملاحظة ما يلي:

- الملحق 1 (جهة التصدير وجهة الاستيراد) :تكون شركة GSK أو متلقو الخدمات التابعون لها المعنيون في الاتحاد الأوروبي و/أو المملكة المتحدة بموجب الاتفاقية (الاتفاقيات) المبرمة مع المورد هم جهة تصدير البيانات فيما يتعلق بالمعلومات الشخصية لشركة GSK. ويكون المورد هو جهة استيراد البيانات فيما يتعلق بالمعلومات الشخصية لشركة GSK.

- الملحق 1 (وصف عمليات نقل البيانات): يُرجى الاطلاع على تعريف المعلومات الشخصية والخدمات التي ستقدمها جهة الاستيراد. لا يتم نقل أي بيانات حساسة. ويُعتبر تكرار نقل البيانات مستمرًا. ويتم تحديد طبيعة أنشطة المعالجة وأغراض النقل في الاتفاقية (الاتفاقيات) المبرمة مع المورد. وسيتم الاحتفاظ بالبيانات بما يتماشى مع سياسات الاحتفاظ بالبيانات الخاصة بجهة تصدير البيانات.

- الملحق 1 (السلطات المختصة): على النحو المنصوص عليه في البند 13 من البنود النموذجية للنقل من مراقب إلى مراقب والبنود النموذجية للنقل من مراقب إلى معالج.

- الملحق 2 (التدابير التقنية والتنظيمية): يُرجى الاطلاع على التدابير المتعلقة بالأمن الموضحة أدناه

يوافق الطرفان على أن الخيار 2 من البند 9 "الاستعانة بالمعالجين من الباطن" من البنود النموذجية للنقل من مراقب إلى معالج ينطبق حيثما يقوم المورد بإشراك معالج من الباطن ويوافق المورد والمعالج من الباطن على الالتزام **بالبنود النموذجية للنقل من معالج إلى معالج**، مما يعني 1) الملحق بالإضافة إلى الوحدة الثالثة: النقل من معالج إلى معالج (متوفرة هنا) والمتضمنة في هذه الاتفاقية عن طريق الإشارة حسبما يتم تحديثها أو تعديلها أو استبدالها أو إلغاؤها من وقت لآخر من قبل المفوضية الاوروبية؛ و/أو (2) أي اتفاقية مقابلة أو معادلة للنقل الدولي للبيانات أو ملحق البنود النموذجية الذي اعتمدته السلطة الإشرافية في المملكة المتحدة.

في حالة اعتقاد المورد بأنه غير قادر على تلبية المتطلبات على النحو الذي تحدده شركة GSK بشكلٍ معقول، يجب على المورد أن يخطر الشركة على الفور بعدم قدرته ويكون للشركة الحق في إنهاء الاتفاقية.

يوافق الطرفان على سريان البنود النموذجية المبرمة في بلدان خارج المنطقة الاقتصادية الأوروبية حيث: (1) يتم الاعتراف بأحكامها كإجراء وقائي مناسب فيما يتعلق بعمليات النقل الدولية للبيانات الشخصية إلى البلدان التي تطبق تدابير غير كافية أو (2) تقتضي قوانين حماية البيانات وجود أحكام تعاقدية لحماية عمليات النقل الدولية للمعلومات الشخصية. وعند تفسير البنود النموذجية، في تلك البلدان، سيتم تفسير أي إشارة إلى مصطلح "الدولة العضو التي تم تأسيس جهة تصدير البيانات فيها" على أنها تعني البلد الذي تم تأسيس الكيان التابع لشركة GSK فيه؛ وتكون أي إشارة إلى اللائحة (الاتحاد الأوروبي) 2016/679 إشارة إلى قانون البلد الذي تم تأسيس شركة GSK

فيه خارج المنطقة الاقتصادية الأوروبية. وتعني أي إشارة إلى "البلد الذي يُطبق تدابير كافية" أي بلد يُعتقد أنه يوفر، أو يوفر بطريقة أخرى، مستوى مكافئًا من الحماية لأغراض قوانين حماية البيانات المعمول بها، في تلك البلدان خارج المنطقة الاقتصادية الأوروبية حيث تغطي البنود النموذجية عمليات نقل البيانات الشخصية.

التدابير المتعلقة بالأمن

"بيانات شركة GSK" يُقصد بها أي بيانات أو معلومات تقدمها شركة GSK أو يتم تقديمها نيابة عنها أو يحصل عليها المورد أو موظفوه فيما يتعلق بالتفاوض بشأن الاتفاقية وتنفيذها أو أداء التزامات المورد بموجب الاتفاقية، بما في ذلك أي من البيانات والمعلومات التي إما: (1) يتم إنشاؤها أو إصدارها أو جمعها أو معالجتها من قبل موظفي المورد خلال أداء التزامات المورد بموجب الاتفاقية، أو (2) تكون موجودة في أنظمة معلومات شركة GSK أو المورد أو يتم الوصول إليها من خلالها، بالإضافة إلى أي بيانات ومعلومات مشتقة من المعلومات السابقة.

"المعالجة" تعني أي عملية أو مجموعة من العمليات التي يتم إجراؤها على أي معلومات أو بيانات، سواءً كانت بوسائل مؤتمتة أم لا، مثل الجمع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو المواءمة أو التغيير أو الاسترجاع أو الاطلاع أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر أو الإتاحة أو التعديل أو الدمج أو التقييد أو المحو أو التدمير.

"بيئة المورد" يُقصد بها مجموعة من الأجهزة والبرامج وأنظمة التشغيل وأنظمة قواعد البيانات والأدوات ومكونات الشبكة التي يستخدمها المورد أو يتم استخدامها نيابة عنه لتلقي بيانات شركة GSK أو الاحتفاظ بها أو معالجتها أو تخزينها أو الوصول إليها أو نقلها.

"موظفو المورد" يُقصد بهم أي من وجميع الموظفين الذين يتعاقد معهم أو يعينهم المورد والمقاولون من الباطن التابعون له لأداء أي جزء من الخدمات.

يشكل جدول الأمن هذا جزءًا من الاتفاقية المبرمة بين شركة GSK والمورد. وفي حالة وجود أي تعارض فيما يتعلق بالأمن السيبراني بين شروط جدول الأمن هذا وشروط الاتفاقية، يسري جدول الأمن هذا. وتحمل المصطلحات المكتوبة بحروف كبيرة غير المعرفة في جدول الأمن هذا المعاني المنسوبة إليها في أجزاء أخرى من الاتفاقية.

1. **المسؤوليات** .يتعين على المورد ما يلي: (أ) استخدام ضوابط تشفير قوية لحماية جميع البيانات الخاصة بشركة GSK من الإفصاح أو الوصول أو التغيير غير المصرح به أثناء النقل إلى بيئة المورد أو خارجها عبر الشبكات التابعة لأطراف ثالثة؛ و(ب) الحفاظ على عمليات المراقبة بما يتماشى مع أفضل ممارسات الصناعة لاكتشاف البرامج الضارة والفيروسات وبرامج التجسس ومنعها والتعافي منها، بما في ذلك تحديث برامج مكافحة الفيروسات ومكافحة البرامج الضارة ومكافحة التجسس على فترات منتظمة؛ و(ج) الحفاظ على السياسات والإجراءات والضوابط التقنية المتعلقة بإدارة الوصول بما يتماشى مع أفضل ممارسات الصناعة لضمان أن جميع عمليات الوصول إلى بيانات شركة GSK الخاضعة لمراقبته يتم التصريح بها بشكل مناسب.

2. **الخرق الأمني** .يقوم المورد بإبلاغ شركة GSK عبر البريد الإلكتروني cstd@gsk.com عن أي استخدام أو فقدان أو إتلاف أو إفصاح أو وصول أو تحريف أو تعديل أو بيع أو تأجير أو معالجة أخرى عرضية أو غير مصرح بها أو غير قانونية تم التحقق منها بشأن أي بيانات خاصة بشركة GSK (**"الخرق الأمني"**) في غضون أربع وعشرين (24) ساعة من تحقق المورد. ويضمن المورد إدارة جميع الحوادث المتعلقة بالأمن التي تنطوي على بيانات شركة GSK وفقًا لإجراءات الاستجابة للحوادث المناسبة. ويعمل المورد مع شركة GSK بحسن نية لتحديد السبب الجذري للخرق الأمني ومعالجته.

ANEXO

TERMOS DE PROTEÇÃO DE DADOS – INFORMAÇÕES PESSOAIS BÁSICAS

Afiliada Coberta significa: cada Afiliada da GSK que tenha o benefício dos Serviços como terceiro (uma lista das quais será fornecida pela GSK ao Fornecedor mediante solicitação). Afiliada é toda entidade que, com relação a qualquer outra entidade, seja Controlada, esteja sob Controle comum ou Controle essa outra entidade. "Controle" e seus derivados significam a propriedade (direta ou indireta) da maioria das ações com direito a voto de tal entidade, a capacidade (direta ou indireta) de nomear a maioria dos diretores de tal entidade ou a autoridade para direcionar a gestão ou as políticas de tal entidade, por contrato ou de outra forma;

Legislação de Proteção de Dados significa: (a) o Regulamento Geral sobre a Proteção de Dados (UE) 2016/679 sobre a proteção de pessoas físicas em relação ao processamento de dados pessoais e a livre movimentação desses dados, e as leis e/ou os regulamentos aplicáveis que implementem e/ou exerçam derrogações de acordo com esse regulamento e/ou o substituam ou suplantem (**RGPD**); (b) o RGPD do Reino Unido conforme adaptado pela Lei de Proteção de Dados do Reino Unido 2018; (c) a Lei de Privacidade do Consumidor da Califórnia de 2018 (Código Civil da Califórnia 1798.100 – 1798.199) (California Consumer Privacy Act, **CCPA**); e (d) todas as outras leis relativas ao processamento de dados pessoais;

Informações Pessoais significa o seguinte conjunto: nome e/ou sobrenome, iniciais, dados de contato de trabalho, associações de grupo, número de identificação de rede ou usuário, credenciais de login, histórico e habilidades de trabalho, gênero ou cargo, comparecimento a eventos de funcionários da GSK e trabalhadores complementares que usem os Serviços;

Informações Pessoais da GSK significa Informações Pessoais: (i) fornecidas pela GSK ou em nome da GSK ao Fornecedor (inclusive quando o Fornecedor tiver acesso a Informações Pessoais mantidas pela GSK ou em seu nome), ou que o Fornecedor coletar ou gerar em nome da GSK; (ii) que forem processadas pelo Fornecedor conforme o Contrato ou com relação a ele; e (iii) das quais a GSK seja controladora ou proprietária (ou equivalente);

Anexo de Segurança significa *o anexo de segurança cibernética anexado a este documento como Apêndice 1.*

Os termos **controlador, avaliação de impacto de proteção de dados, titular dos dados, dados pessoais, violação de dados pessoais, processador, processamento, prestador de serviços** e **autoridade de controle** devem ser conforme definido na respectiva Legislação de Proteção de Dados. Qualquer referência à GSK significará a entidade contratante da GSK usada no Contrato e as Afiliadas Cobertas.

Termos do processador

Caso o Fornecedor esteja atuando como processador de Informações Pessoais da GSK nos termos da respectiva Legislação de Proteção de Dados, os seguintes termos serão aplicados:

1. Cada parte cumprirá suas obrigações de acordo com a respectiva Legislação de Proteção de Dados. A GSK e o Fornecedor concordam que, em relação às Informações Pessoais da GSK processadas nos termos deste Contrato, a GSK será a controladora e o Fornecedor será o processador. Para os fins da CCPA, o Fornecedor é um prestador de serviços para a GSK, e o processamento de Informações Pessoais da GSK pelo Fornecedor será realizado apenas para os fins da GSK, de acordo com este Anexo; nenhuma contraprestação monetária ou outra contraprestação valiosa está sendo fornecida pelo Fornecedor à GSK e, portanto, a GSK não está vendendo Informações Pessoais da GSK ao Fornecedor, conforme definido pela CCPA.

2. O Fornecedor cumprirá o seguinte em relação às Informações Pessoais da GSK:

a) processará as Informações Pessoais da GSK somente de acordo com as instruções legais por escrito da GSK e exclusivamente para os fins de prestação de Serviços pelo Fornecedor à GSK nos termos deste Contrato pelo prazo do Contrato ou pelos prazos adicionais dispostos no Contrato, se for o caso;

b) nem o Fornecedor nem qualquer um de seus funcionários, agentes, consultores ou cessionários terão direito de processar as Informações Pessoais da GSK para seu próprio benefício comercial de forma alguma;

c) implementará e adotará medidas de segurança técnicas e organizacionais adequadas, inclusive, sem limitação, as medidas estabelecidas no Anexo de segurança. As referências no Anexo de segurança aos "Dados da GSK" incluirão Informações Pessoais da GSK;

d) manterá as Informações Pessoais da GSK em sigilo de acordo com os termos deste Anexo, e as referências neste Anexo e no Anexo de segurança às Informações Confidenciais da GSK incluirão as Informações Pessoais da GSK;

e) imporá obrigações de confidencialidade equivalentes às obrigações estabelecidas no âmbito do Contrato ao pessoal em questão que tenha acesso às Informações Pessoais da GSK;

f) não contratará outro processador ("**subprocessador**") sem a aprovação prévia por escrito da GSK (e, para esses fins, a GSK consente com as seguintes categorias de subprocessador: prestadores de serviços de infraestrutura de hospedagem, o uso de contratados individuais, e subprocessadores informados à GSK no momento em que o Contrato é celebrado) e transferirá as Informações Pessoais da GSK para tais subprocessadores aprovados somente nos termos de um contrato por escrito que imponha obrigações consistentes com as estabelecidas neste Anexo. Quando o Fornecedor nomeia um subprocessador de acordo com este item 2(f), ele permanece responsável pelos atos e omissões do subprocessador;

g) fornecerá toda a assistência possível à GSK com (i) a realização de avaliações de impacto de proteção de dados exigidas por lei e/ou avaliações de impacto de transferência de dados; (ii) o cumprimento dos direitos dos titulares dos dados; e (iii) o atendimento a solicitações de qualquer autoridade de controle em relação às Informações Pessoais da GSK;

h) notificará a GSK imediatamente após tomar conhecimento de alguma violação de dados pessoais em relação às Informações Pessoais da GSK e fornecerá assistência à GSK em relação a tal violação;

i) notificará a GSK imediatamente se receber uma solicitação por escrito de (i) um titular de dados para exercer qualquer um de seus direitos em relação às Informações Pessoais da GSK nos termos da Legislação de Proteção de Dados; ou de (ii) uma autoridade de controle em relação ao processamento de Informações Pessoais da GSK;

j) salvo disposição em contrário no Contrato, devolverá ou destruirá todas as Informações Pessoais da GSK em sua posse ou sob seu controle (inclusive Informações Pessoais da GSK processadas por subprocessadores permitidos) quando da rescisão ou expiração do Contrato; e

k) mediante solicitação por escrito da GSK, fornecerá à GSK todas as informações necessárias para demonstrar a conformidade com este Anexo, podendo incluir relatórios de auditoria de segurança de terceiros disponíveis.

Termos do controlador

Caso o fornecedor esteja atuando como controlador de Informações Pessoais da GSK de acordo com a respectiva Legislação de Proteção de Dados, os seguintes termos serão aplicáveis:

1. Cada parte atua como controladora independente e cumprirá suas obrigações de acordo com a Legislação de Proteção de Dados aplicável. A GSK e o Fornecedor concordam que, em relação aos dados pessoais processados nos termos deste Anexo, para os objetivos da CCPA, nenhuma contraprestação monetária ou outra contraprestação valiosa está sendo fornecida pelo Fornecedor à GSK em troca das Informações Pessoais da GSK e, portanto, a GSK não está vendendo Informações Pessoais da GSK ao Fornecedor conforme definido pela CCPA.

2. Se o Fornecedor receber alguma comunicação de alguma autoridade de controle relacionada direta ou indiretamente ao (a) processamento de Informações Pessoais da GSK pelo Fornecedor; ou a (b) um possível descumprimento da Legislação de Proteção de Dados em relação ao processamento de Informações Pessoais da GSK, na medida permitida pelas leis aplicáveis, o Fornecedor deverá encaminhar imediatamente a comunicação à GSK e cooperar e oferecer toda a assistência possível à GSK em relação a isso.

3. Se um titular dos dados fizer uma solicitação por escrito a qualquer uma das partes para exercer qualquer um de seus direitos de acordo com a Legislação de Proteção de Dados em relação às Informações Pessoais da GSK, a parte receptora atenderá ao pedido de acordo a Legislação de Proteção de Dados. À medida que a solicitação se referir ao processamento de Informações Pessoais da GSK realizadas pela outra parte, a parte receptora deverá: (i) prontamente e sem atraso indevido, encaminhar a solicitação para a outra parte; e (ii) cooperar e fornecer toda a assistência possível em relação a essa solicitação para permitir que a outra parte responda de acordo com a Legislação de Proteção de Dados.

4. Sem limitar qualquer disposição do Anexo de segurança, ao tomar conhecimento de uma violação de dados pessoais que afete as Informações Pessoais da GSK, o Fornecedor (a) notificará imediatamente a GSK e fornecerá à GSK uma descrição razoável da violação; e (b) não publicará nenhuma comunicação relativa à violação sem primeiro consultar a GSK, salvo se puder notificar uma violação a uma autoridade supervisora na medida exigida pela Lei de Proteção de Dados aplicável.

Transferência internacional de dados

Quando a GSK, atuando como exportadora de dados, transferir Informações Pessoais da GSK ao Fornecedor, atuando como importador de dados, de uma maneira que constitua uma transferência de dados internacional restrita de acordo com a Legislação de Proteção de Dados aplicável, pelo presente, ambas as partes celebram e cumprirão as Cláusulas Modelo aplicáveis que abrangem a relação entre as partes:

- O Anexo à Decisão de Implementação da Comissão sobre cláusulas contratuais padrão para a transferência de dados pessoais para países terceiros de acordo com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ("**Anexo**"), juntamente com o MÓDULO UM: transferir de controlador para controlador (disponível **aqui**) e incorporado neste documento por referência como atualizado, alterado, substituído ou suplantado de tempos em tempos pela Comissão Europeia; e/ou (ii) qualquer contrato de transferência de dados internacional correspondente ou equivalente ou adendo às Cláusulas Modelo adotadas pela autoridade de controle no Reino Unido ("**Cláusulas Modelo C2C**");
- O Anexo, juntamente com o MÓDULO DOIS: transferir de controlador para processador (disponível **aqui**) e incorporado neste documento por referência como atualizado, alterado, substituído ou suplantado de tempos em tempos pela Comissão Europeia; e/ou (ii) qualquer contrato ou adendo de transferência de dados internacional correspondente ou equivalente às Cláusulas Modelo adotadas pela autoridade de controle no Reino Unido ("**Cláusulas Modelo C2P**");

"**Cláusulas Modelo**" refere-se ao Anexo juntamente com as Cláusulas Modelo C2C e as Cláusulas Modelo C2P.

Para os fins das Cláusulas Modelo, as partes concordam que:

- A opção entre colchetes da Cláusula 11 "Reparo" não se aplica
- A opção um é selecionada para a Cláusula 17 "Lei aplicável", e a lei da Irlanda será aplicável.
- Os tribunais da Irlanda serão competentes nos termos da Cláusula 18 "Eleição de foro".

Para os fins das Cláusulas Modelo C2P e das Cláusulas Modelo C2C aplicáveis, observe o seguinte:

- Anexo 1 (Exportador e importador): a GSK ou os respectivos destinatários do serviço da GSK localizados na UE e/ou no Reino Unido nos termos do(s) contrato(s) com o Fornecedor são um Exportador de Dados em relação às Informações Pessoais da GSK. O Fornecedor é um Importador de Dados em relação às Informações Pessoais da GSK.
- Anexo 1 (Descrição das transferências): consulte a definição de Informações Pessoais e Serviços a serem fornecidos pelo Importador. Nenhum dado confidencial é transferido. A frequência da transferência é contínua. A natureza das atividades de processamento e as finalidades da transferência estão definidas no(s) contrato(s) com o Fornecedor. Os dados serão retidos de acordo com as políticas de retenção de dados do Exportador de Dados.
- Anexo 1 (Autoridades competentes): conforme estabelecido na cláusula 13 das Cláusulas Modelo C2C e Cláusulas Modelo C2P.
- Anexo 2 (Medidas técnicas e organizacionais): consulte as Medidas de segurança estabelecidas abaixo.

As partes concordam que a opção 2 da Cláusula 9 "Uso de subprocessadores" das Cláusulas Modelo C2P será aplicada quando o Fornecedor contratar um subprocessador e o Fornecedor e o subprocessador concordarem em cumprir as **Cláusulas Modelo P2P**, o que significa i) o Anexo juntamente com o MÓDULO TRÊS: transferir de processador para processador (disponível **aqui**) e incorporado neste documento por referência como atualizado, alterado, substituído ou suplantado de tempos em tempos pela Comissão Europeia; e/ou (ii) qualquer contrato ou adendo de transferência de dados internacional correspondente ou equivalente às Cláusulas Modelo adotadas pela autoridade de controle no Reino Unido.

Caso o Fornecedor acredite que não poderá atender aos requisitos estabelecidos pela GSK, o Fornecedor notificará a GSK imediatamente sobre a impossibilidade, e a GSK terá o direito de rescindir o Contrato.

As Partes concordam que as Cláusulas Modelo celebradas terão efeito em países fora do Espaço Econômico Europeu onde: (i) suas disposições sejam reconhecidas como proteção suficiente em relação a transferências internacionais de Dados Pessoais para países não adequados ou (ii) a Legislação de Proteção de Dados exija a existência de disposições contratuais para proteger transferências internacionais de Informações Pessoais. Ao interpretar as Cláusulas Modelo, nesses países, todas as referências ao termo "Estado-membro no qual o exportador de dados está estabelecido" serão interpretadas como o país no qual a entidade da GSK esteja estabelecida; e todas as referências ao Regulamento (UE) 2016/679 serão de acordo com a lei do país onde a GSK esteja estabelecida fora do EEE. Todas as referências a "País adequado" significam país que forneça ou que se considere que forneça um nível equivalente de proteção para os fins da Legislação de Proteção de Dados aplicável, nos países fora do Espaço Econômico Europeu, onde as Cláusulas Modelo abrangerão as transferências de Dados Pessoais.

Medidas de segurança

"Dados da GSK" significa informações ou dados fornecidos pela GSK ou em nome dela ou obtidos pelo Fornecedor ou pelo Pessoal do Fornecedor relacionados à negociação e à assinatura do Contrato ou ao cumprimento das obrigações do Fornecedor nos termos do Contrato, inclusive informações e dados: (i) criados, gerados, coletados ou processados pelo Pessoal do Fornecedor no desempenho das obrigações do Fornecedor nos termos do Contrato, ou (ii) que residam nos sistemas de informação da GSK ou nos sistemas de informação do Fornecedor, ou sejam acessados através deles, e informações e dados derivados do exposto acima.

"**Processamento**" significa qualquer operação ou conjunto de operações que seja realizada em qualquer informação ou dado, seja por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou disponibilização, alinhamento ou combinação, restrição, exclusão ou destruição.

"Ambiente do Fornecedor" significa a combinação de hardware, software, sistemas operacionais, sistemas de banco de dados, ferramentas e componentes de rede usados pelo Fornecedor ou em nome dele para receber, manter, processar, armazenar, acessar ou transmitir Dados da GSK.

"Pessoal do Fornecedor" significa todo e qualquer pessoal contratado ou empregado pelo Fornecedor e por seus Subcontratados para executar qualquer parte dos Serviços.

Este Anexo de segurança é parte integrante do Contrato entre a GSK e o Fornecedor. Em caso de conflito com relação à segurança cibernética entre os termos deste Anexo de segurança e os termos do Contrato, este Anexo de segurança prevalecerá. Os termos em letras maiúsculas não definidos neste Anexo de segurança terão os significados atribuídos a eles em outras partes do Contrato.

1. Responsabilidades. É responsabilidade do Fornecedor: (a) usar controles de criptografia robustos para proteger todos os Dados da GSK contra divulgação não autorizada, acesso ou alteração em trânsito para dentro ou fora do Ambiente do Fornecedor em redes de terceiros; (b) manter os processos de controle alinhados com as melhores práticas do setor para detecção, prevenção, e recuperação de malware, vírus e spyware, inclusive a atualização de antivírus, software antimalware e antispyware em intervalos regulares; e (c) manter políticas e procedimentos de gerenciamento de acesso, e controles técnicos de acordo com as melhores práticas do setor para assegurar que todo acesso aos Dados da GSK sob seu controle tenha sido devidamente autorizado.

2. Violação de segurança. O Fornecedor relatará à GSK por e-mail para cstd@gsk.com qualquer acesso ou uso, perda, destruição, divulgação, corrupção, modificação, venda, locação ou outro processamento acidental, não autorizado ou ilegal verificado de Dados da GSK ("**Violação de Segurança**") no prazo de 24 (vinte e quatro) horas a contar da conclusão da verificação do Fornecedor. O Fornecedor assegurará que todos os incidentes de segurança envolvendo Dados da GSK sejam gerenciados de acordo com os procedimentos adequados de resposta a incidentes e trabalhará com a GSK de boa-fé para identificar uma causa raiz e remediar a Violação de Segurança.

附件

数据保护条款—基本个人信息

相关关联方指：以第三方身份享受服务权益的每一个 GSK 关联方（GSK 将应要求向供应商提供此类关联方清单）。就任何其他实体而言，关联方是指受此类其他实体控制、与此类其他实体受共同控制或控制此类其他实体的任何实体。"控制"及其派生词是指（直接或间接）拥有此类实体的大部分有表决权股份，或有能力（直接或间接）委任此类实体的大部分董事，或有权指示此类实体的管理或政策，无论是通过合同还是其他方式；

数据保护法指：(a) 关于保护自然人在个人数据处理和此类数据自由流动中权利的欧盟第 2016/679 号《通用数据保护条例》，以及实施/行使该条例项下免除适用和/或取代或替代该条例的任何适用法律和/或法规 (**GDPR**)；及 (b) 经 2018 年《英国数据保护法》修订的 GDPR；(c) 2018 年《加州消费者隐私法》（《加州民法典》第 1798.100 – 1798.199 条）(**CCPA**)；及 (d) 所有涉及个人数据处理的其他法律；

个人信息指以下范围内的个人数据：使用服务的 GSK 员工和临时工的名字和/或姓氏、姓名缩写、工作联系方式、团体成员身份、网络或用户识别号、登录凭据、工作履历和技能、性别或职务以及活动参与情况；

GSK 个人信息指以下任何个人信息：(i) 由 GSK 或代表其向供应商提供的个人信息（包括供应商有权访问、由 GSK 或代表其持有的个人信息的情况），或供应商代表 GSK 收集或生成的个人信息；(ii) 供应商在本协议项下或与本协议相关而处理的个人信息；及 (iii) GSK 是控制者或所有者（或同等身份）的个人信息；

安全附件指*本文件随附的网络安全附件，即附则 1*。

控制者、数据保护影响评估、数据主体、个人数据、个人数据泄露、处理者、处理、服务提供商以及**监管机构**等词语的定义参见相关数据保护法。凡提及 GSK 时均指协议中使用的 GSK 签约实体，以及相关关联方。

处理者条款

如果供应商在相关数据保护法项下担任 GSK 个人信息的处理者，则以下条款适用：

1. 各方应遵守其在适用数据保护法项下的义务。GSK 和供应商同意，就在本协议项下处理的 GSK 个人信息而言，GSK 将是控制者，供应商将是处理者。就 CCPA 而言，供应商是 GSK 的服务提供商，供应商处理 GSK 个人信息应仅根据本附件为了 GSK 而进行，供应商未向 GSK 提供任何金钱或其他有价值的对价，因此 GSK 未向供应商出售（定义见 CCPA）GSK 个人信息。

2. 关于 GSK 个人信息，供应商应遵守以下要求：

a) 仅根据 GSK 的合法书面指示、为了向 GSK 提供本协议项下服务的唯一目的、在本协议期限内或本协议中载明的任何额外期限内（如适用）处理 GSK 个人信息；

b) 供应商、其任何员工、代理人、顾问或受让人均无权为其自己任何形式的商业利益而处理 GSK 个人信息；

c) 实施并维持适当的技术和组织安全措施，包括但不限于安全附件中列出的措施。安全附件中提及的"GSK 数据"应包括 GSK 个人信息；

d) 根据本附件条款对 GSK 个人信息保密；本附件及安全附件中提及的 GSK 机密信息应包括 GSK 个人信息；

e) 要求有权访问 GSK 个人信息的相关人员承担与本协议中规定的义务相当的保密义务；

f) 未经 GSK 事先书面批准，不得聘请其他处理者（"**子处理者**"）（就此目的而言，GSK 同意接受以下类别的子处理者：托管基础设施服务提供商、个人承包商以及在签订协议时已经告知 GSK 的子处理者），只能根据书面合同（规定与本附件相同的义务）将 GSK 个人信息传输给此类经过批准的子处理者。如供应商根据本第 2(f) 条委任子处理者，其仍应对子处理者的作为和不作为负责；

g) 在以下方面向 GSK 提供合理协助：(i) 实施法律要求的数据保护影响评估和/或数据传输影响评估；(ii) 遵照数据主体的权利；及 (iii) 对任何监管机构提出的关于 GSK 个人信息的要求作出回应；

h) 在获知任何 GSK 个人信息发生个人数据泄露后，立即通知 GSK 并就处理此类泄露向 GSK 提供相关协助；

i) 如果收到以下各方发出的书面要求，立即通知 GSK：(i) 数据主体，要求行使其在数据保护法项下与 GSK 个人信息相关的任何权利；或 (ii) 监管机构，涉及 GSK 个人信息的处理；

j) 除非协议中另有规定，否则在协议终止或期满后，归还或销毁其持有或控制的所有 GSK 个人信息（包括由经许可的子处理者处理的任何 GSK 个人信息）；及

k) 应 GSK 的书面要求，向 GSK 提供证明遵守本附件的合理必要信息，包括任何可提供的第三方安全审计报告。

控制者条款

如果供应商在相关数据保护法项下担任 GSK 个人信息的控制者，则以下条款适用：

1. 各方以独立控制者的身份行事，并应遵守其在适用数据保护法项下的义务。GSK 和供应商同意，关于在本附件项下处理的个人数据，就 CCPA 而言，供应商未向 GSK 提供任何金钱或其他有价值的对价，作为 GSK 个人信息的交换，因此 GSK 未向供应商出售（定义见 CCPA）GSK 个人信息。

2. 如果供应商收到监管机构发出的直接或间接涉及以下各项的任何通讯信息：a) 供应商处理 GSK 个人信息；或 (b) 处理 GSK 个人信息可能未遵守数据保护法，则供应商应在适用法律允许的范围内，立即将此类通讯信息转发给 GSK，并就此向 GSK 提供合理的配合和协助。

3. 如果数据主体向任何一方提出书面要求，希望行使其在数据保护法项下与 GSK 个人信息相关的任何权利，接收方应根据数据保护法对此要求作出回应。如果此类要求涉及由另一方处理的 GSK 个人信息，接收方应：(i) 立即将要求转发给另一方，不得无故延迟；及 (ii) 配合并合理协助处理该要求，以便另一方能够根据数据保护法作出回应。

4. 在不限制安全附件任何规定的情况下，如获知影响 GSK 个人信息的个人数据泄露，供应商应 (a) 立即通知 GSK，并向 GSK 提供对泄露情况的合理描述；及 (b) 在未首先征求 GSK 意见的情况下，不得就泄露发布任何通讯信息，但在适用数据保护法要求的范围内，可将泄露情况通知监管机构。

国际数据传输

如 GSK（作为数据输出方）将 GSK 个人信息传输给供应商（作为数据输入方），且此传输构成适用数据保护法项下的受限国际数据传输，则双方特此就双方之间的关系签订相应的示范条款并将遵守其规定：

- 根据欧洲议会和欧洲理事会第 2016/679 号条例（欧盟），关于向第三国传输个人数据的标准合同条款的委员会实施决策附录（"**附录**"），以及第一模块：控制者到控制者传输（参见此处），通过引用纳入本文件，包括欧洲委员会做出的更新、修订、更换或替代；和/或 (ii) 英国监管机构通过的相应或同等国际数据传输协议或对示范条款的补充（"**C2C 示范条款**"）；
- 附录及第二模块：控制者到处理者传输（参见此处），通过引用纳入本文件，包括欧洲委员会做出的更新、修订、更换或替代；和/或 (ii) 英国监管机构通过的相应或同等国际数据传输协议或对示范条款的补充（"**C2P 示范条款**"）；

"**示范条款**"指附录及 C2C 示范条款和 C2P 示范条款。

就示范条款而言，双方同意：

- 第 11 条"补救"方框中的选项不适用
- 第 17 条"适用法律"选择第一项，爱尔兰法律适用。
- 关于第 18 条"法院和管辖权选择"，爱尔兰法院拥有司法管辖权。

就适用的 C2P 示范条款和 C2C 示范条款而言，请注意以下事项：

- 附录 1（输出方和输入方）：GSK 或位于欧盟和/或英国、与供应商签订协议的相关 GSK 服务接收方是 GSK 个人信息的数据输出方。供应商是 GSK 个人信息的数据输入方。
- 附录 1（传输描述）：请参见个人信息和输入方提供的服务的定义。不传输敏感数据。传输频率为连续。处理活动的性质和传输的目的见与供应商签订的协议。数据将根据数据输出方的数据保留政策保留。
- 附录 1（主管机构）：请参见 C2C 示范条款和 C2P 示范条款第 13 条
- 附录 2（技术和组织措施）：请参见下文所述的安全措施

双方同意，如果供应商聘请子处理者，则 C-P 示范条款第 9 条"使用子处理者"选项 2 适用，且供应商和子处理者应同意遵守 **P-P 示范条款**，即 i) 附录和第三模块：处理者到处理者传输（参见此处），通过引用纳入本文件，包括欧洲委员会不时做出的更新、修订、更换或替代；和/或 (ii) 英国监管机构通过的相应或同等国际数据传输协议或对示范条款的补充；

如果供应商认为其无法满足 GSK 的合理要求，则供应商应立即将其无法满足的情况通知 GSK，且 GSK 应有权终止协议。

双方同意，在以下情况下，订立的示范条款在欧洲经济区以外的国家/地区应有效：(i) 对于向未提供充分保护的国家/地区进行个人数据国际传输，示范条款的规定被认为是适当的保护措施，或 (ii) 数据保护法要求制定保护个人信息国际传输的合同规定。在这些国家/地区解释示范条款时，凡提及"数据输出方成立所在的成员国"，均应解释为 GSK 实体成立所在的国家/地区；凡提及欧盟第 2016/679 号条例，均应解释为欧洲经济区之外 GSK 成立所在国家/地区的法律。凡提及"提供充分保护的国家/地区"，均指被认为提供或以其他方式提供了欧洲经济区之外国家/地区（示范条款适用于个人数据的传输）的适用数据保护法项下同等保护水平的任何国家/地区。

安全措施

"GSK 数据"指在协议谈判或签署过程中，或供应商履行在协议项下义务的过程中，由 GSK **或代表其提供的或供**应商或供应商人员获取的任何数据或信息，包括以下任何此类数据和信息：(i) **由供**应商人员在履行供应商在协议项下义务的过程

中创建、生成、收集或处理的数据和信息，或 (ii) **存**储于 GSK **信息系**统或供应商信息系统中或可通过这些系统访问，以及通过上述衍生而得的任何数据和信息。

"**处理**"指对任何信息或数据进行的任何操作或系列操作，无论是否是通过自动化手段，例如收集、记录、组织、结构、存储、改编或改动、检索、咨询、使用、传输披露、传播或以其他方式提供、调整或合并、限制、擦除或销毁。

"供应商环境"指由供应商或代表供应商用于接收、维护、处理、存储、访问或传输 GSK 数据的硬件、软件、操作系统、数据库系统、工具和网络组件的组合。

"供应商人员"指供应商或其分包商聘用或雇用履行任何部分服务的任何和所有**人**员。

本安全附件构成 GSK 与供应商之间协议的组成部分。如本安全附件的条款与协议条款之间关于网络安全出现任何冲突，以本安全附件为准。本安全附件中未定义的特定术语具有协议其他部分赋予的含义。

1. 责任。供应商应：(a) 使用强加密保护，防止所有 GSK 数据在通过第三方网络从供应商环境传入或传出过程中遭到未经授权的披露、访问或更改；(b) 制定符合行业最佳实践的控制程序，以检测和预防恶意软件、病毒和间谍软件并制定好恢复措施，包括定期更新反病毒、反恶意软件和反间谍软件的软件；(c) 制定符合行业最佳实践的访问权限管理政策、程序和技术控制措施，确保所有访问其所控制 GSK 数据的行为均得到适当授权。

2. 安全违规。对于任何 GSK 数据经核实的意外、未经授权或非法使用、丢失、销毁、披露、访问、破坏、修改、出售、出租或其他处理（"**安全违规**"），供应商应在核实后二十四 (24) 小时内通过发送电子邮件至 cstd@gsk.com 向 GSK 报告。供应商应确保所有涉及 GSK 数据的安全事件均根据适当的事件响应程序进行管理。供应商应善意配合 GSK，以确定根本原因并纠正安全违规。

附表

資料保護條款 – 基本個人資訊

涵蓋附屬企業係指：作為第三方享有服務益處的各個 GSK 關係企業（GSK 將根據請求向供應商提供一份清單）。附屬企業係指對於任何其他實體而言，由此類其他實體控制、共同控制或控制此類其他實體的任何實體。「控制權」及其衍生詞係指（直接或間接）透過合約或其他方式，擁有該實體多數表決權的股份，或者是能夠（直接或間接）任命該實體多數董事或指示該實體管理層或政策的授權；

資料保護法係指：(a) 關於在處理個人資料及該資料自然流通方面保護自然人的《通用資料保護法規 (EU) 2016/679》，以及依據該法實施及/或行使廢除並予以取代的任何適用法律及/或法規 (**GDPR**)；及 (b) 根據 2018 年《英國資料保護法》所定之 GDPR；(c) 2018 年《美國加州消費者隱私法》（加州民法典第 1798.100-1798.199條 ）(**CCPA**)；和 (d) 有關個人資料處理的所有其他法律；

個人資訊係指以下組合中的個人資料：名字和/或姓氏、姓名縮寫、工作聯絡詳情、團隊成員資格、網路或使用者識別號碼、登入憑證、工作經歷和技能、性別或頭銜、GSK 員工和使用服務之補充工作人員的活動出席狀況；

GSK 個人資訊係指以下任何個人資訊：(i) 由 GSK 或代表 GSK 提供予供應商（包括供應商有權存取 GSK 或其代表擁有的個人資訊），或供應商代表 GSK 收集或產生的任何個人資訊；(ii) 供應商因本協議或與本協議有關而處理之個人資訊；及 (iii) GSK 為其控管者或所有權人（或同等人員）之任何個人資訊；

安全附表係指附錄 1 所附之*網路安全附表*。

控管者、資料保護影響評估、資料當事人、個人資料洩露、處理者、處理、服務供應商和**主管機關**等詞彙，應依據相關資料保護法的定義。凡提及 GSK 之處應指協議中使用的 GSK 簽約實體及涵蓋附屬企業。

處理者條款

若供應商根據相關資料保護法擔任 GSK 個人資訊的處理者，則適用以下條款：

1. 各方應遵守適用資料保護法規定之義務。GSK 和供應商同意，根據本協議處理的 GSK 個人資訊，GSK 將為控管者，而供應商將為處理者。就 CCPA 而言，供應商是 GSK 的服務供應商，且供應商對 GSK 個人資訊的處理僅應出於根據本附表的 GSK 目的進行，因供應商未向 GSK 提供金錢或其他有值對價，因此 GSK 不會如 CCPA 所定義向供應商銷售 GSK 個人資訊。

2. 供應商應遵守以下有關 GSK 個人資訊的規定：

a) 僅根據 GSK 的合法書面指示處理 GSK 個人資訊，且僅用於供應商在本協議期間或本協議所載的任何其他期間（若適用）向 GSK 提供服務；

b) 供應商或其任何員工、代理商、顧問或受讓者無權為其自身商業利益以任何形式處理 GSK 個人資訊；

c) 實施並維護適當的技術和組織安全措施，包括但不限於安全附表中規定的措施。安全附表中所指之「GSK 資料」應包括 GSK 個人資訊；

d) 根據本附表條款及本附表中的參照，對 GSK 個人資料進行保密，而且 GSK 機密資訊的安全附表應包括 GSK 個人資訊；

e) 對有權存取 GSK 個人資訊的相關人員，施予相當於本協議所規定之義務的保密義務；

f) 未經 GSK 事先書面核准，不得聘用其他處理者（以下簡稱「**輔助處理者**」）（出於相同目的，GSK 同意以下類別的輔助處理者：代管基礎設施服務供應商、使用個人承包商以及 GSK 於訂立協議時知悉的輔助處理者），同時僅根據書面合約將 GSK 個人資訊傳輸至上述經核准之輔助處理者，其中該合約賦予與本附表中所載一致的義務。供應商根據本條款 2 (f) 任用輔助處理者時，應對該輔助處理者的作為和不作為負責；

g) 提供 GSK 以下合理協助：(i) 進行任何法律規定的資料保護影響評估和/或資料傳輸影響評估；(ii) 遵守資料當事人的權利；以及 (iii) 回應任何主管機關就 GSK 個人資訊提出的請求；

h) 在獲悉有關任何 GSK 個人資訊的個人資料洩漏後，立即通知 GSK，並就相關洩漏事宜為 GSK 提供協助；

i) 在收到來自以下對象的書面通知後立即通知 GSK：(i) 資料當事人根據資料保護法行使與 GSK 個人資訊相關的任何權利時；或 (ii) 與處理 GSK 個人資訊相關的主管機關；

j) 除非本協議另行規定，否則在協議終止或到期時，歸還或銷毀所持有或受其控制的所有 GSK 個人資訊（包括經許可輔助處理者處理的任何 GSK 個人資訊）；以及

k) 根據 GSK 的書面請求，向 GSK 提供證明遵守本附表所需的合理資訊，其中可能包括任何可用的第三方安全稽核報告。

控管者條款

若供應商根據相關資料保護法擔任 GSK 個人資訊的控管者，則適用以下條款：

1. 各方擔任獨立控管者，並應遵守所適用之資料保護法規定的義務。GSK 和供應商同意，就本附表所處理的個人資料而言，在 CCPA 目的下，供應商未向 GSK 提供金錢或其他有值對價，以換取 GSK 個人資訊，因此 GSK 不會如 CCPA 所定義向供應商銷售 GSK 個人資訊。

2. 若供應商自主管機關收到與以下直接或間接有關的任何通訊，應在適用法律允許範圍，立即將該通訊內容轉達 GSK，並就相關事宜向 GSK 提供合理的合作及協助：(a) 供應商處理 GSK 個人資訊方面；或 (b) 有關處理 GSK 個人資訊方面潛在違反資料保護法的行為。

3. 若資料當事人向任一方提出書面請求，要求行使其在 GSK 個人資訊方面資料保護法所規定的任何權利，則接收方應根據資料保護法回應該請求。如果請求涉及另一方處理 GSK 個人資訊，接收方應：(i) 及時且不得不當延遲地向另一方提交請求；及 (ii) 就該項請求予以配合並提供合理協助，以便另一方按照資料保護法作出回應。

4. 在不限制安全附表的任何規定下，於獲悉影響 GSK 個人資訊的個人資料洩露後，供應商：(a) 應立即通知 GSK 並提供合理的洩漏描述給 GSK；(b) 不得在未事先諮詢 GSK 的情況下發表有關洩漏行為的任何通訊，但在適用資料保護法規定範圍內得將相關洩漏事宜通知主管機構除外。

跨國資料傳輸

GSK 作為資料輸出方，以根據適用的資料保護法構成限制性跨國資料傳輸的方式，將 GSK 個人資訊傳輸予作為資料輸入方之供應商，雙方特此簽訂並將遵守涵蓋雙方關係的適用示範條款：

- 根據歐洲議會和委員會的法規 2016/679，將個人資料傳輸至第三國的標準合約條款之執委會執行裁定書附件 （以下簡稱「**附件**」）連同單元一：由控管者傳輸至控管者（可**在此**取得），並在此透過引用方式納入，由歐盟執委會不時更新、修訂或取代之；及/或 (ii) 任何對應或同等的跨國資料傳輸協議或英國主管機關所核准示範條款的增補合約（以下簡稱「**C2C 示範條款**」）；
- 附件連同單元二：由控管者傳輸至處理者（可**在此**取得），並在此透過引用方式納入，由歐盟執委會不時更新、修訂或取代之；及/或 (ii) 任何對應或同等的跨國資料傳輸協議或英國主管機關所核准示範條款的增補合約（以下簡稱「**C2P 示範條款**」）；

「**示範條款**」係指隨附於 C2C 示範條款及 C2P 示範條款之附件。

就示範條款而言，雙方當事人同意：

- 不適用第 11 條「補償」中方括弧內的選項。
- 第 17 條「準據法」選擇選項 1，並適用愛爾蘭法律。

- 愛爾蘭法院將依據第 18 條「選擇法院與管轄權」具有管轄權。

就適用 C2P 示範條款及 C2C 示範條款而言，請注意下列事項：

- 附件 1（輸出方和輸入方）：依據與供應商訂立的協議，GSK 或位於歐盟和/或英國的相關 GSK 服務接受方為 GSK 個人資訊的資料輸出方。供應商為 GSK 個人資訊的資料輸入方。
- 附件 1（傳輸之說明）：請見輸入方所提供之個人資訊與服務定義。不得傳輸任何敏感資料。傳輸頻率為連續。處理活動的性質和傳輸的目的載於與供應商簽訂的協議中。資料將依照資料輸出方的資料保留政策予以保留。
- 附件 1（主管機關）：如 C2C 示範條款和 C2P 示範條款第 13 條所述。
- 附件 2（技術及組織措施）：請見下列安全措施。

雙方同意，在供應商聘用輔助處理者時，應適用 C-P 示範條款第 9 條「使用輔助處理者」中的選項 2，同時供應商和輔助處理者應同意遵守 **P-P 示範條款**，意指 (i) 附件連同單元三：由處理者傳輸至處理者（可於**此處**取得），並在此透過引用方式納入，由歐盟執委會不時更新、修訂或取代之；及/或 (ii) 任何對應或同等的跨國資料傳輸協議或英國主管機關所核准示範條款的增補合約；

若供應商不認為其可符合 GSK 合理規定的要求，供應商應將其無法履行情事立即通知 GSK，且 GSK 有權終止協議。

各方同意，所簽訂的示範條款在歐洲經濟區以外的國家具有效力：(i) 其規定被認為是與將個人資料跨國傳輸至保護不足之國家時的相關適當保護措施，或 (ii) 資料保護法律規定應存在保護個人資料跨國傳輸的合約條款。在解釋示範條款時，在這些國家中，凡提及「資料輸出方所在之成員國」一詞時，將解釋為 GSK 實體設立所在的國家；而凡提及法規《（EU）2016/679》，將為 GSK 在歐洲經濟區以外設立的國家法律。凡提及「適當國家」時，均指涵蓋個人資料傳輸之示範條款應適用的歐洲經濟區以外國家，為適用資料保護法令目的，被認為提供或以其他方式提供同等保護的國家。

安全措施

「GSK 資料」是指由 GSK 提供或代表 GSK 提供，或由供應商或供應商人員就協議的談判和執行，或履行本協議下供應商義務等，而獲取的任何資料或資訊，包括以下任一資料和資訊：(i) 由供應商人員在履行本協議規定之供應商義務時所建立、產生、收集或處理，或 (ii) 存在於 GSK 資訊系統或供應商資訊系統，或透過 GSK 資訊系統或供應商資訊系統存取，以及衍生自前述系統之任何資料和資訊。

「**處理**」係指針對任何資訊或資料執行的任何操作或一組操作，無論其是否以自動化方式執行，例如收集、錄製、組織、建構、儲存、改編或變更、擷取、參閱、利用、透過傳輸揭露、散播或以其他方式提供、比對或組合、限制、清除或銷毀。

「供應商環境」係指供應商或其代表為接收、維護、處理、儲存、存取或傳輸 GSK 資料而使用之硬體、軟體、作業系統、資料庫系統、工具及網路元件的組合。

「供應商人員」係指供應商及其分包商聘用或雇用以執行服務任何部分的任何及所有人員。

本安全附件構成 GSK 與供應商共同簽訂之本協議的一部分。若本安全附件條款與本協議條款在網路安全方面有任何衝突，應以本安全附表為準。本安全附表中未定義之英文大寫詞彙，其定義與該詞彙於本協議其他部分之定義相同。

1. 責任。供應商應：(a) 使用嚴格的加密控管來保護所有 GSK 資料，使其在透過第三方網路進出供應商環境的過程中免遭未經授權的揭露、存取或變更；(b) 維持符合業界最佳實務的控管流程，以偵測、預防惡意軟體、病毒和間諜軟體（其中包括定期更新防毒軟體、反惡意軟體和反間諜軟體），並從中復原；(c) 維護符合業界最佳實務的存取管理政策、程序及技術控管，以確保控管中對 GSK 資料的所有存取獲得適當授權。

2. 安全漏洞。供應商將在其驗證二十四 (24) 小時內透過電子郵件去信至 cstd@gsk.com，就任何 GSK 資料未經驗證的意外、未授權或非法利用、損失、銷毀、揭露、存取、毀損、修改、銷售、租賃或其他處理狀況報告 GSK（以下簡稱「**安**

全洩漏」）。供應商將確保涉及 GSK 資料的所有安全事件均按照適當的事件回應程序進行管理，供應商應善意與 GSK 合作，以確定根本原因並補救安全漏洞。

PLÁN

PODMÍNKY OCHRANY ÚDAJŮ – ZÁKLADNÍ OSOBNÍ INFORMACE

Zahrnutá přidružená společnost znamená: každou přidruženou společnost společnosti GSK, která požívá služeb jako třetí strana (jejich seznam bude poskytnut společností GSK dodavateli na požádání). Přidružená společnost je subjekt, který ve vztahu k jakémukoliv jinému subjektu, je ovládán nebo se nachází pod společným ovádáním s tímto subjektem nebo tento jiný subjekt ovládá. „Ovládání" a odvozené výrazy označují vlastnictví (přímé nebo nepřímé) většiny akcií s hlasovacím právem takového subjektu nebo schopnost (přímo či nepřímo) jmenovat většinu ředitelů takového subjektu za účelem řízení spravovování podniíkových směrnic takového subjektu, na základě smlouvy či jinak;

Zákony na ochranu osobních údajů znamenají: (a) obecné nařízení o ochraně údajů (EU) 2016/679 na ochranu fyzických osob ve vztahu ke zpracování osobních údajů a svobodnému pohybu těchto údajů a jakékoliv platné zákony a/nebo nařízení, které zavádějí a/nebo které v jeho rámci uplatňují výjimky a/nebo jej nahrazují (**GDPR**); (b) GDPR upravené britským zákonem o ochraně osobních údajů z roku 2018; (c) kalifornský zákon o ochraně soukromí spotřebitelů z roku 2018 (Cal. Civ. Code 1798.100 – 1798.199) (**CCPA**); a (d) veškeré ostatní zákony vztahující se na zpracování osobních údajů.

Osobní informace znamenají osobní informace, které zahrnují následující osobní údaje: křestní jméno a/nebo příjmení, iniciály, kontaktní údaje, členství ve skupinách, síťová nebo uživatelská identifikační čísla, přihlašovací údaje, pracovní historie nebo schopnosti, pohlaví nebo titul a účasti na událostech zaměstnanců a zastupujících pracovníků společnosti GSK využívajících služby

Osobní informace společnosti GSK znamenají veškeré osobní údaje: (i) poskytnuté společností GSK nebo jejím jménem dodavateli (včetně situací, kdy má dodavatel přístup k osobním údajům drženým společností GSK nebo jejím jménem), nebo které dodavatel shromáždí nebo vytvoří jménem společnosti GSK; (ii) které jsou zpracovány dodavatelem v rámci nebo ve spojení s touto smlouvou; a (iii) ve vztahu kde společnost GSK je jejich kontrolorem nebo vlastníkem (nebo ekvivalentem vlastníka).

Plán bezpečnosti označuje *plán kybernetické bezpečnosti připojený k tomuto dokumentu jako příloha 1*.

Výrazy **správce, posouzení vlivu na ochranu osobních údajů, subjekt údajů, osobní údaje, porušení zabezpečení osobních údajů, zpracovatel, zpracování, poskytovatel služeb** a **dozorový úřad** mají význam definovaný příslušnými zákony na ochranu osobních údajů. Odkaz na společnost GSK označuje smluvní subjekt společnosti GSK použitý ve smlouvě, jakož i zahrnuté přidružené společnosti.

Podmínky zpracovatele

V případě, že dodavatel vystupuje jako zpracovatel osobních informací společnosti GSK podle příslušných zákonů na ochranu osobních údajů, platí následující podmínky:

1. Každá ze stran bude dodržovat povinnosti, které se na ni vztahují podle platných zákonů na ochranu osobních údajů. Společnost GSK a dodavatel souhlasí s tím, že ve vztahu k osobnícm údajům společnosti GSK zpracovávaným podle této smlouvy bude společnost GSK správcem údajů a dodavatel bude zpracovatelem údajů. Pro účely CCPA je dodavatel poskytovatelem služeb pro společnost GSK a ke zpracování osobních informací společnosti GSK bude docházet pouze pro účely společnosti GSK v souladu s tímto plánem a dodavatel neposkytuje společnosti GSK peněžitou ani jinou protihodnotu, a tudíž společnost GSK osobní informace společnosti GSK neprodává dodavateli, jak je definováno CCPA.

2. Dodavatel je povinen dodržovat následující povinnosti ve vztahu k osobním informacím společnosti GSK:

a) zpracovávat osobní informace společnosti GSK pouze na základě zákonných psaných pokynů a pouze pro účely poskytování služeb dodavatelem společnosti GSK podle této smlouvy po dobu trvání období smlouvy nebo jiné další období případně uvedené ve smlouvě;

b) dodavatel ani jeho zaměstnanci, zástupci, poradci nebo určené osoby nemají právo zpracovávat osobní informace společnosti GSK pro svůj vlastní komerční prospěch v jakékoli formě;

c) zavést a udržovat vhodná technická a organizační bezpečnostní opatření, mimo jiné včetně opatření uvedených v bezpečnostním plánu. Odkazy na „údaje společnosti GSK" v bezpečnostním plánu zahrnují osobní informace společnosti GSK;

d) uchovávat osobní informace společnosti GSK v důvěrnosti v souladu s podmínkami tohoto plánu a odkazy na důvěrné informace společnosti GSK v tomto plánu a v bezpečnostním plánu zahrnují osobní informace společnosti GSK;

e) uložit povinnosti k zachování důvěrnosti rovnocenné s povinnostmi stanovenými touto smlouvou příslušnému personálu, který má přístup k osobním informacím společnosti GSK;

f) nezapojit jiného zpracovatele („**dílčího zpracovatele"**) bez předchozího písemného schválení společnosti GSK (a pro tyto účely společnosti GSK uděluje souhlas s následujícími kategoriemi dílčích zpracovatelů: poskytovatelé služeb hostingové infrastruktury, použití individuálních dodavatelů a dílčí zpracovatelé, kteří jsou společnosti GSK oznámeni v době uzavření smlouvy) a předávat osobní informace společnosti GSK takovým schváleným dílčím zpracovatelům pouze na základě písemné smlouvy, která je zavazuje ke stejným povinostem, jako jsou ty uvedené v tomto plánu. Zapojí-li dodavatel dílčího zpracovatele v souladu s tímto ustanovením 2 písm. f), zůstává i nadále odpovědným za jednání a opomenutí dílčího zpracovatele;

g) poskytovat společnosti GSK přiměřenou součinnost při (i) provádění zákonem požadovaných posouzení vlivu na ochranu osbních údajů a/nebo posouzení vlivu předávání na ochranu osobních údajů; (ii) dodržování práv subjektů údajů a (iii) reagování na žádosti dozorových úřadů ve vztahu k osobním informacím společnosti GSK;

h) neprodleně vyrozumět společnost GSK poté, co se dozví o porušení zabezpečení osobních údajů ve vztahu k osobním informacím společnosti GSK a poskytnout společnosti GSK součinnost ve vztahu k tomuto porušení;

i) neprodleně vyrozumět společnosti GSK, jestliže obdrží písemnou žádost od (i) subjektu údajů o uplatnění práv týkající se osobních informací společnosti GSK podle zákonů na ochranu osobních údajů nebo (ii) nebo dozorového úřadu ve vztahu ke zpracování osobních informací společnosti GSK;

j) není-li ve smlouvě uvedeno jinak, vrátit nebo zničit veškeré osobní informace společnosti GSK, která má ve svém držení nebo správě (včetně osobních informací společnosti GSK zpracovávaných schválenými dílčími zpracovateli), v důsledku ukončení nebo vypršení platnosti smlouvy;

k) na písemnou žádost společnosti GSK poskytnout společnosti GSK informace nezbytné k prokázání dodržování tohoto plánu, což může zahrnovat i dostupné zprávy o bezpečnostním auditu třetích stran.

Podmínky správce

V případě, že dodavatel vystupuje jako správce osobních informací společnosti GSK podle příslušných zákonů na ochranu osobních údajů, platí následující podmínky:

1. Každá ze stran vystupuje jako nezávislý správce údajů a bude dodržovat povinnosti, které se na ni vztahují podle platných zákonů na ochranu osobních údajů. Společnost GSK a dodavatel souhlasí s tím, že ve vztahu k osobním údajům zpracovávaným podle tohoto plánu pro účely CCPA není dodavatelem poskytována peněžitá ani jiná protihodnota výměnou za osobní informace společnosti GSK, a tudíž společnost GSK neprodává osobní informace společnosti GSK dodavateli, jak je definováno CCPA.

2. Obdrží-li dodavatel sdělení ze strany dozorového úřadu týkající se přímo nebo nepřímo (a) zpracování osobních informací společnosti GSK dodavatelem nebo (b) potenciálního nedodržení zákonů na ochranu osobních údajů týkajícího se zpracování osobních informací společnosti GSK, dodavatel v rozsahu povoleném platnými zákony neprodleně postoupí toto sdělení společnosti GSK a poskytne společnosti GSK přiměřenou spolupráci a součinnost v souvislosti s tímto sdělením.

3. Vznese-li subjekt údajů písemnou žádost za účelem uplatnění práv podle zákonů na ochranu osobních údajů týkající se osobních informací společnosti GSK, strana, která žádost obdrží, odpoví na tuto žádost v souladu se zákony na ochranu osobních údajů. V rozsahu, v jakém se žádost týká zpracování osobních informací společnosti GSK prováděných jinou stranou, strana, která žádost obdrží: (i) okamžitě a neprodleně žádost postoupí druhé straně a (ii) bude spolupracovat a poskytne přiměřenou součinnost v souvislosti s touto žádostí, aby umožnila druhé straně reagovat v souladu se zákony na ochranu osobních údajů.

4. Aniž by tím došlo k omezení ustanovení bezpečnostního plánu, dozví-li se dodavatel o porušení zabezpečení osobních údajů, která má dopad na osobní informace společnosti GSK, pak (a) okamžitě vyrozumí společnost GSK a poskytne jí přiměřený popis porušení a (b) nezveřejní sdělení týkající se porušení bez předchozí konzultace se společností GSK, s tím, že o porušení smí vyrozumět dozorový úřad v rozsahu požadovaném platými zákony na ochranu osobních údajů.

Mezinárodní předávání osobních údajů

Pokud společnost GSK vystupující jako vývozce údajů předává osobní informace společnosti GSK dodavateli vystupujícímu jako dovozce údajů způsobem, který představuje omezené mezinárodní předávání osobních údajů podle zákonů na ochranu osobních údajů, obě strany tímto uzavírají a budou se řídit vzorovými doložkami, které se vztahují na vztah mezi stranami:

- Příloha k prováděcímu rozhodnutí Komise o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízeni (EU) 2016/679 Evropského parlamentu a Rady („**příloha**“) společně s MODULEM JEDNA: Předávání správcem správci (dostupné **zde**) a začleněná do tohoto dokumentu odkazem v aktualizovaném znění, změněném, zrušeném nebo nahrazeném Evropskou komisí; a/nebo (ii) odpovídající nebo rovnocenná smlouva o mezinárodním předávání osobních údajů nebo dodatek ke vzorovým doložkám přijatým dozorovým úřadem ve Spojeném království („**vzorové doložky C2C**“);
- Příloha společně s MODULEM DVĚ: Předávání správcem zpracovateli (dostupné **zde**) a začleněná do tohoto dokumentu odkazem v aktualizovaném znění, změněném, zrušeném nebo nahrazeném Evropskou komisí; a/nebo (ii) odpovídající nebo rovnocenná smlouva o mezinárodním předávání osobních údajů nebo dodatek ke vzorovým doložkám přijatým dozorovým úřadem ve Spojeném království („**vzorové doložky C2P**“);

„**Vzorové doložky**“ označují přílohu spolu se vzorovými doložkami C2C a C2P.

Pro účely vzorových doložek strany souhlasí s tím, že:

- Varianta v hranatých závorkách doložky 11 „Prostředek napravy“ se nepoužije
- Varianta jedna je zvolena pro doložku 17 „Rozhodné právo“ a použije se právo Irska.
- Soudy Irska budou příslušné podle doložky 18 „Výběr místa a příslušnost“.

Pro účely příslušných vzorových doložek C2P a C2C vezměte prosím na vědomí následující:

- Příloha 1 (vývozce a dovozce): Společnost GSK nebo příslušní příjemci služeb společnosti GSK nacházející se v EU a/nebo Spojeném království podle smlouvy (smluv) s dodavatelem je vývozcem údajů ve vztahu k osobním informacím společnosti GSK. Dodavatel je dovozcem údajů ve vztahu k osobním informacím společnosti GSK
- Příloha 1 (Popis předávání): viz definici osobních informací a služeb poskytovaných dovozcem. Citlivé údaje nejsou předávány. Četnost předávání je nepřetržitá. Povaha činností zpracování a účely zpracování jsou stanoveny ve smlouvě (smlouvách) s dodavatelem. Údaje budou uchovávány v souladu se směrnicemi o uchovávání údajů vývozce údajů.

- Příloha 1 (Příslušné úřady): jak je uvedeno v doložce 13 vzorových doložek C2Ca C2P
- Příloha 2 (Technická a organizační opatření): viz bezpečnostní opatření uvedená níže

Strany souhlasí, že varianta 2 doložky 9 „Použití dílčích zpracovatelů“ vzorových doložek C-P platí, pokud dodavatel zapojí dílčího zpracovatele a dodavatel a dílčí zpracovatel souhlasí s dodržováním **vzorových doložek P-P**, což znamená (i) přílohu společně s MODULEM TŘI: Předávání zpracovatelem zpracovateli (dostupné **zde**) a začleněnou do tohoto dokumentu odkazem v aktualizovaném znění, změněném, zrušeném nebo nahrazeném Evropskou komisí; a/nebo (ii) odpovídající nebo rovnocennou smlouvu o mezinárodním předávání osobních údajů nebo dodatek ke vzorovým doložkám přijatým dozorovým úřadem ve Spojeném království;

V případě, že se dodavatel domnívá, že není schopen dodržet požadavky přiměřeně stanovené společností GSK, dodavatel o této neschopnosti neprodleně společnost GSK vyrozumí a společnost GSK má právo smlouvu ukončit.

Strany souhlasí, že uzavřené vzorové doložky jsou účinné v zemích mimo prostor EHP, pokud: (i) jejich ustanovení jsou považována za poskytující dostatečnou ochranu ve vztahu k mezinárodním předáváním osobních údajů do zemí neposkytujících dostatečnou ochranu nebo (ii) zákony na ochranu osobních údajů požadují existenci smluvních ustanovení za účelem ochrany mezinárodních předávání osobních údajů. Při výkladu vzorových doložek v těchto zemích odkaz na výraz „členský stát, kde se nachází vývozce údajů“ bude vykládán tak, že označuje země, kde se nachází subjekt společnosti GSK; a odkaz na nařízení (EU) 2016/679 je odkazem na právní předpisy země, kde se společnost GSK nachází mimo prostor EHP. Odkaz na „zemi poskytující přiměřenou ochranu“ označuje zemi, která je považována za poskytující, nebo která jinak poskytuje, rovnocennou úroveň ochrany pro účely platných zákonů na ochranu osobních údajů v zemích mimo EHP, kde se vzorové doložky vztahují na předávání osobních údajů.

Bezpečnostní opatření

„Údaje společnosti GSK“ znamenají údaje nebo informace poskytnuté společností GSK nebo jejím jménem nebo obdržené dodavatelem nebo personálem dodavatele ve spojení s projednáváním nebo podpisem smlouvy nebo plněním povinností dodavatele podle této smlouvy, včetně takových údajů a informací, které jsou: (i) vytvořeny, vygenerovány, shromážděny nebo zpracovávány personálem dodavatele při plnění povinností dodavatele podle této smlouvy nebo (ii) se nachází v informačních systémech společnosti GSK nebo informačních systémech dodavatele nebo je k nim získáván přístup jejich prostřednictvím, jakož i údaje a informace z nich odvozené.

„**Zpracování**“ znamená operaci nebo sadu operací, které jsou prováděny s informacemi nebo údaji, ať už automatizovaně nebo neautomatizovaně, jako je sbírání, zaznamenávání, organizování, strukturování, ukládání, přizpůsobování nebo upravování, vyhledávání, konzultování, používání, sdělování přenosem, rozšiřování nebo jiné metody zpřístupňování, seřazování nebo kombinování, omezování, odstraňování nebo zničení.

„Prostředí dodavatele“ znamená kombinaci hardwaru, softwaru, operačních systémů, databázových systémů, nástrojů a síťových komponentů používaných dodavatelem nebo jeho jménem za účelem obdžení, uchovávání, zpracováví, uložení, přístupu nebo přenosu údajů společnosti GSK.

„Personál dodavatele“ znamená veškerý personál zapojený nebo zaměstnaný dodavatelem nebo jeho subdodavateli k plnění části služeb.

Bezpečnostní plán je součástí smlouvy mezi společností GSK a dodavatelem. V případě rozporu mezi podmínkami tohoto bezpečnostního plánu a podmínkami smlouvy ve vztahu ke kybernetické bezpečnosti, má přednost tento bezpečnostní plán. Výrazy psané s počátečními velkými písmeny, které nejsou definovány v tomto bezpečnostním plánu, mají význam, který je jim udělený v ostatních částech smlouvy.

1. Odpovědnosti. Dodavatel bude: (a) používat silné průmyslové šifrovací kontroly AES 256 pro ochranu veškerých údajů společnosti GSK před nepovolaným zpřístupněním, přístupem nebo změnami během přepravy do nebo z prostředí dodavatele přes sítě třetí strany; (b) udržovat kontrolní postupy dle osvědčených postupů v rámci odvětví k detekci, prevenci a regenerování postup malwaru, virů a spywaru, včetně pravidelných aktualizací antivirových, anti-malwarových a anti-spywarových softwarů; (c) spravovat směrnice týkající se správy přístupu, procedůr a technické kontroly dle osvědčených postupů v rámci odvětví za účelem zajištění, že veškerý přístup k údajům společnosti GSK v jeho správě je řádně autorizovaný.

2. Porušení bezpečnosti. Dodavatel nahlásí společnosti GSK e-mailem na adresu cstd@gsk.com veškeré případy nezákonného použití, ztráty, zničení, zpřístupnění, přístupu, poškození, modifikace, prodeje, pronajmutí nebo jiného zpracování údajů společnosti GSK („**porušení bezpečnosti**“) do čtyřiadvaceti (24) hodin od ověření dodavatelem. Dodavatel zajistí, že všechny bezpečnostní incidenty týkající se údajů společnosti GSK jsou řízeny dle vhodných postupů reakce na incidenty a bude se společností GSK spolupracovat v dobré víře k identifikaci hlavní příčiny a nápravě porušení bezpečnosti.

SCHEMA

VOORWAARDEN MET BETREKKING TOT GEGEVENSBESCHERMING – ELEMENTAIRE PERSOONLIJKE INFORMATIE

Gedekte gelieerde onderneming betekent: elke Gelieerde onderneming van GSK die van de Diensten van een derde gebruikmaakt (een lijst daarvan wordt op verzoek door GSK aan de Leverancier verstrekt). Een Gelieerde onderneming is een rechtspersoon die, met betrekking tot een andere rechtspersoon, onder zeggenschap staat van die andere rechtspersoon, onder gemeenschappelijke zeggenschap staat, of over die andere rechtspersoon zeggenschap heeft. "Zeggenschap" en daarvan afgeleide begrippen verwijzen naar de eigendom (rechtstreeks of onrechtstreeks) van een meerderheid van de stemgerechtigde aandelen van een dergelijke rechtspersoon of bestaat in het vermogen (rechtstreeks of onrechtstreeks) om een meerderheid van de bestuurders van een dergelijke rechtspersoon aan te wijzen of de bevoegdheid om de directie of de beleidslijnen van een dergelijke rechtspersoon aan te sturen, contractueel of anderszins;

Wetgeving inzake gegevensbescherming betekent: (a) de Algemene verordening gegevensbescherming (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en alle toepasselijke wet- en/of regelgeving die deze ten uitvoer legt en/of uitzonderingen daarop uitoefent en/of deze vervangt of ten opzichte ervan voorrang heeft (**AVG**); en (b) de GDPR zoals opgesteld door de Britse de Data Protection Act 2018; (c) de California Consumer Privacy Act van 2018 (Cal. Civ. Code 1798.100 - 1798.199) (**CCPA**); en (d) alle andere wetten met betrekking tot de verwerking van persoonsgegevens.

Persoonlijke informatie verwijst naar persoonsgegevens behorende tot het volgende type: voornaam en/of achternaam, initialen, werkcontactgegevens, groepslidmaatschappen, netwerk- of gebruikersidentificatienummer, inloggegevens, werkgeschiedenis en vaardigheden, geslacht of titel, aanwezigheid bij evenementen door GSK-werknemers en aanvullende werknemers die gebruik maken van de Diensten.

Persoonlijke informatie van GSK verwijst naar alle Persoonlijke informatie die: (i) door of namens GSK aan de Leverancier worden verstrekt (inclusief wanneer de Leverancier toegang heeft tot Persoonlijke informatie die door GSK of namens haar wordt bewaard), of die de Leverancier namens GSK verzamelt of genereert; (ii) door de Leverancier wordt verwerkt onder of in verband met deze Overeenkomst; en (iii) ten aanzien waarvan GSK een verwerkingsverantwoordelijke of eigenaar (of gelijkwaardig) is;

Beveiligingsschema betekent *de cyberbeveiligingsschema die bij deze als Bijlage 1 is bijgevoegd*.

De termen **verwerkingsverantwoordelijke, gegevensbeschermingseffectbeoordeling, betrokkene, persoonsgegevens, inbreuk op persoonsgegevens, verwerker, verwerking, dienstverlener** en **toezichthouder** hebben de betekenis die daar in het kader van de relevante wetgeving inzake gegevensbescherming aan gegeven wordt. Verwijzingen naar GSK verwijzen naar de aanbestedende GSK-rechtspersoon die in de Overeenkomst wordt gebruikt, evenals naar Gedekte gelieerde ondernemingen.

Voorwaarden voor verwerkers

Ingeval de leverancier als een verwerker van Persoonlijke informatie van GSK handelt krachtens de relevante wetgeving inzake gegevensbescherming, zijn de volgende voorwaarden van toepassing:

1. Elke partij is gehouden aan haar verplichtingen te voldoen uit hoofde van de toepasselijke wetgeving inzake gegevensbescherming. GSK en de Leverancier gaan ermee akkoord dat met betrekking tot de Persoonlijke informatie van GSK die krachtens deze Overeenkomst wordt verwerkt, GSK de verwerkingsverantwoordelijke zal zijn en de Leverancier de verwerker. In het kader van de CCPA is de Leverancier een dienstverlener aan GSK en mag de Leverancier de Persoonlijke informatie van GSK alleen verwerken voor de door GSK daarmee nagestreefde doelen overeenkomstig dit Schema, onder voorwaarde dat er geen geldelijke vergoeding wordt verstrekt door, of andersoortige vermogensoverdracht plaatsvindt zijdens, de Leverancier aan GSK en GSK derhalve geen Persoonlijke informatie van GSK aan de Leverancier verkoopt in de zin van het in de CCPA bepaalde.

2. De Leverancier is gehouden aan naleving van het volgende met betrekking tot de Persoonlijke informatie van GSK:

a) de Persoonlijke informatie van GSK mag alleen worden verwerkt uit hoofde van rechtsgeldige schriftelijke instructies afkomstig van GSK en uitsluitend met de levering van diensten door de Leverancier aan GSK krachtens deze Overeenkomst als doel, voor de duur van de Overeenkomst of een in de Overeenkomst vermelde, aanvullende periode, indien van toepassing;

b) noch de Leverancier, noch een van zijn werknemers, lasthebbers, consultants of rechtverkrijgenden heeft het recht om de Persoonlijke informatie van GSK in welke vorm dan ook te verwerken met als doel, deze zelf commercieel te exploiteren;

c) er moeten passende technische en organisatorische beveiligingsmaatregelen worden geïmplementeerd en gehandhaafd, inclusief maar niet beperkt tot de maatregelen die in het Beveiligingsschema zijn uiteengezet. Verwijzingen in het Beveiligingsschema naar "Gegevens van GSK" verwijzen tevens naar Persoonlijke informatie van GSK;

d) de vertrouwelijkheid van de Persoonlijke informatie van GSK moet worden bewaard in overeenstemming met de in dit Schema uiteengezette voorwaarden en alle verwijzingen naar de Vertrouwelijke informatie van GSK in het Schema en het Beveiligingsschema verwijzen tevens naar de Persoonlijke informatie van GSK;

e) er moeten geheimhoudingsverplichtingen worden opgelegd die gelijkwaardig zijn aan de in de Overeenkomst uiteengezette verplichtingen voor relevant personeel dat toegang heeft tot Persoonlijke informatie van GSK;

f) er mag generlei andere verwerker in dienst worden genomen ("**subverwerker**") zonder de voorafgaandelijke schriftelijke toestemming van GSK (en in dat kader geeft GSK aan in te stemmen met de volgende categorieën van subverwerkers: dienstverleners op het gebied van de hostinginfrastructuur, individuele contractanten en aan GSK bekendgemaakte subcontractanten op het moment dat de Overeenkomst wordt aangegaan) en Persoonlijke informatie van GSK mag alleen aan dergelijke goedgekeurde subverwerkers worden overgedragen op grond van een schriftelijke overeenkomst die verplichtingen oplegt die met de in dit Schema uiteengezette in

overeenstemming zijn. Wanneer de Leverancier in overeenstemming met deze clausule 2(f) een subverwerker aanwijst, blijft hij voor de handelingen en nalatigheden van de subverwerker aansprakelijk;

g) aan GSK moet redelijke ondersteuning worden geboden bij (i) het uitvoeren van wettelijk vereiste gegevensbeschermingseffectbeoordelingen en/of gegevensoverdrachteffectbeoordelingen, (ii) het naleven van de rechten van betrokkenen en (iii) het reageren op verzoeken van toezichthouders met betrekking tot Persoonlijke informatie van GSK;

h) GSK moet er onmiddellijk op de hoogte worden gesteld als u kennis hebt genomen van een inbreuk in verband met persoonsgegevens die tot Persoonlijke informatie van GSK enige betrekking hebben en GSK in verband met een dergelijke inbreuk ondersteuning bieden;

i) GSK er onverwijld van op de hoogte stellen als hij een schriftelijk verzoek ontvangt van (i) een betrokkene tot uitoefening van zijn/haar rechten met betrekking tot de Persoonlijke informatie van GSK krachtens de wetgeving inzake gegevensbescherming, of (ii) een toezichthouder met betrekking tot de verwerking van Persoonlijke informatie van GSK;

j) tenzij anderszins bepaald in de Overeenkomst, alle Persoonlijke informatie van GSK die de Leverancier in zijn bezit heeft of die onder zijn zeggenschap valt (met inbegrip van alle Persoonlijke informatie van GSK die door toegestane subverwerkers is verwerkt) bij beëindiging of afloop van de Overeenkomst te retourneren of te vernietigen; en

k) op schriftelijk verzoek van GSK, aan GSK redelijke informatie verstrekken die nodig is om aan te tonen dat dit Schema wordt nageleefd, met inbegrip van eventueel beschikbare beveiligingsgerelateerde auditverslagen van derden.

Voorwaarden voor verwerkingsverantwoordelijken

Ingeval de leverancier als verwerkingsverantwoordelijke van Persoonlijke informatie van GSK handelt krachtens de relevante wetgeving inzake gegevensbescherming, zijn de volgende voorwaarden van toepassing:

1. Elke partij handelt als onafhankelijke verwerkingsverantwoordelijke en is gehouden aan haar verplichtingen te voldoen uit hoofde van de toepasselijke wetgeving inzake gegevensbescherming. GSK en de Leverancier gaan ermee akkoord dat, met betrekking tot de persoonsgegevens die uit hoofde van dit Schema worden verwerkt, er in de zin van de CCPA geen geldelijke vergoeding wordt verstrekt door, of andersoortige vermogensoverdracht plaatsvindt zijdens, de Leverancier aan GSK in ruil voor de Persoonlijke informatie van GSK en GSK derhalve geen Persoonlijke informatie van GSK aan de Leverancier verkoopt in de zin van het in de CCPA bepaalde.

2. Als de Leverancier enigerlei communicatie ontvangt van een toezichthouder die rechtstreeks of onrechtstreeks verband houdt met a) de verwerking door de Leverancier van Persoonlijke informatie van GSK of (b) een mogelijk verzuim om te voldoen aan de wetgeving inzake gegevensbescherming met betrekking tot de verwerking van Persoonlijke informatie van GSK, is de Leverancier gehouden, voor zover toegestaan door de toepasselijke wetgeving, de communicatie onmiddellijk door te sturen naar GSK en redelijke samenwerking en assistentie te verlenen aan GSK in verband daarmee.

3. Als een betrokkene een schriftelijk verzoek indient bij een van de partijen om gelijk welke van zijn/haar rechten uit hoofde van de wetgeving inzake gegevensbescherming uit te oefenen met betrekking tot de Persoonlijke informatie van GSK, is de ontvangende partij gehouden op dat verzoek te reageren op een wijze die in overeenstemming is met de wetgeving inzake gegevensbescherming. Voor zover het verzoek betrekking heeft op de verwerking van Persoonlijke informatie van GSK door de andere partij, is de ontvangende partij gehouden: (i) onmiddellijk en zonder onnodige vertraging het verzoek door te sturen naar de andere partij en (ii) samen te werken en redelijke hulp te bieden in verband met dat verzoek om de andere partij in staat te stellen in overeenstemming met de wetgeving inzake gegevensbescherming te reageren.

4. Onverminderd de bepalingen van het Beveiligingsschema, is de Leverancier gehouden, nadat deze kennis heeft genomen van een inbreuk in verband met Persoonlijke informatie van GSK, (a) GSK onmiddellijk op de hoogte te stellen en aan GSK een redelijke beschrijving van de inbreuk te verstrekken en (b) generlei communicatie met betrekking tot de inbreuk te publiceren zonder eerst contact op te nemen met GSK, tenzij de Leverancier verplicht is tot melding van de inbreuk aan een toezichthouder krachtens de toepasselijke wetgeving inzake gegevensbescherming.

Internationale gegevensoverdracht

Wanneer GSK, in de hoedanigheid van gegevensexporteur, Persoonlijke informatie van GSK aan de Leverancier overdraagt, in de hoedanigheid van gegevensimporteur, op een manier die krachtens de toepasselijke wetgeving inzake gegevensbescherming een beperkte internationale gegevensoverdracht vormt, gaan beide partijen hierbij de toepasselijke, op de relatie tussen de partijen betrekking hebbende modelcontractbepalingen aan en verbinden ze zich tot naleving daarvan:

- Het Aanhangsel bij het uitvoeringsbesluit van de Commissie inzake modelcontractbepalingen met betrekking tot de overdracht van persoonsgegevens aan derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad ("**Aanhangsel**") in combinatie met MODULE ÉÉN: Overdracht van verwerkingsverantwoordelijke aan verwerkingsverantwoordelijke (**hier beschikbaar**) en in dit Aanhangsel door middel van verwijzing opgenomen, zoals van tijd tot tijd bijgewerkt, gewijzigd of vervangen door de Europese Commissie, en/of (ii) elk(e) overeenkomstig(e) of gelijkwaardig(e) overeenkomst of addendum met betrekking tot de internationale overdracht van gegevens bij de modelcontractbepalingen die door de toezichthouder in het Verenigd Koninkrijk overgenomen zijn ("**C2C-modelcontractbepalingen**");

- Het aanhangsel bij MODULE TWEE: Overdracht van verwerkingsverantwoordelijke aan verwerker (**hier** beschikbaar) en in dit Aanhangsel door middel van verwijzing opgenomen, zoals van tijd tot tijd bijgewerkt, gewijzigd of vervangen door de Europese Commissie, en/of (ii) elk(e) overeenkomstig(e) of gelijkwaardig(e) overeenkomst of addendum met betrekking tot de internationale overdracht van gegevens bij de modelcontractbepalingen die door de toezichthouder in het Verenigd Koninkrijk overgenomen zijn ("**C2P-modelcontractbepalingen**");

"**Modelcontractbepalingen**" betekent het Aanhangsel in combinatie met de C2C-modelcontractbepalingen en C2P-modelcontractbepalingen.

Met betrekking tot de Modelcontractbepalingen komen de partijen overeen dat:

- De optie tussen vierkante haakjes van Bepaling 11 "Verhaal" ("Redress") niet van toepassing is
- Optie één wordt geselecteerd wat betreft Bepaling 17 "Toepasselijk recht" ("Governing Law") en dat het Ierse recht van toepassing is.
- De rechtbanken van Ierland rechtsbevoegdheid hebben op grond van Bepaling 18 "Forumkeuze en rechterlijke bevoegdheid" ("Choice of Forum and Jurisdiction").

Met betrekking tot de toepasselijke C2P-modelcontractbepalingen en C2C-modelcontractbepalingen, dient het volgende in acht genomen te worden:

- Aanhangsel 1 (Exporteur en importeur): GSK of de desbetreffende GSK-dienstenontvangers in de Europese Unie en/of het Verenigd Koninkrijk krachtens de overeenkomst(en) met de Leverancier is/zijn een Gegevensexporteur met betrekking tot de Persoonlijke informatie van GSK. De Leverancier is een gegevensimporteur met betrekking tot de Persoonlijke informatie van GSK
- Aanhangsel 1 (Beschrijving van de overdrachten): zie de definitie van de Persoonlijke informatie en diensten die door de Importeur moeten worden verstrekt. Er worden geen gevoelige gegevens overgedragen. De frequentie van de overdracht is continu. De aard van de verwerkingsactiviteiten en de doeleinden van de overdracht worden uiteengezet in de overeenkomst(en) met de Leverancier. De gegevens worden bewaard in overeenstemming met het gegevensbewaarbeleid van de Gegevensexporteur.
- Aanhangsel 1 (Bevoegde autoriteiten): zoals uiteengezet in Bepaling 13 van de C2C-modelcontractbepalingen en C2P-modelcontractbepalingen
- Aanhangsel 2 (Technische en organisatorische maatregelen): zie de hieronder uiteengezette Beveiligingsmaatregelen

De partijen komen overeen dat optie 2 van Bepaling 9 "Gebruik van subverwerkers" ("Use of Sub-Processors") van de C-P-modelcontractbepalingen van toepassing is ingeval de Leverancier een subverwerker inschakelt en de Leverancier en subverwerker ermee instemmen aan de **P-P-modelcontractbepalingen** gebonden te zijn, wat betekent i) het Aanhangsel in combinatie met MODULE DRIE: Overdracht van verwerker aan verwerker (**hier** beschikbaar) en in dit Aanhangsel door middel van verwijzing opgenomen, zoals van tijd tot tijd bijgewerkt, gewijzigd of vervangen door de Europese Commissie, en/of (ii) elk(e) overeenkomstig(e) of gelijkwaardig(e) overeenkomst of addendum met betrekking tot de internationale overdracht van gegevens bij de modelcontractbepalingen die door de toezichthouder in het Verenigd Koninkrijk overgenomen zijn;

Ingeval de Leverancier van mening is dat hij niet kan voldoen aan de vereisten zoals redelijkerwijs door GSK uiteengezet, is de Leverancier gehouden GSK onmiddellijk op de hoogte te stellen van zijn onvermogen en heeft GSK het recht om de Overeenkomst te beëindigen.

De Partijen komen overeen dat de aangegane modelcontractbepalingen van kracht zullen zijn in landen buiten de Europese Economische Ruimte waar: (i) hun bepalingen erkend worden als passende waarborg met betrekking tot internationale overdrachten van Persoonsgegevens naar niet-adequate landen of (ii) de Wetgeving inzake gegevensbescherming het bestaan van contractuele bepalingen verplicht stelt ter bescherming van internationale overdrachten van Persoonsgegevens. Bij de interpretatie van de modelcontractbepalingen wordt in die landen elke verwijzing naar de term "Lidstaat waarin de gegevensexporteur is gevestigd" geïnterpreteerd als het land waarin de GSK-rechtspersoon is gevestigd, waarbij geldt dat elke verwijzing naar Verordening (EU) 2016/679 betrekking heeft op de dienovereenkomstige wet van het land waarin GSK buiten de EER gevestigd is. Elke verwijzing naar een "Adequaat land" verwijst naar om het even welk land dat wordt geacht een gelijkwaardig niveau van bescherming te bieden, of anderszins een gelijkwaardig beschermingsniveau biedt, in de zin van de toepasselijke wetgeving inzake gegevensbescherming, in die landen buiten de Europese Economische Ruimte waarin de modelcontractbepalingen op de overdracht van Persoonsgegevens van toepassing moeten zijn.

Beveiligingsmaatregelen

"Gegevens van GSK" betekent alle gegevens of informatie die worden/wordt verstrekt door of namens GSK of verkregen door de Leverancier of het Personeel van de Leverancier in verband met de onderhandeling en uitvoering van de Overeenkomst of de uitvoering van de verplichtingen van de Leverancier krachtens de Overeenkomst, met inbegrip van gegevens en informatie die: (i) worden/wordt aangemaakt, gegenereerd, verzameld of verwerkt door het personeel van de Leverancier bij de voltooiing van de verplichtingen van de Leverancier uit hoofde van de Overeenkomst, of (ii) zich bevindt in of wordt geopend via de informatiesystemen van GSK of informatiesystemen van leveranciers, evenals alle gegevens en informatie die van het voorgaande zijn afgeleid.

"**Verwerking**" betekent elke bewerking of elk geheel van bewerkingen met betrekking tot informatie of gegevens, al dan niet uitgevoerd met behulp van geautomatiseerde verwerking, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het beperken, wissen of vernietigen.

"Leveranciersomgeving" betekent de combinatie van hardware, software, besturingssystemen, databasesystemen, tools en netwerkcomponenten die door of namens de Leverancier worden gebruikt om Gegevens van GSK te ontvangen, te onderhouden, te verwerken, op te slaan, te openen of te verzenden.

"Personeel van de Leverancier" betekent al het personeel dat door de Leverancier en zijn Onderaannemers wordt ingehuurd of in dienst genomen om een deel van de Diensten uit te voeren.

Dit Beveiligingsschema maakt deel uit van de Overeenkomst door en tussen GSK en de Leverancier. In het geval van een conflict met betrekking

tot cyberbeveiliging tussen de voorwaarden van dit Beveiligingsschema en de voorwaarden van de Overeenkomst, krijgt dit Beveiligingsschema voorrang. Termen met een hoofdletter die niet in dit Beveiligingsschema zijn gedefinieerd, hebben de betekenis die er in andere delen van de Overeenkomst aan wordt toegekend.

1. Verantwoordelijkheden. De Leverancier is gehouden: (a) versleutelingscontroles te gebruiken om alle Gegevens van GSK te beschermen tegen ongeautoriseerde openbaarmaking, toegang of wijziging tijdens de doorvoer naar of vanuit de Omgeving van de Leverancier via netwerken van derden, (b) controleprocessen te onderhouden in overeenstemming met de beste praktijken in de sector om malware, virussen en spyware op te sporen en infectie ermee te voorkomen, alsmede om systemen ervan te herstellen, met inbegrip van het regelmatig updaten van antivirus-, anti-malware- en anti-spyware-software en (c) beleidslijnen, procedures en technische controles voor toegangsbeheer te onderhouden in overeenstemming met de beste praktijken in de sector om ervoor te zorgen dat alle toegang tot Gegevens van GSK in zijn beheer op de juiste wijze is geautoriseerd.

2. Inbreuk op de beveiliging. De Leverancier doet binnen vierentwintig (24) uur na verificatie zijdens de Leverancier per e-mail aan GSK, gericht aan het adres cstd@gsk.com, melding van om het even welk(e) geverifieerd(e) accidente(e)l(e), ongeautoriseerd(e) of onwettig(e) gebruik, verlies, vernietiging, openbaarmaking, toegang, corruptie, wijziging, verkoop, verhuur of andersoortige Verwerking van Gegevens van GSK (een "**Inbreuk op de beveiliging**"). De Leverancier zal ervoor zorgen dat alle beveiligingsincidenten waarbij Gegevens van GSK betrokken zijn, worden beheerd in overeenstemming met de toepasselijke procedures voor respons op incidenten en de Leverancier is gehouden te goeder trouw samen te werken met GSK om een onderliggende oorzaak vast te stellen en de Inbreuk op de beveiliging te verhelpen.

ANNEXE

PROTECTION DES DONNÉES A CARACTERE PERSONNEL

INFORMATIONS PERSONNELLES BASIQUES

Les Parties conviennent que le traitement des Informations personnelles en vertu du présent Contrat ou en rapport avec celui-ci sera conforme à la présente Annexe.

DEFINITIONS

« Information personnelle » désigne : toute donnée à caractère personnel telle que : le prénom et/ou le nom, les initiales, les coordonnées professionnelles, les adhésions à des groupes, le numéro d'identification du réseau ou de l'utilisateur, les identifiants de connexion, les antécédents professionnels et les compétences, le sexe ou le titre, la participation à des événements des employés de GSK et des travailleurs complémentaires utilisant les Services.

« Information personnelle de GSK » :désigne toute Information personnelle *:* utilisée aux fins des Biens et/ou Services qui est fournie par ou pour le compte de GSK au Fournisseur (y compris lorsque le Fournisseur a accès aux données personnelles détenues par GSK ou pour son compte), ou que le Fournisseur recueille ou génère pour le compte de GSK, qui est traitée par le Fournisseur en vertu du présent Contrat ou en rapport avec celui-ci, et au titre de laquelle GSK est responsable ou propriétaire (ou équivalent). Dans le Contrat et l'Annexe sur la sécurité de l'information, les références aux Informations confidentielles de GSK ou aux Données de GSK incluent les Informations personnelles de GSK.

« Législation en matière de protection des données » désigne : (a) le Règlement Général sur la Protection des Données (UE) n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) ainsi que toute loi ou réglementation applicable qui met en œuvre et/ou exerce des dérogations, remplace ou supplante le RGPD (RGPD) ; (b) la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés; (c) le RGPD UK tel qu'adapté par la loi britannique de 2018 sur la protection des données personnelles, la loi californienne de 2018 sur la protection de la vie privée des consommateurs (Cal. Civ. Code 1798.100 – 1798.199 (CCPA) (d) toutes les autres lois concernant le traitement d'informations à caractère personnel.

« Plan de sécurité » désigne : l'annexe sécurité de l'information jointes aux présentes en tant qu'Annexe 1.

Société Affiliée concernée désigne : chaque Société Affiliée de GSK qui bénéficie des Biens et/ou Services en tant que tiers (dont la liste sera fournie par GSK au Fournisseur sur demande). Une Société Affiliée est toute entité qui, à l'égard de toute autre entité, est contrôlée par, sous contrôle commun ou contrôle cette autre entité. **Contrôle** et ses dérivés signifient la propriété (directe ou indirecte) de la majorité des actions avec droit de vote de cette entité ou est la capacité (directe ou indirecte) de nommer la majorité des administrateurs de cette entité ou l'autorité qui dirige la gestion ou les politiques de cette entité, par contrat ou autrement.

Les termes **« responsable du traitement », « analyse d'impact relative à la protection des données », « personne(s) concernée(s) », « données à caractère personnel », « violation de données à caractère personnel », « sous-traitant », « traitement », « prestataire de services »** et **« autorité de contrôle concernée »** sont définis conformément à la Législation en matière de protection des données applicable. Toute référence à GSK désigne l'entité contractante GSK partie au Contrat, ainsi que les Sociétés Affiliées concernées.

DISPOSITIONS RELATIVES AU SOUS-TRAITANT DES DONNEES

Dans l'éventualité où le Fournisseur agit comme sous-traitant des Informations personnelles de GSK conformément à la Législation en matière de protection des données applicable, les dispositions suivantes s'appliquent :

1. Chaque Partie doit se conformer à ses obligations en vertu de la Législation en matière de protection des données applicable. GSK et le Fournisseur reconnaissent, en ce qui concerne les Informations personnelles de GSK traitées dans le cadre du Contrat, que GSK est le Responsable du traitement et le Fournisseur est le Sous-traitant. Aux fins du CCPA, le Fournisseur est un prestaire de services pour GSK et le traitement Informations personnelles de GSK par le Fournisseur ne sera effectué que pour les finalités déterminées par GSK conformément à la présente Annexe, qu'aucune contrepartie monétaire ou autre contrepartie de valeur n'est fournie par le Fournisseur à GSK et que, par conséquent, GSK ne vend pas les Informations personnelles de GSK au Fournisseur au sens du CCPA.
2. Le Fournisseur doit se conformer à ce qui suit en ce qui concerne les Informations personnelles de GSK :

a) traiter les Informations personnelles de GSK uniquement selon les instructions écrites légitimes de GSK et uniquement aux fins des Biens et/ou Services par le Fournisseur pour GSK en vertu du Contrat pour la durée du Contrat ou toute période supplémentaire indiquée dans le Contrat, le cas échéant ;

b) Ni le Fournisseur, ni aucun de ses employés, agents, consultants ou assignés ne doit traiter les Informations personnelles de GSK à leur propre avantage commercial sous quelque forme que ce soit ;

c) mettre en œuvre et maintenir des mesures de sécurité techniques et organisationnelles appropriées, incluant sans s'y limiter, les mesures énoncées dans le Plan de sécurité. Toute référence dans ce plan aux « Données GSK » inclut les Informations personnelles de GSK ;

d) garder confidentielles les Informations personnelles de GSK conformément à cette Annexe et au Plan de sécurité des informations confidentielles de GSK qui englobent les Informations personnelles de GSK ;

e) imposer des obligations de confidentialité équivalentes aux obligations prévues par le Contrat au personnel concerné ayant accès aux Informations personnelles de GSK ;

f) ne pas engager un sous-traitant (« sous-traitant ultérieur ») sans l'approbation écrite préalable de GSK (et à ces fins, GSK consent aux catégories suivantes de sous-traitants ultérieurs : les fournisseurs de services d'infrastructure d'hébergement, le recours à des entrepreneurs individuels et les sous-traitants ultérieurs portés à la connaissance de GSK au moment de la conclusion du Contrat) et ne transférer les Informations personnelles de GSK à ces sous-traitants ultérieurs approuvés qu'en vertu d'un contrat écrit qui impose des obligations conformes à celles énoncées dans la présente Annexe. Lorsque le Fournisseur désigne un sous-traitant ultérieur conformément à la présente clause 2(f), il demeure responsable des actes et omissions du sous-traitant ultérieur ;

g) fournir à GSK une assistance raisonnable pour (i) réaliser toute analyse d'impact sur la protection des données et/ou analyse d'impact sur le transfert des données exigées par la loi (ii) respecter les droits des personnes concernées ; et (iii) répondre aux demandes de toute autorité de contrôle concernant les Informations personnelles de GSK ;

h) informer GSK sans délai après avoir pris connaissance d'une violation des données personnelles concernant toute Information personnelle de GSK et fournir à GSK une assistance en rapport avec cette violation ;

i) informer GSK sans délai s'il reçoit une demande écrite (i) d'une personne concernée pour exercer l'un de ses droits en relation avec les Informations personnelles de GSK en vertu de la Législation sur la protection des données ; ou (ii) d'une autorité de contrôle en relation avec le traitement des Informations personnelles de GSK ;

j) sauf disposition contraire dans le Contrat, restituer ou détruire toutes les Informations personnelles de GSK en sa possession ou sous son contrôle (y compris les Informations personnelles de GSK traitées par des sous-traitants autorisés) à la résolution ou à l'expiration du Contrat; et

k) sur demande écrite de GSK, fournir à GSK les informations raisonnables nécessaires pour démontrer la conformité à la présente Annexe, ce qui peut inclure tout rapport d'audit de sécurité d'un tiers disponible.

DISPOSITIONS RELATIVES AU RESPONSABLE DU TRAITEMENT

Dans l'éventualité où le Fournisseur agit comme Responsable du traitement des Informations personnelles de GSK conformément à la Législation en matière de protection des données applicable, les dispositions suivantes s'appliquent :

1. Chaque Partie agit comme un Responsable du traitement indépendant et doit se conformer à ses obligations en vertu de la Législation en matière de protection des données applicable. GSK et le Fournisseur reconnaissent, en ce qui concerne les Informations personnelles de GSK traitées dans le cadre du Contrat, aux fins du CCPA, qu'aucune contrepartie monétaire ou autre contrepartie de valeur n'est fournie par le Fournisseur à GSK et que, par conséquent, GSK ne vend pas les Informations personnelles de GSK au Fournisseur au sens du CCPA.

2. Si le Fournisseur reçoit de la part d'une autorité de contrôle concernée une communication directement ou indirectement liée (a) au traitement par le Fournisseur des Informations personnelles de GSK ; ou (b) à un possible non-respect de la Législation en matière de protection des données en relation avec le traitement des Informations personnelles de GSK, le Fournisseur, dans la mesure où la loi applicable le permet, transmet sans délai cette communication à GSK, et coopère et assiste raisonnablement GSK en relation avec cette communication.

3. Si une personne concernée demande par écrit à l'une des Parties d'exercer l'un de ses droits en vertu de la Législation en matière de protection des données en rapport avec les Informations personnelles de GSK, la Partie destinataire de la demande y répond conformément aux dispositions de la Législation en matière de protection des données. Dans la mesure où la demande concerne le traitement d'Informations personnelles partagées par l'autre Partie, la Partie destinataire : (i) transmet rapidement et sans retard injustifié la demande à l'autre Partie, et (ii) coopère et fournit toute l'assistance raisonnable en lien avec cette demande pour permettre à l'autre Partie d'y répondre conformément à la Législation en matière de protection des données.

4. Sans préjudice des dispositions du Plan de sécurité, dès qu'il a connaissance d'une violation concernant les Informations personnelles de GSK, le Fournisseur doit (a) notifier promptement GSK et fournir à GSK une description raisonnable de la violation ; et (b) ne pas publier de communication concernant la violation sans consulter GSK au préalable, à l'exception d'une notification d'une violation à une autorité de contrôle dans la mesure requise par la Législation sur la protection des données applicable.

TRANSFERT INTERNATIONAUX DE DONNEES

Lorsque GSK, agissant en tant qu'exportateur de données, transfère des Informations personnelles GSK au Fournisseur, agissant en tant qu'importateur de données, d'une manière qui constitue un transfert international de données restreint en vertu de la Législation sur la protection des données applicable, les deux Parties conviennent de respecter les Clauses contractuelles types applicables couvrant la relation entre les Parties :

- L'annexe de la décision d'exécution de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil (ci-après l' « Annexe ») avec son MODULE 1 : transfert de responsable du traitement à responsable du traitement (disponible sur le site https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0914&from=FR) et intégrée aux présentes par référence, telle que mise à jour, modifiée, remplacée ou supprimée de temps à autre par la Commission européenne et/ou tout accord international de transfert de données correspondant ou équivalent aux Clauses contractuelles types adopté par l'autorité de contrôle au Royaume-Uni ou tout avenant à un tel accord (« Clauses contractuelles types de Responsable du traitement à Responsable du traitement ») ;
- L'Annexe avec son MODULE 2 : transfert de responsable du traitement à sous-traitant (disponible sur le site https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0914&from=FR) et incorporée ici par référence, telle que mise à jour, modifiée, remplacée ou supprimée de temps à autre par la Commission européenne et/ou tout accord international de transfert de données correspondant ou équivalent aux Clauses contractuelles types adopté par l'autorité de contrôle au Royaume-Uni ou tout avenant à un tel accord (« Clauses contractuelles types de Responsable du traitement à Sous-traitant »).

« Clauses contractuelles types » désigne l'Annexe ainsi que les Clauses contractuelles types de Responsable du traitement à Responsable du traitement et les Clauses contractuelles types de Responsable du traitement à Sous-traitant.

Aux fins des Clauses contractuelles types, les Parties conviennent de ce qui suit :

- L'option entre crochets de la clause 11 « Voie de recours » ne s'applique pas.
- L'option 1 est sélectionnée pour la clause 17 « Droit Applicable » et le droit français s'applique.
- Les tribunaux français seront compétents en vertu de la clause 18 « Election de for et juridiction ».

Aux fins des Clauses contractuelles types de Responsable du traitement à Responsable du traitement et des Clauses contractuelles types de Responsable du traitement à Sous-traitant applicables, veuillez noter ce qui suit :

- Annexe 1 (Exportateur et Importateur): GSK ou les bénéficiaires concernés de GSK des Biens et/ou Services situés dans l'UE et/ou au Royaume-Uni dans le cadre du Contrat avec le Fournisseur est un Exportateur de données en ce qui concerne les Informations personnelles GSK. Le Fournisseur est un Importateur de données en ce qui concerne les Informations personnelles GSK.
- Annexe 1 (Description des transferts) :veuillez consulter la définition d'Information personnelle et les Biens et/ ou Services devant être réalisées par l'Importateur. Aucune donnée sensible n'est transférée. La fréquence du transfert est continue. La nature des activités de traitement et les objectifs du transfert sont définis dans le ou les contrats conclus avec le Fournisseur. Les données seront conservées conformément aux politiques de conservation des données de l'Exportateur de données.
- Annexe 1 (Autorité de contrôle compétente) : comme indiqué à la clause 13 des Clauses contractuelles types de Responsable du traitement à un Responsable du traitement et des Clauses contractuelles types de Responsable du traitement à Sous-traitant.
- Annexe 2 (Mesures techniques et organisationnelles) : veuillez-vous reporter au Plan de sécurité.

Les Parties conviennent que l'option 2 de la clause 9 « Recours à des sous-traitants ultérieurs » des Clauses contractuelles types de Responsable du traitement à Sous-traitant s'applique lorsque le Fournisseur engage un sous-traitant ultérieur et que le Fournisseur et le sous-traitant ultérieur conviennent de se conformer aux Clauses contractuelles types d'un Sous-traitant à un Sous-traitant, c'est à dire i) l'Annexe avec son MODULE 3 : transfert de sous-traitant à sous-traitant (disponible sur le site https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0914&from=FR) incorporée ici par référence, telle que mise à jour, modifiée, remplacée ou supprimée de temps à autre par la Commission européenne et/ou tout accord international de transfert de données correspondant ou équivalent aux Clauses contractuelles types adopté par l'autorité de contrôle au Royaume-Uni ou tout avenant à un tel accord.

Si le Fournisseur ne pense pas pouvoir satisfaire aux exigences raisonnablement définies par GSK, il doit immédiatement informer GSK de son incapacité et GSK a le droit de résoudre le Contrat.

Les Parties conviennent que les Clauses contractuelles types conclues produisent leurs effets dans les pays en dehors de l'Espace économique européen où (i) leurs dispositions sont reconnues comme une garantie appropriée en matière de transferts internationaux d'informations à caractère personnel vers des pays non adéquats ou (ii) la Législation en matière de protection des données requiert l'existence de dispositions contractuelles pour protéger les transferts internationaux d'Informations personnelles. Dans l'interprétation des Clauses contractuelles types, dans ces pays, toute référence à l'expression "État membre dans lequel l'exportateur de données est établi" sera interprétée comme désignant le pays dans lequel l'entité GSK est établie ; et toute référence au Règlement (EU) 2016/679 sera considérée comme désignant la loi du pays dans lequel GSK est établie en dehors de l'EEE. Toute référence à un pays adéquat désigne tout pays qui est réputé offrir, ou qui offre autrement, un niveau de protection équivalent à la Législation en matière de protection des données applicable, pays en dehors de l'Espace économique européen pour lesquels les Clauses contractuelles types couvriront les transferts d'informations à caractère personnel.

ANNEXE 1

SÉCURITÉ DE L'INFORMATION

La présente Annexe relative à la sécurité de l'information fait partie du Contrat entre GSK et le Fournisseur. En cas de conflit entre les termes de la présente Annexe et les termes du Contrat, la présente Annexe prévaudra. Les termes commençant par une majuscule et non définis dans la présente Annexe auront la signification qui leur est attribuée dans d'autres parties du Contrat.

« Données GSK » désignent toutes les données ou informations fournies par ou au nom de GSK, ou obtenus par le Fournisseur ou le Personnel du Fournisseur, dans le cadre de la négociation et de l'exécution du Contrat ou de l'exécution des obligations du Fournisseur en vertu du Contrat, y compris toutes les données et informations qui (a) sont créées, générées, collectées ou traitées par le Personnel du Fournisseur dans le cadre de l'exécution des obligations du Fournisseur en vertu du Contrat ; ou (b) résident dans ou sont accessibles par le biais des systèmes d'information de GSK ou des systèmes d'information du Fournisseur, ainsi que les données et informations drivées de ce qui précède.

« Environnement du Fournisseur » désigne la combinaison de matériel, de logiciels, de systèmes d'exploitation, de systèmes de base de données, d'outils et de composants de réseau utilisés par ou pour le compte du Fournisseur afin de recevoir, maintenir, traiter, stocker, accéder ou transmettre les Données GSK.

« Personnel du Fournisseur » désigne tout personnel engagé ou employé par le Fournisseur et ses sous-traitants pour exécuter une partie des Biens et/ou Services.

« **Traitement** » désigne toute opération ou ensemble d'opérations effectuées sur toute information ou donnée, que ce soit ou non par des moyens automatisés, tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou l'altération, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre mise à disposition, l'alignement ou la combinaison, la restriction, l'effacement ou la destruction.

2. **Responsabilités.** Le Fournisseur doit : (a) utiliser des contrôles de cryptage rigoureux pour protéger toutes les Données GSK en transit vers l'Environnement du Fournisseur ou en dehors de celui-ci vers des réseaux de tiers contre une divulgation, un accès ou une modification non autorisés (b) maintenir des processus de contrôle conformes aux meilleures pratiques de l'industrie pour détecter, prévenir et se rétablir de logiciels malveillants, de virus et de logiciels espions, incluant la mise à jour à intervalles réguliers des logiciels anti-virus, anti-malveillants et anti-espions ; (c) maintenir des politiques de gestion des accès, des procédures et des contrôles techniques conformes aux meilleures pratiques de l'industrie pour s'assurer que tous les accès aux Données GSK sous son contrôle sont dûment autorisés.

3. **Violation de sécurité.** Le Fournisseur signalera à GSK par e-mail à cstd@gsk.com tout(e) utilisation, perte, destruction, divulgation, accès, corruption, modification, vente, location ou autre Traitement accidentel, non autorisé ou illégal vérifié de toute Donnée GSK (une « Violation de sécurité ») dans les vingt-quatre (24) heures suivant la vérification du Fournisseur. Le Fournisseur s'assurera que tous les incidents de sécurité impliquant des Données GSK soient gérés conformément aux procédures appropriées de réponse aux incidents. Le Fournisseur travaillera avec GSK en toute bonne foi pour identifier la cause racine et remédier à la Violation de sécurité.

ANLAGE

DATENSCHUTZBESTIMMUNGEN – GRUNDLEGENDE PERSONENBEZOGENE DATEN

Abgedecktes verbundenes Unternehmen bedeutet: jedes verbundene Unternehmen von GSK, das die Dienstleistungen als Dritter in Anspruch nimmt (eine Liste der Dritten wird dem Lieferanten auf Anfrage von GSK zur Verfügung gestellt). Ein verbundenes Unternehmen ist ein Unternehmen, das in Bezug auf ein anderes Unternehmen von diesem kontrolliert wird, unter derselben Kontrolle wie dieses steht oder es kontrolliert. „Kontrolle" und alle davon abgeleiteten Begriffe bedeuten eine (direkte oder indirekte) Mehrheitsbeteiligung an den stimmberechtigten Geschäftsanteilen bzw. Aktien des Unternehmens oder die Möglichkeit, (direkt oder indirekt) die Mehrheit der Geschäftsführer*innen bzw. Vorstandsmitglieder des Unternehmens zu bestellen, oder die Befugnis, die Geschäftsführung oder Richtlinien des Unternehmens zu leiten, ob aufgrund von Vertrag oder anderweitig.

Datenschutzgesetze bedeutet: (a) die Datenschutz-Grundverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und alle anwendbaren Gesetze und/oder Verordnungen, die diesbezügliche Ausnahmeregelungen enthalten und/oder umsetzen und/oder diese ersetzen oder ablösen (**DSGVO**), und (b) die DSGVO des Vereinigten Königreichs nach Maßgabe des britischen Datenschutzgesetzes von 2018; (c) das Verbraucherdatenschutzgesetz des US-Bundesstaats Kalifornien (California Consumer Privacy Act, Cal. Civ. Code 1798.100 – 1798.199) (**CCPA**) und (d) alle anderen Gesetze bezüglich der Verarbeitung personenbezogener Daten.

Personenbezogene Daten bedeutet personenbezogene Daten mit folgendem Datensatz: Vorname und/oder Nachname, Initialen, Arbeitskontaktdaten, Gruppenmitgliedschaften, Netzwerk- oder Benutzeridentifikationsnummer, Anmeldedaten, Arbeitserfahrung und Fähigkeiten, Geschlecht oder Anrede, Veranstaltungsteilnahme von GSK-Mitarbeiter*innen und komplementären Mitarbeiter*innen, die die Dienstleistungen nutzen.

Personenbezogene Daten von GSK bedeutet personenbezogene Daten, die: (i) dem Lieferanten von oder im Namen von GSK bereitgestellt werden (so etwa, wenn der Lieferant Zugang zu personenbezogenen Daten hat, die von oder im Auftrag von GSK aufbewahrt werden) oder die der Lieferant im Auftrag von GSK erhebt oder generiert; (ii) die vom Lieferanten im Rahmen oder in Verbindung mit diesem Vertrag verarbeitet werden und (iii) in Bezug auf die GSK ein Verantwortlicher oder Eigentümer ist (oder eine gleichwertige Position innehat).

Sicherheitsplan bedeutet *den Cybersicherheitsplan, der hier als Anhang 1 beigefügt wird*.

Die Begriffe **Verantwortlicher, Datenschutz-Folgenabschätzung, betroffene Person, personenbezogene Daten, Verletzung des Schutzes personenbezogener Daten, Auftragsverarbeiter, Verarbeitung, Dienstleister** und **Aufsichtsbehörde** werden gemäß den einschlägigen Datenschutzgesetzen definiert. GSK bedeutet den im Vertrag angegebenen GSK-Vertragspartner sowie abgedeckte verbundene Unternehmen.

Bedingungen für Auftragsverarbeiter

Ist der Lieferant nach den einschlägigen Datenschutzgesetzen als Auftragsverarbeiter für personenbezogene Daten von GSK tätig, gelten folgende Bedingungen:

1. Jede Partei erfüllt ihre Pflichten gemäß den geltenden Datenschutzgesetzen. GSK und der Lieferant vereinbaren, dass GSK in Bezug auf die im Rahmen dieses Vertrags verarbeiteten personenbezogenen Daten von GSK der Verantwortliche ist und der Lieferant der Auftragsverarbeiter ist. Für die Zwecke des CCPA ist der Lieferant ein Dienstleister für GSK und die Verarbeitung personenbezogener Daten von GSK durch den Lieferanten erfolgt nur für die Zwecke von GSK in Übereinstimmung mit dieser Anlage, wobei GSK vom Lieferanten keine finanzielle oder andere geldwerte Gegenleistung erhält und GSK daher im Sinne des CCPA keine personenbezogenen Daten von GSK an den Lieferanten verkauft.

2. Der Lieferant muss in Bezug auf personenbezogene Daten von GSK Folgendes befolgen:

a) die personenbezogenen Daten von GSK nur gemäß den rechtmäßigen schriftlichen Anweisungen von GSK und ausschließlich für die Zwecke der Erbringung von Dienstleistungen durch den Lieferanten an GSK im Rahmen dieses Vertrags für die Laufzeit des Vertrags oder gegebenenfalls eines zusätzlichen im Vertrag angegebenen Zeitraums zu verarbeiten;

b) weder der Lieferant noch seine Mitarbeiter*innen, Vertreter*innen, Berater*innen oder Abtretungsempfänger*innen haben das Recht, personenbezogene Daten von GSK in jeglicher Form zum eigenen wirtschaftlichen Nutzen zu verarbeiten;

c) angemessene technische und organisatorische Sicherheitsmaßnahmen umzusetzen und beizubehalten, wie unter anderem die im Sicherheitsplan vorgesehenen Maßnahmen. Werden im Sicherheitsplan „Daten von GSK" erwähnt, umfasst dies auch personenbezogene Daten von GSK;

d) die personenbezogenen Daten von GSK gemäß den Bedingungen dieser Anlage vertraulich zu behandeln und wenn in dieser Anlage und dem Sicherheitsplan vertrauliche Informationen von GSK erwähnt werden, umfasst dies auch personenbezogene Daten von GSK;

e) dem zuständigen Personal, das Zugang zu personenbezogenen Daten von GSK hat, Vertraulichkeitspflichten aufzuerlegen, die den im Rahmen des Vertrags vorgesehenen Pflichten entsprechen;

f) ohne die vorherige schriftliche Genehmigung von GSK keinen anderen Auftragsverarbeiter („**Unterauftragsverarbeiter**") zu beauftragen (und für diese Zwecke stimmt GSK den folgenden Kategorien von Unterauftragsverarbeitern zu: Hosting-Infrastrukturdienstleistern, dem Einsatz einzelner Auftragnehmer und Unterauftragsverarbeiter, die GSK zum Zeitpunkt des Vertragsabschlusses bekanntgegeben werden) und die personenbezogenen Daten von GSK an solche genehmigten Unterauftragsverarbeiter nur im Rahmen eines schriftlichen Vertrags zu übermitteln, mit dem Pflichten auferlegt werden, die mit den in dieser Anlage vorgesehenen vereinbar sind.

Wenn der Lieferant gemäß dieser Klausel 2(f) einen Unterauftragsverarbeiter beauftragt, haftet er weiterhin für die Handlungen und Unterlassungen des Unterauftragsverarbeiters;

g) GSK angemessene Unterstützung zu bieten bei (i) der Durchführung von gesetzlich vorgeschriebenen Datenschutz-Folgenabschätzungen und/oder Folgenabschätzungen für die Datenübermittlung; (ii) der Gewährung von Rechten betroffener Personen und (iii) der Beantwortung von Anfragen von Aufsichtsbehörden in Bezug auf personenbezogene Daten von GSK;

h) GSK unverzüglich zu benachrichtigen, sobald GSK von einer Verletzung des Schutzes personenbezogener Daten in Bezug auf personenbezogene Daten von GSK Kenntnis erlangt, und GSK in Bezug auf diese Verletzung zu unterstützen;

i) GSK unverzüglich zu benachrichtigen, wenn er eine schriftliche Anfrage erhält von (i) einer betroffenen Person bezüglich der Ausübung eines ihrer Rechte in Bezug auf personenbezogene Daten von GSK gemäß den Datenschutzgesetzen oder (ii) einer Aufsichtsbehörde in Bezug auf die Verarbeitung personenbezogener Daten von GSK;

j) sofern im Vertrag nichts anderes vorgesehen ist, alle personenbezogenen Daten von GSK, die sich in seinem Besitz oder unter seiner Kontrolle befinden (einschließlich personenbezogener Daten von GSK, die von zulässigen Unterauftragsverarbeitern verarbeitet werden), bei Kündigung oder Ablauf des Vertrags entweder zurückzugeben oder zu vernichten und

k) auf schriftliche Anfrage von GSK GSK angemessene Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung dieser Anlage nachzuweisen. Dies kann auch verfügbare Sicherheitsauditberichte Dritter umfassen.

Bedingungen für Verantwortliche

Für den Fall, dass der Lieferant nach den einschlägigen Datenschutzgesetzen als Verantwortlicher für personenbezogene Daten von GSK tätig ist, gelten die folgenden Bedingungen:

1. Jede Partei ist als unabhängiger Verantwortlicher tätig und muss ihre Pflichten nach den geltenden Datenschutzgesetzen erfüllen. GSK und der Lieferant vereinbaren, dass in Bezug auf die im Rahmen dieser Anlage verarbeiteten personenbezogenen Daten für die Zwecke des CCPA vom Lieferanten keine finanzielle oder andere geldwerte Gegenleistung für die personenbezogenen Daten von GSK an GSK geleistet wird und GSK daher personenbezogene Daten von GSK nicht im Sinne des CCPA an den Lieferanten verkauft.

2. Erhält der Lieferant eine Mitteilung von einer Aufsichtsbehörde, die sich direkt oder indirekt auf a) die Verarbeitung personenbezogener Daten von GSK durch den Lieferanten oder (b) eine potenzielle Nichteinhaltung der Datenschutzgesetze in Bezug auf die Verarbeitung personenbezogener Daten von GSK bezieht, muss der Lieferant, soweit dies nach geltendem Recht zulässig ist, die Mitteilung unverzüglich an GSK weiterleiten und GSK hierzu angemessene Zusammenarbeit und Unterstützung bieten.

3. Stellt eine betroffene Person eine schriftliche Anfrage an eine der Parteien zur Ausübung eines ihrer Rechte gemäß den Datenschutzgesetzen in Bezug auf personenbezogene Daten von GSK, dann muss die empfangende Partei diese Anfrage gemäß den Datenschutzgesetzen beantworten. Soweit die Anfrage die Verarbeitung personenbezogener Daten von GSK betrifft, die von der anderen Partei vorgenommen wurde, muss die empfangende Partei: (i) die Anfrage unverzüglich und ohne unangemessene Verzögerung an die andere Partei weiterleiten und (ii) in Bezug auf diese Anfrage kooperieren und angemessene Unterstützung leisten, um der anderen Partei zu ermöglichen, gemäß den Datenschutzgesetzen zu antworten.

4. Unbeschadet der Bestimmungen des Sicherheitsplans wird der Lieferant, wenn er Kenntnis von einer personenbezogene Daten von GSK betreffenden Verletzung des Schutzes personenbezogener Daten erlangt, (a) GSK unverzüglich benachrichtigen und GSK eine angemessene Beschreibung der Verletzung bereitstellen und (b) keine Kommunikation über die Verletzung veröffentlichen, ohne zuvor GSK zu konsultieren, mit der Ausnahme, dass er eine Verletzung einer Aufsichtsbehörde melden kann, soweit dies nach den geltenden Datenschutzgesetzen erforderlich ist.

Internationale Datenübermittlung

Übermittelt GSK als Datenexporteur personenbezogene Daten von GSK an den Lieferanten als Datenimporteur derart, dass eine nach den geltenden Datenschutzgesetzen beschränkte internationale Datenübermittlung erfolgt, vereinbaren die Parteien für die zwischen ihnen bestehende Beziehung hiermit die geltenden Musterklauseln und werden diese einhalten:

- Der Anhang zum Durchführungsbeschluss der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates („**Anhang**"), zusammen mit MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche (**hier** verfügbar) und in diese Anlage durch Bezugnahme in der jeweils von der Europäischen Kommission aktualisierten, geänderten, ersetzten oder neugefassten Fassung aufgenommen und/oder (ii) eine entsprechende oder gleichwertige Vereinbarung oder ein Nachtrag zu den Musterklauseln, die von der Aufsichtsbehörde im Vereinigten Königreich erlassen wurden, zu internationalen Datenübermittlungen („**C2C-Musterklauseln**");
- Der Anhang zusammen mit MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter (**hier** verfügbar) und in diese Anlage durch Bezugnahme in der jeweils von der Europäischen Kommission aktualisierten, geänderten, ersetzten oder neugefassten Fassung aufgenommen und/oder (ii) eine entsprechende oder gleichwertige Vereinbarung oder ein Nachtrag zu den Musterklauseln, die von der Aufsichtsbehörde im Vereinigten Königreich erlassen wurden, zu internationalen Datenübermittlungen („**C2P-Musterklauseln**");

„**Musterklauseln**" bedeutet den Anhang zusammen mit den C2C-Musterklauseln und den C2P-Musterklauseln.

Für die Zwecke der Musterklauseln vereinbaren die Parteien wie folgt:

- Die Option in eckigen Klammern in Ziffer 11 „Rechtsbehelf" findet keine Anwendung

- In Klausel 17 „Geltendes Recht“ wird die Option 1 gewählt und es gilt das Recht Irlands.
- Nach Klausel 18 „Gerichtsstand und Zuständigkeit“ sind die Gerichte Irlands zuständig.

Für die Zwecke der geltenden C2P-Musterklauseln und der C2C-Musterklauseln beachten Sie bitte Folgendes:

- Annex1 (Exporteur und Importeur): GSK oder die relevanten GSK-Dienstleistungsempfänger, die sich in der EU und/oder im Vereinigten Königreich befinden, im Rahmen der Vereinbarung(en) mit dem Lieferanten, sind in Bezug auf personenbezogene Daten von GSK ein Datenexporteur. Der Lieferant ist in Bezug auf personenbezogene Daten von GSK ein Datenimporteur.
- Anhang 1 (Beschreibung der Übermittlungen): siehe Definition der vom Importeur bereitzustellenden personenbezogenen Daten und Dienstleistungen. Es werden keine sensiblen Daten übermittelt. Die Häufigkeit der Übermittlung ist fortlaufend. Die Art der Verarbeitungstätigkeiten und die Zwecke der Übermittlung werden in der/den Vereinbarung(en) mit dem Lieferanten festgelegt. Die Daten werden in Übereinstimmung mit den Datenaufbewahrungsrichtlinien des Datenexporteurs aufbewahrt.
- Anhang 1 (Zuständige Behörden): wie in Klausel 13 der C2C-Musterklauseln und der C2P-Musterklauseln vorgesehen
- Anhang 2 (Technische und organisatorische Maßnahmen): siehe nachstehende Sicherheitsmaßnahmen

Die Parteien vereinbaren, dass Option 2 in Klausel 9 „Einsatz von Unterauftragsverarbeitern“ der C-P-Musterklauseln gilt, wenn der Lieferant einen Unterauftragsverarbeiter beauftragt, und der Lieferant und der Unterauftragsverarbeiter sich verpflichten müssen, die **P-P-Musterklauseln einzuhalten**, d. h. i) den Anhang zusammen mit MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter (**hier** verfügbar) und in diese Anlage durch Bezugnahme in der jeweils von der Europäischen Kommission aktualisierten, geänderten, ersetzten oder neugefassten Fassung aufgenommen und/oder (ii) eine entsprechende oder gleichwertige Vereinbarung oder ein Nachtrag zu den Musterklauseln, die von der Aufsichtsbehörde im Vereinigten Königreich erlassen wurden, zu internationalen Datenübermittlungen;

Ist der Lieferant der Meinung, dass er die von GSK vernünftigerweise festgelegten Anforderungen nicht erfüllen kann, muss der Lieferant GSK unverzüglich über diese Unmöglichkeit informieren und GSK hat das Recht, den Vertrag zu kündigen.

Die Parteien vereinbaren, dass die vereinbarten Musterklauseln in Ländern außerhalb des Europäischen Wirtschaftsraums wirksam sind, wenn: (i) ihre Bestimmungen als geeignete Garantie in Bezug auf internationale Übermittlungen personenbezogener Daten in Länder ohne angemessenes Schutzniveau anerkannt werden oder (ii) die Datenschutzgesetze das Vorhandensein vertraglicher Bestimmungen zum Schutz internationaler Übermittlungen personenbezogener Daten erfordern. Bei der Auslegung der Musterklauseln wird in diesen Ländern der Begriff „Mitgliedstaat, in dem der Datenexporteur niedergelassen ist“ so ausgelegt, dass damit das Land gmeint ist, in dem das GSK-Unternehmen niedergelassen ist; und wird die Verordnung (EU) 2016/679 erwähnt, bezieht sich dies auf das Recht des Landes, in dem GSK außerhalb des EWR niedergelassen ist. „Land mit angemessenem Schutzniveau“ bedeutet ein Land, von dem für die Zwecke der geltenden Datenschutzgesetze in den Ländern außerhalb des Europäischen Wirtschaftsraums, in denen für die Übermittlung personenbezogener Daten die Musterklauseln gelten, angenommen wird, dass es ein angemessenes Schutzniveau bietet, oder das anderweitig ein angemessenes Datenschutzniveau bietet.

Sicherheitsmaßnahmen

„GSK-Daten“ bedeutet Daten oder Informationen, die von oder im Namen von GSK bereitgestellt oder vom Lieferanten oder dem Personal des Lieferanten in Verbindung mit der Verhandlung über den Vertrag und seiner Unterzeichnung oder der Erfüllung der Pflichten des Lieferanten aus dem Vertrag erhalten werden, wie unter anderem Daten und Informationen, die entweder: (i) während der Erfüllung der Pflichten des Lieferanten aus dem Vertrag vom Personal des Lieferanten erstellt, generiert, erhoben oder verarbeitet werden oder (ii) sich in Informationssystemen von GSK oder Informationssystemen des Lieferanten befinden oder auf die darüber zugegriffen wird, sowie Daten und Informationen, die von Vorstehendem abgeleitet werden.

„**Verarbeitung**“ bezeichnet jeden Vorgang oder jede Reihe von Vorgängen, die an Informationen oder Daten durchgeführt werden, unabhängig davon, ob sie automatisiert erfolgen oder nicht, wie z. B. Erhebung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Änderung, Abruf, Konsultation, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder anderweitige Bereitstellung, Datenabgleich oder -kombination, Einschränkung, Löschung oder Vernichtung.

„**Umgebung des Lieferanten**“ bedeutet die Kombination aus Hardware, Software, Betriebssystemen, Datenbanksystemen, Tools und Netzwerkkomponenten, die vom oder im Namen des Lieferanten verwendet werden, um GSK-Daten zu empfangen, zu pflegen, zu verarbeiten, zu speichern, darauf zuzugreifen oder sie zu übermitteln.

„Personal des Lieferanten“ bedeutet Mitarbeiter*innen, die vom Lieferanten und seinen Unterauftragnehmern mit der Erbringung eines Teils der Dienstleistungen beauftragt oder beschäftigt werden.

Dieser Sicherheitsplan ist Teil des Vertrags zwischen GSK und dem Lieferanten. Besteht in Bezug auf die Cybersicherheit ein Widerspruch zwischen den Bedingungen dieses Sicherheitsplans und den Bedingungen des Vertrags, hat dieser Sicherheitsplan Vorrang. Begriffe, die in diesem Sicherheitsplan nicht definiert werden, haben die Bedeutungen, die ihnen in anderen Teilen des Vertrags zugeschrieben werden.

1. Zuständigkeiten. Der Lieferant wird (a) starke Verschlüsselungskontrollen verwenden, um alle GSK-Daten vor unbefugter Offenlegung, Zugriff oder Veränderung bei der Übermittlung in oder aus der Umgebung des Lieferanten über Netzwerke Dritter zu schützen; (a) Kontrollverfahren im Einklang mit den bewährten Verfahren der Branche führen, um Malware, Viren und Spyware zu entdecken, zu verhindern und das System wiederherzustellen, einschließlich der regelmäßigen Aktualisierung von Virenschutz-, Anti-Malware- und Anti-Spyware-Software; (c) Richtlinien, Verfahren und technische Kontrollen zur Verwaltung des Zugriffs in Übereinstimmung mit den bewährten Praktiken der Branche

führen, um zu gewährleisten, dass jeglicher Zugriff auf GSK-Daten, die sich unter seiner Kontrolle befinden, mit der angemessenen Befugnis erfolgt.

2. Sicherheitsverletzung. Der Lieferant meldet GSK per E-Mail an cstd@gsk.com jede festgestellte versehentliche, unbefugte oder unrechtmäßige Nutzung, jeden Verlust, jede Vernichtung, jede Offenlegung, jeden Zugriff, jede Korruption, jede Veränderung, jeden Verkauf, jede Vermietung und sonstige Verarbeitung von GSK-Daten (eine „**Sicherheitsverletzung**“) innerhalb von vierundzwanzig (24) Stunden ab Feststellung durch den Lieferanten. Der Lieferant gewährleistet, dass alle Sicherheitsvorfälle, die GSK-Daten betreffen, in Übereinstimmung mit den entsprechenden Verfahren für die Reaktion auf Vorfälle behandelt werden, und arbeitet mit GSK in gutem Glauben zusammen, um eine Grundursache zu ermitteln und die Sicherheitsverletzung zu beheben.

ΠΑΡΑΡΤΗΜΑ

ΟΡΟΙ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ – ΒΑΣΙΚΕΣ ΠΡΟΣΩΠΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Καλυπτόμενη Συνδεδεμένη Εταιρεία σημαίνει: κάθε συνδεδεμένη εταιρεία της GSK που έχει το όφελος των Υπηρεσιών ως τρίτο μέρος (κατάλογος των οποίων θα παρασχεθεί από την GSK στον Προμηθευτή κατόπιν αιτήματος). Μια Συνδεδεμένη Εταιρεία είναι οποιοδήποτε νομικό πρόσωπο το οποίο, όσον αφορά σε οποιοδήποτε άλλο νομικό πρόσωπο, ελέγχεται από, βρίσκεται υπό κοινό έλεγχο ή ελέγχει το εν λόγω άλλο νομικό πρόσωπο. Ο όρος «Έλεγχος» και τα παράγωγά του σημαίνει την κυριότητα (απευθείας ή έμμεσα) μιας πλειοψηφίας των μετοχών με δικαίωμα ψήφου του εν λόγω νομικού προσώπου ή τη δυνατότητα (απευθείας ή έμμεσα) διορισμού μιας πλειοψηφίας των μελών του Δ.Σ. του εν λόγω νομικού προσώπου ή την εξουσία να κατευθύνει τη διεύθυνση ή τις πολιτικές του εν λόγω νομικού προσώπου, μέσω σύμβασης ή άλλως·

«Νόμοι περί Προστασίας Δεδομένων» σημαίνει: (α) τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων όσον αφορά στην επεξεργασία των προσωπικών δεδομένων και για την ελεύθερη διακίνηση των εν λόγω δεδομένων και οποιουσδήποτε ισχύοντες νόμους ή/και κανονισμούς που εφαρμόζουν ή/και ασκούν παρεκκλίσεις βάσει αυτού ή/και αντικαθιστούν ή υπερισχύουν αυτού (ΓΚΠΔ), και (β) τον ΓΚΠΔ όπως διαμορφώθηκε από το Νόμο περί Προστασίας Δεδομένων του Ηνωμένου Βασιλείου του 2018, (γ) τον Νόμο Ιδιωτικού Απορρήτου Καταναλωτών της California του 2018 (Cal. Civ. Code 1798.100 - 1798.199) (CCPA) και (δ) όλους τους άλλους νόμους που αφορούν στην επεξεργασία προσωπικών δεδομένων·

«Προσωπικές Πληροφορίες» σημαίνει τα προσωπικά δεδομένα εντός του παρακάτω συνόλου: όνομα ή/και επώνυμο, αρχικά, στοιχεία επικοινωνίας εργασίας, συνδρομές σε ομάδες, αριθμό ταυτοποίησης δικτύου ή χρήστη, διαπιστευτήρια σύνδεσης, ιστορικό εργασιακής απασχόλησης και δεξιότητες, φύλο ή τίτλο, συμμετοχή σε εκδηλώσεις υπαλλήλων της GSK και συμπληρωματικών εργαζομένων που χρησιμοποιούν τις Υπηρεσίες

«Προσωπικές Πληροφορίες της GSK» σημαίνει οποιεσδήποτε Προσωπικές Πληροφορίες (i) που παρέχονται από ή εκ μέρους της GSK στον Προμηθευτή (συμπεριλαμβανομένων των περιπτώσεων όπου ο Προμηθευτής έχει πρόσβαση σε προσωπικές πληροφορίες που διατηρούνται από την GSK ή για λογαριασμό της) ή που ο Προμηθευτής συλλέγει ή παράγει εκ μέρους της GSK, (ii) που υποβάλλονται σε επεξεργασία από τον Προμηθευτή με βάση ή σε σχέση με την παρούσα Σύμβαση και (iii) σε σχέση με τις οποίες η GSK είναι ο υπεύθυνος επεξεργασίας ή ιδιοκτήτης αυτών (ή ισοδύναμη ιδιότητα)·

Παράρτημα ασφαλείας είναι *το παράρτημα ασφαλείας στον κυβερνοχώρο που επισυνάπτεται στο παρόν ως Παράρτημα 1*.

Οι όροι **υπεύθυνος επεξεργασίας δεδομένων, εκτίμηση αντικτύπου προστασίας των δεδομένων, υποκείμενο των δεδομένων, προσωπικά δεδομένα, παραβίαση προσωπικών δεδομένων, εκτελών την επεξεργασία, επεξεργασία, πάροχος υπηρεσιών** και **εποπτική αρχή,** ορίζονται σύμφωνα με τους σχετικούς Νόμους περί Προστασίας Δεδομένων. Οποιαδήποτε αναφορά στην GSK θα σημαίνει το συμβαλλόμενο νομικό πρόσωπο της GSK που χρησιμοποιείται στη Σύμβαση, καθώς και τις Καλυπτόμενες Συνδεδεμένες Εταιρείες.

Όροι Εκτελούντος την Επεξεργασία

Στην περίπτωση που ο προμηθευτής ενεργεί ως εκτελών την επεξεργασία των Προσωπικών Πληροφοριών της GSK σύμφωνα με τους σχετικούς Νόμους περί Προστασίας Δεδομένων, θα ισχύουν οι ακόλουθοι όροι:

1. Κάθε συμβαλλόμενο μέρος θα συμμορφώνεται με τις υποχρεώσεις του σύμφωνα με τους ισχύοντες Νόμους περί Προστασίας Δεδομένων. Η GSK και ο Προμηθευτής συμφωνούν ότι όσον αφορά στις Προσωπικές Πληροφορίες της GSK που υποβάλλονται σε επεξεργασία σύμφωνα με την παρούσα Σύμβαση, η GSK θα είναι ο υπεύθυνος επεξεργασίας και ο Προμηθευτής θα είναι ο εκτελών την επεξεργασία. Για τους σκοπούς του Νόμου CCPA, ο Προμηθευτής είναι ένας πάροχος υπηρεσιών στην GSK και η επεξεργασία των Προσωπικών Πληροφοριών της GSK από τον Προμηθευτή θα πραγματοποιείται μόνο για τους σκοπούς της GSK, σύμφωνα με το παρόν Παράρτημα, ότι δεν παρέχεται χρηματικό ή άλλο αντάλλαγμα αξίας από τον Προμηθευτή στην GSK και συνεπώς η GSK δεν πωλεί Προσωπικές Πληροφορίες της GSK στον Προμηθευτή όπως ορίζεται από το Νόμο CCPA.

2. Ο Προμηθευτής θα συμμορφώνεται με τα παρακάτω σχετικά με τις Προσωπικές Πληροφορίες της GSK:

a) επεξεργάζεται Προσωπικές Πληροφορίες της GSK μόνο σύμφωνα με νόμιμες γραπτές οδηγίες της GSK και αποκλειστικά για τους σκοπούς της παροχής Υπηρεσιών από τον Προμηθευτή προς την GSK σύμφωνα με την παρούσα Σύμβαση, για όλη τη διάρκεια της Σύμβασης ή για οποιαδήποτε πρόσθετη περίοδο που αναφέρεται στη Σύμβαση, εάν ισχύει·

b) ούτε ο Προμηθευτής, ούτε οποιοσδήποτε από τους υπαλλήλους, τους αντιπροσώπους, τους συμβούλους ή τους εκπροσώπους του έχει οποιοδήποτε δικαίωμα να επεξεργάζεται Προσωπικές Πληροφορίες της GSK για δικό του εμπορικό όφελος σε οποιαδήποτε μορφή·

c) εφαρμόζει και διατηρεί κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας, συμπεριλαμβανομένων, χωρίς περιορισμό, των μέτρων που ορίζονται στο Παράρτημα Ασφαλείας. Οι αναφορές στα «Δεδομένα της GSK» στο Παράρτημα Ασφαλείας θα περιλαμβάνουν τις Προσωπικές Πληροφορίες της GSK·

d) διατηρεί εμπιστευτικές τις Προσωπικές Πληροφορίες της GSK σύμφωνα με τους όρους του παρόντος Παραρτήματος και οι αναφορές στις Εμπιστευτικές Πληροφορίες της GSK σε αυτό το Παράρτημα και το Παράρτημα Ασφαλείας θα περιλαμβάνουν τις Προσωπικές Πληροφορίες της GSK·

e) επιβάλλει υποχρεώσεις εμπιστευτικότητας ισοδύναμες με τις υποχρεώσεις που ορίζονται βάσει της Σύμβασης στο σχετικό προσωπικό που έχει πρόσβαση σε Προσωπικές Πληροφορίες της GSK·

f) δεν θα εμπλέξει έναν άλλο εκτελούντα την επεξεργασία («**υπεργολάβος επεξεργασίας»**) χωρίς την εκ των προτέρων γραπτή έγκριση της GSK (και για τους σκοπούς αυτούς, η GSK συναινεί με τις ακόλουθες κατηγορίες υπεργολάβου επεξεργασίας: παρόχους υπηρεσιών

υποδομής φιλοξενίας, χρήση μεμονωμένων εργολάβων και υπεργολάβους επεξεργασίας δεδομένων που γίνονται γνωστοί στην GSK κατά τη σύναψη της Σύμβασης) και θα διαβιβάζει τις Προσωπικές Πληροφορίες της GSK σε τέτοιους εγκεκριμένους υπεργολάβους επεξεργασίας δεδομένων μόνο βάσει γραπτής σύμβασης που επιβάλλει υποχρεώσεις συνεπείς με αυτές που ορίζονται στο παρόν Παράρτημα. Όταν ο Προμηθευτής διορίσει έναν υπεργολάβο επεξεργασίας δεδομένων σύμφωνα με την παρούσα ρήτρα 2(στ), παραμένει υπεύθυνος για τις πράξεις και παραλείψεις του υπεργολάβου επεξεργασίας·

g) παρέχει εύλογη βοήθεια στην GSK (i) για τη διεξαγωγή οποιασδήποτε νομικά απαιτούμενης αξιολόγησης αντικτύπου προστασίας δεδομένων ή/και αξιολόγησης αντίκτυπου διαβίβασης δεδομένων, (ii) για τη συμμόρφωση με τα δικαιώματα των υποκειμένων των δεδομένων και (iii) για την απάντηση σε αιτήματα οποιασδήποτε εποπτικής αρχής σχετικά με Προσωπικές Πληροφορίες της GSK·

h) θα ειδοποιήσει την GSK χωρίς καθυστέρηση αφού λάβει γνώση μιας παραβίασης προσωπικών δεδομένων σχετικά με οποιεσδήποτε Προσωπικές Πληροφορίες της GSK και θα παρέχει βοήθεια στην GSK σχετικά με μια τέτοια παραβίαση·

i) θα ειδοποιήσει την GSK χωρίς καθυστέρηση εάν λάβει ένα γραπτό αίτημα από (i) ένα υποκείμενο δεδομένων για την άσκηση οποιωνδήποτε εκ των δικαιωμάτων του σχετικά με τις Προσωπικές Πληροφορίες της GSK, σύμφωνα με τους Νόμους περί Προστασίας Δεδομένων ή (ii) μια εποπτική αρχή σχετικά με την επεξεργασία των Προσωπικών Πληροφοριών της GSK·

j) εκτός εάν ορίζεται διαφορετικά στη Σύμβαση, είτε θα επιστρέψει είτε θα καταστρέψει όλες τις Προσωπικές Πληροφορίες της GSK που βρίσκονται στην κατοχή του ή υπό τον έλεγχό του (συμπεριλαμβανομένων οποιωνδήποτε Προσωπικών Πληροφοριών της GSK που υποβάλλονται σε επεξεργασία από επιτρεπόμενους υπεργολάβους επεξεργασίας) κατά τον τερματισμό ή τη λήξη της Σύμβασης και

k) κατόπιν γραπτού αιτήματος της GSK, θα παρέχει στην GSK εύλογες πληροφορίες απαραίτητες για την επίδειξη συμμόρφωσης με αυτό το Παράρτημα, οι οποίες μπορεί να περιλαμβάνουν οποιεσδήποτε διαθέσιμες αναφορές ελέγχου ασφαλείας τρίτων μερών.

Όροι Υπεύθυνου Επεξεργασίας

Σε περίπτωση που ο προμηθευτής ενεργεί ως υπεύθυνος επεξεργασίας των Προσωπικών Πληροφοριών της GSK σύμφωνα με τους σχετικούς Νόμους περί Προστασίας Δεδομένων, θα ισχύουν οι ακόλουθοι όροι:

1. Κάθε συμβαλλόμενος ενεργεί ως ανεξάρτητος υπεύθυνος επεξεργασίας και συμμορφώνεται με τις υποχρεώσεις του βάσει των ισχυόντων Νόμων περί Προστασίας Δεδομένων. Η GSK και ο Προμηθευτής συμφωνούν ότι, σε σχέση με τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία βάσει αυτού του Παραρτήματος, για τους σκοπούς του Νόμου CCPA, δεν παρέχεται καμία χρηματική ή άλλη αποζημίωση αξίας από τον Προμηθευτή προς την GSK ως αντάλλαγμα για τις Προσωπικές Πληροφορίες της GSK και συνεπώς η GSK δεν πωλεί Προσωπικές Πληροφορίες της GSK στον Προμηθευτή, όπως ορίζεται από το Νόμο CCPA.

2. Εάν ο Προμηθευτής λάβει οποιαδήποτε κοινοποίηση από μια εποπτική αρχή που σχετίζεται απευθείας ή έμμεσα με (α) την επεξεργασία των Προσωπικών Πληροφοριών της GSK από τον Προμηθευτή ή (β) μια ενδεχόμενη παράλειψη συμμόρφωσης με τους Νόμους περί Προστασίας Δεδομένων σε σχέση με την επεξεργασία των Προσωπικών Πληροφοριών της GSK, ο Προμηθευτής, στον βαθμό που επιτρέπεται από τους εφαρμόσιμους νόμους, θα προωθήσει αμέσως την επικοινωνία στην GSK και θα παράσχει σχετική εύλογη συνεργασία και βοήθεια στην GSK.

3. Εάν ένα υποκείμενο των δεδομένων υποβάλει γραπτό αίτημα σε οποιοδήποτε μέρος για να ασκήσει οποιοδήποτε από τα δικαιώματά του σύμφωνα με τους Νόμους περί Προστασίας Δεδομένων όσον αφορά στις Προσωπικές Πληροφορίες της GSK, το παραλαμβάνον μέρος θα απαντήσει σε αυτό το αίτημα σύμφωνα με τους Νόμους περί Προστασίας Δεδομένων. Στο βαθμό που το αίτημα αφορά στην ανάληψη επεξεργασίας Προσωπικών Πληροφοριών της GSK από το άλλο μέρος, το παραλαμβάνον μέρος: (i) έγκαιρα και χωρίς αδικαιολόγητη καθυστέρηση προωθεί το αίτημα στο άλλο μέρος και (ii) συνεργάζεται και παρέχει εύλογη βοήθεια σε σχέση με το εν λόγω αίτημα για να δώσει τη δυνατότητα στο άλλο μέρος να απαντήσει σύμφωνα με τους Νόμους περί Προστασίας Δεδομένων.

4. Χωρίς περιορισμό οποιασδήποτε διάταξης του Παραρτήματος Ασφαλείας, αφού λάβει γνώση μιας παραβίασης προσωπικών δεδομένων που επηρεάζει τις Προσωπικές Πληροφορίες της GSK, ο Προμηθευτής (α) θα ειδοποιήσει αμέσως την GSK και θα παράσχει στην GSK μια εύλογη περιγραφή της παραβίασης και (β) δεν θα δημοσιεύσει οποιαδήποτε επικοινωνία σχετικά με την παραβίαση χωρίς να συμβουλευτεί εκ των προτέρων την GSK, εκτός από το ότι μπορεί να κοινοποιήσει μια παραβίαση σε μια εποπτική αρχή στο βαθμό που απαιτείται από τους ισχύοντες Νόμους περί Προστασίας Δεδομένων.

Διεθνής διαβίβαση δεδομένων

Όταν η GSK, ενεργώντας ως εξαγωγέας δεδομένων, διαβιβάζει Προσωπικές Πληροφορίες της GSK στον Προμηθευτή, ενεργώντας ως εισαγωγέας δεδομένων, με τρόπο που αποτελεί περιορισμένη διεθνή διαβίβαση δεδομένων σύμφωνα με τους ισχύοντες Νόμους περί Προστασίας Δεδομένων, αμφότερα τα μέρη έχουν συνάψει δια της παρούσας και θα συμμορφώνονται με τις ισχύουσες Πρότυπες Ρήτρες που καλύπτουν τη σχέση μεταξύ των μερών:

- Το Παράρτημα της Απόφασης Υλοποίησης της Επιτροπής σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου («**Παράρτημα**») μαζί με την ΕΝΟΤΗΤΑ ΕΝΑ: Διαβίβαση από υπεύθυνο επεξεργασίας προς υπεύθυνο επεξεργασίας (διαθέσιμη **εδώ**) και ενσωματώνεται στο παρόν δι' αναφοράς ως ενημερωμένη, τροποποιημένη ή αντικατεστημένη κατά καιρούς από την Ευρωπαϊκή Επιτροπή ή/και (ii) οποιαδήποτε αντίστοιχη ή ισοδύναμη διεθνή συμφωνία διαβίβασης δεδομένων ή παράρτημα στις Πρότυπες Ρήτρες που έχουν υιοθετηθεί από την εποπτική αρχή στο Ηνωμένο Βασίλειο («Πρότυπες Ρήτρες C2C»)·
- Το Παράρτημα μαζί με τη ΕΝΟΤΗΤΑ ΔΥΟ: Διαβίβαση από υπεύθυνο επεξεργασίας προς εκτελούντα την επεξεργασία (διαθέσιμη εδώ) και ενσωματώνεται στο παρόν δι' αναφοράς ως ενημερωμένη, τροποποιημένη ή αντικατεστημένη κατά καιρούς από την Ευρωπαϊκή

Επιτροπή ή/και (ii) οποιαδήποτε αντίστοιχη ή ισοδύναμη διεθνή συμφωνία διαβίβασης δεδομένων ή παράρτημα στις Πρότυπες Ρήτρες που έχουν υιοθετηθεί από την εποπτική αρχή στο Ηνωμένο Βασίλειο («Πρότυπες Ρήτρες C2C»)·

«**Πρότυπες Ρήτρες**» σημαίνει το Παράρτημα μαζί με τις Πρότυπες Ρήτρες C2C και τις Πρότυπες Ρήτρες C2P.

Για τους σκοπούς των Πρότυπων Ρητρών, τα συμβαλλόμενα μέρη συμφωνούν ότι:

- Η επιλογή σε αγκύλες της Ρήτρας 11 «Επανόρθωση» δεν θα ισχύει
- Η επιλογή ένα επιλέγεται για τη Ρήτρα 17 «Διέπον Δίκαιο» και θα ισχύει το δίκαιο της Ιρλανδίας.
- Τα δικαστήρια της Ιρλανδίας θα έχουν δικαιοδοσία σύμφωνα με τη Ρήτρα 18 «Επιλογή Φόρουμ και Δικαιοδοσίας».

Για τους σκοπούς των εφαρμόσιμων Προτύπων Ρητρών C2P και C2C, σημειώστε τα εξής:

- Παράρτημα 1 (Εξαγωγέας και Εισαγωγέας): Η GSK ή οι σχετικοί παραλήπτες υπηρεσιών της GSK που βρίσκονται στην ΕΕ ή/και στο Ηνωμένο Βασίλειο σύμφωνα με τις συμβάσεις με τον Προμηθευτή είναι ένας Εξαγωγέας Δεδομένων σε σχέση με τις Προσωπικές Πληροφορίες της GSK. Ο Προμηθευτής είναι Εισαγωγέας Δεδομένων σε σχέση με τις Προσωπικές Πληροφορίες της GSK
- Παράρτημα 1 (Περιγραφή Διαβιβάσεων): δείτε τον ορισμό των Προσωπικών Πληροφοριών και Υπηρεσιών που θα παρασχεθούν από τον Εισαγωγέα. Δεν διαβιβάζονται ευαίσθητα δεδομένα. Η συχνότητα της διαβίβασης είναι συνεχής. Ο χαρακτήρας των δραστηριοτήτων επεξεργασίας και οι σκοποί της διαβίβασης καθορίζονται στις συμβάσεις με τον Προμηθευτή. Τα δεδομένα θα διατηρούνται σύμφωνα με τις πολιτικές διατήρησης δεδομένων του Εξαγωγέα Δεδομένων.
- Παράρτημα 1 (Αρμόδιες Αρχές): όπως ορίζεται στη ρήτρα 13 των Προτύπων Ρητρών C2C και των Προτύπων Ρητρών C2P
- Παράρτημα 2 (Τεχνικά και Οργανωτικά Μέτρα): δείτε τα Μέτρα Ασφαλείας που αναφέρονται παρακάτω

Τα συμβαλλόμενα μέρη συμφωνούν ότι η επιλογή 2 της ρήτρας 9 «Χρήση Υπεργολάβων Επεξεργασίας» των Προτύπων Ρητρών C-P θα ισχύει όταν ο Προμηθευτής εμπλέκει έναν υπεργολάβο επεξεργασίας δεδομένων και ο Προμηθευτής και ο υπεργολάβος επεξεργασίας δεδομένων θα συμφωνήσουν να συμμορφώνονται με τις **Πρότυπες Ρήτρες P-P**, που σημαίνει i) το Παράρτημα μαζί με την ΕΝΟΤΗΤΑ ΤΡΙΑ: Διαβίβαση από εκτελούντα την επεξεργασία προς εκτελούντα την επεξεργασία (διαθέσιμη εδώ) και ενσωματώνεται στο παρόν δι' αναφοράς ως ενημερωμένη, τροποποιημένη ή αντικατεστημένη κατά καιρούς από την Ευρωπαϊκή Επιτροπή ή/και (ii) οποιαδήποτε αντίστοιχη ή ισοδύναμη διεθνή συμφωνία διαβίβασης δεδομένων ή παράρτημα στις Πρότυπες Ρήτρες που έχει υιοθετηθεί από την εποπτική αρχή στο Ηνωμένο Βασίλειο·

Σε περίπτωση που ο Προμηθευτής δεν πιστεύει ότι μπορεί να ανταποκριθεί στις απαιτήσεις που ορίζονται εύλογα από την GSK, ο Προμηθευτής θα ειδοποιήσει αμέσως την GSK για την αδυναμία του και η GSK θα έχει το δικαίωμα να καταγγείλει τη Σύμβαση.

Τα Συμβαλλόμενα Μέρη συμφωνούν ότι οι Πρότυπες Ρήτρες που συνάπτονται θα έχουν ισχύ σε χώρες εκτός του Ευρωπαϊκού Οικονομικού Χώρου, όπου: (i) οι διατάξεις τους αναγνωρίζονται ως κατάλληλη διασφάλιση σε σχέση με τις διεθνείς διαβιβάσεις Προσωπικών Δεδομένων σε χώρες χωρίς επάρκεια προστασίας ή (ii) οι Νόμοι περί Προστασίας Δεδομένων απαιτούν την ύπαρξη συμβατικών διατάξεων για την προστασία των διεθνών διαβιβάσεων Προσωπικών Πληροφοριών. Κατά την ερμηνεία των Προτύπων Ρητρών, σε αυτές τις χώρες, οποιαδήποτε αναφορά στον όρο «Κράτος Μέλος στο οποίο είναι εγκατεστημένος ο εξαγωγέας δεδομένων», θα ερμηνεύεται ώστε να σημαίνει τη χώρα στην οποία είναι εγκατεστημένη η οντότητα της GSK και οποιαδήποτε αναφορά στον Κανονισμό (ΕΕ) 2016/679 θα αναφέρεται στο δίκαιο της χώρας στην οποία η GSK είναι εγκατεστημένη εκτός του ΕΟΧ. Οποιαδήποτε αναφορά σε μια «Χώρα με επάρκεια προστασίας» θα σημαίνει οποιαδήποτε χώρα που θεωρείται ότι παρέχει ή που κατά τα άλλα παρέχει, ισοδύναμο επίπεδο προστασίας για τους σκοπούς των ισχυόντων Νόμων για την Προστασία Δεδομένων, στις χώρες εκτός του Ευρωπαϊκού Οικονομικού Χώρου όπου οι Πρότυπες Ρήτρες θα καλύπτουν τις διαβιβάσεις Προσωπικών Δεδομένων.

Μέτρα ασφαλείας

«Δεδομένα της GSK» σημαίνει οποιαδήποτε δεδομένα ή πληροφορίες που παρέχονται από ή εκ μέρους της GSK ή αποκτώνται από τον Προμηθευτή ή το Προσωπικό του Προμηθευτή σε σχέση με τη διαπραγμάτευση και υπογραφή της Σύμβασης ή την εκπλήρωση των υποχρεώσεων του Προμηθευτή βάσει της Σύμβασης, συμπεριλαμβανομένων οποιωνδήποτε τέτοιων δεδομένων και πληροφοριών που είτε: (i) δημιουργούνται, παράγονται, συλλέγονται ή υποβάλλονται σε επεξεργασία από το Προσωπικό του Προμηθευτή κατά την εκπλήρωση των υποχρεώσεων του Προμηθευτή βάσει της Σύμβασης, ή (ii) παραμένουν ή προσπελάζονται μέσω των πληροφοριακών συστημάτων της GSK ή των συστημάτων πληροφορικής του Προμηθευτή, όπως και οποιαδήποτε δεδομένα και πληροφορίες που προκύπτουν από τα προαναφερθέντα.

Ο όρος «**Επεξεργασία**» σημαίνει οποιαδήποτε λειτουργία ή σύνολο λειτουργιών που πραγματοποιείται σε οποιεσδήποτε πληροφορίες ή δεδομένα, με αυτοματοποιημένα ή μη μέσα, όπως συλλογή, καταγραφή, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, διαβούλευση, χρήση, γνωστοποίηση μέσω μετάδοσης, διάδοση ή με άλλο τρόπο διάθεση, ευθυγράμμιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.

«Περιβάλλον Προμηθευτή» είναι ο συνδυασμός υλικού, λογισμικού, λειτουργικών συστημάτων, συστημάτων βάσεων δεδομένων, εργαλείων και στοιχείων δικτύου που χρησιμοποιούνται από ή για λογαριασμό του Προμηθευτή για τη λήψη, διατήρηση, επεξεργασία, αποθήκευση, πρόσβαση ή μετάδοση Δεδομένων της GSK.

Ο όρος «Προσωπικό του Προμηθευτή» σημαίνει κάθε μέλος του προσωπικού που εμπλέκεται ή απασχολείται από τον Προμηθευτή και τους Υπεργολάβους του για την εκτέλεση οποιουδήποτε μέρους των Υπηρεσιών.

Το παρόν Παράρτημα Ασφαλείας αποτελεί μέρος της Σύμβασης από και μεταξύ της GSK και του Προμηθευτή. Σε περίπτωση οποιασδήποτε αντίφασης όσον αφορά στην ασφάλεια στον κυβερνοχώρο, μεταξύ των όρων του παρόντος Παραρτήματος Ασφαλείας και των όρων της Σύμβασης, θα υπερισχύει το παρόν Παράρτημα Ασφαλείας. Οι όροι που αρχίζουν με κεφαλαία γράμματα και δεν ορίζονται στο παρόν

Παράρτημα Ασφαλείας θα έχουν τις έννοιες που τους αποδίδονται σε άλλα μέρη της Σύμβασης.

1. Ευθύνες. Ο Προμηθευτής θα: (α) χρησιμοποιεί ισχυρούς ελέγχους κρυπτογράφησης για την προστασία όλων των Δεδομένων της GSK από μη εξουσιοδοτημένη γνωστοποίηση, πρόσβαση ή τροποποίηση κατά τη διαβίβαση εντός ή εκτός του περιβάλλοντος του Προμηθευτή μέσω δικτύων τρίτων· (β) διατηρεί διαδικασίες ελέγχου σύμφωνα με τις βέλτιστες πρακτικές του κλάδου για τον εντοπισμό, την πρόληψη και την ανάκτηση από κακόβουλο λογισμικό, ιούς και λογισμικό κατασκοπείας σε τακτά χρονικά διαστήματα· (γ) διατηρεί πολιτικές διαχείρισης πρόσβασης, διαδικασίες και τεχνικούς ελέγχους σύμφωνα με τις βέλτιστες πρακτικές του κλάδου, ώστε να διασφαλιστεί ότι κάθε πρόσβαση στα Δεδομένα της GSK που βρίσκονται υπό τον έλεγχό του είναι κατάλληλα εξουσιοδοτημένη.

2. Παραβίαση ασφαλείας. Ο Προμηθευτής θα αναφέρει στην GSK μέσω email στη διεύθυνση cstd@gsk.com οποιαδήποτε επαληθευμένη τυχαία, μη εξουσιοδοτημένη ή παράνομη χρήση, απώλεια, καταστροφή, γνωστοποίηση, πρόσβαση, αλλοίωση, τροποποίηση, πώληση, ενοικίαση ή άλλη Επεξεργασία οποιωνδήποτε Δεδομένων της GSK (μια «**Παραβίαση Ασφαλείας**») εντός είκοσι τεσσάρων (24) ωρών από την επαλήθευση του Προμηθευτή. Ο Προμηθευτής θα διασφαλίσει ότι η διαχείριση όλων των περιστατικών ασφαλείας που αφορούν Δεδομένα της GSK εκτελείται σύμφωνα με τις κατάλληλες διαδικασίες ανταπόκρισης σε περιστατικά. Ο Προμηθευτής θα συνεργαστεί με την GSK καλή τη πίστει για να προσδιορίσει μια βασική αιτία και να αποκαταστήσει την παραβίαση της ασφάλειας.

DAFTAR

KETENTUAN PERLINDUNGAN DATA – INFORMASI PRIBADI DASAR

Afiliasi Yang Dilindungi berarti: setiap Afiliasi GSK yang memiliki manfaat Layanan sebagai pihak ketiga (daftarnya akan disediakan oleh GSK kepada Pemasok berdasarkan permintaan). Afiliasi adalah setiap entitas yang, sehubungan dengan entitas lain, Dikendalikan oleh, berada di bawah Kendali yang sama dengan entitas lain tersebut. "Kendali" dan turunannya berarti kepemilikan (secara langsung atau tidak langsung) dari mayoritas saham berhak suara dari entitas tersebut atau kemampuan (secara langsung atau tidak langsung) untuk menunjuk mayoritas direktur dari entitas tersebut atau wewenang untuk mengarahkan manajemen atau kebijakan entitas tersebut, melalui kontrak atau lainnya;

Undang-Undang Perlindungan Data berarti: (a) Peraturan Perlindungan Data Umum (UE) Nomor 679 Tahun 2016 tentang perlindungan orang perseorangan sehubungan dengan pemrosesan data pribadi dan tentang pergerakan bebas data tersebut dan setiap hukum dan/atau peraturan yang berlaku yang menerapkan dan/atau melakukan pengurangan berdasarkan hal tersebut dan/atau mengantikannya (**GDPR**); (b) GDPR sebagaimana disesuaikan dengan Undang-Undang Perlindungan Data Inggris Raya Tahun 2018; (c) Undang-Undang Privasi Konsumen California Tahun 2018 (Cal. Civ. Code 1798.100 - 1798.199) (**CCPA**); dan (d) semua undang-undang lain tentang pemrosesan data pribadi;

Informasi Pribadi berarti data pribadi dalam rangkaian berikut: nama depan dan/atau nama belakang, inisial, perincian kontak kerja, keanggotaan grup, jaringan atau nomor identifikasi pengguna, kredensial login, riwayat dan keterampilan kerja, jenis kelamin atau jabatan, kehadiran acara karyawan GSK dan pekerja pelengkap yang menggunakan Layanan

Informasi Pribadi GSK berarti setiap Informasi Pribadi: (i) yang disediakan oleh atau atas nama GSK kepada Pemasok (termasuk apabila Pemasok memiliki akses ke Informasi Pribadi yang disimpan oleh GSK atau atas namanya), atau yang dikumpulkan atau dibuat oleh Pemasok atas nama GSK; (ii) yang diproses oleh Pemasok berdasarkan atau sehubungan dengan Perjanjian ini; dan (iii) sehubungan dengan GSK yang merupakan pengendali atau pemilik (atau yang setara);

Daftar Keamanan berarti *daftar keamanan siber yang dilampirkan sebagai Lampiran 1*.

Istilah **pengendali, penilaian dampak perlindungan data, subjek data, data pribadi, pelanggaran data pribadi, pemroses, pemrosesan, penyedia layanan,** dan **otoritas pengawas** harus didefinisikan berdasarkan Undang-Undang Perlindungan Data yang relevan. Setiap penyebutan GSK berarti entitas yang mengadakan kontrak dengan GSK yang digunakan dalam Perjanjian, serta Afiliasi Yang Tercakup.

Ketentuan Pemroses

Apabila pemasok bertindak sebagai pemroses Informasi Pribadi GSK berdasarkan Undang-Undang Perlindungan Data yang relevan, maka ketentuan berikut akan berlaku:

1. Masing-masing pihak harus mematuhi kewajibannya berdasarkan Undang-Undang Perlindungan Data yang berlaku. GSK dan Pemasok menyetujui bahwa sehubungan dengan Informasi Pribadi GSK yang diproses berdasarkan Perjanjian ini, GSK akan menjadi pengendali dan Pemasok akan menjadi pemroses. Untuk tujuan CCPA, Pemasok adalah penyedia layanan untuk GSK, dan pemrosesan Informasi Pribadi GSK oleh Pemasok harus dilakukan hanya untuk tujuan GSK sesuai dengan Daftar ini, bahwa tidak ada imbalan uang atau barang berharga lainnya yang diberikan oleh Pemasok kepada GSK, dan oleh karena itu, GSK tidak menjual Informasi Pribadi GSK kepada Pemasok sebagaimana ditetapkan oleh CCPA.

2. Pemasok harus mematuhi hal-hal berikut sehubungan dengan Informasi Pribadi GSK:

a) memproses Informasi Pribadi GSK hanya berdasarkan instruksi tertulis yang sah dari GSK dan semata-mata untuk tujuan penyediaan Layanan oleh Pemasok kepada GSK berdasarkan Perjanjian ini selama jangka waktu Perjanjian atau periode tambahan yang dinyatakan dalam Perjanjian, jika berlaku;

b) baik Pemasok, maupun karyawan, agen, konsultan, atau penerimanya tidak berhak memproses Informasi Pribadi GSK demi keuntungan komersial mereka sendiri dalam bentuk apa pun;

c) menerapkan dan mempertahankan langkah-langkah keamanan teknis dan organisasi yang sesuai, termasuk namun tidak terbatas pada langkah-langkah yang ditetapkan pada Daftar Keamanan. Penyebutan "Data GSK" dalam Daftar Keamanan harus mencakup Informasi Pribadi GSK;

d) menjaga kerahasiaan Informasi Pribadi GSK sesuai dengan ketentuan dari Daftar ini, serta referensi dalam Daftar ini dan Daftar Keamanan untuk Informasi Rahasia GSK harus mencakup Informasi Pribadi GSK;

e) membebankan kewajiban kerahasiaan yang setara dengan kewajiban yang ditetapkan berdasarkan Perjanjian kepada personel terkait yang memiliki akses ke Informasi Pribadi GSK;

f) tidak menggunakan pemroses lain ("**sub-pemroses"**) tanpa persetujuan tertulis sebelumnya dari GSK (dan untuk tujuan ini, GSK menyetujui kategori subpemroses berikut: penyedia layanan infrastruktur hosting, penggunaan kontraktor individu, dan subpemroses yang diketahui GSK pada saat Perjanjian ditandatangani), serta mengalihkan Informasi Pribadi GSK ke subpemroses yang disetujui tersebut hanya berdasarkan kontrak tertulis yang membebankan kewajiban yang sesuai dengan yang ditetapkan dalam Daftar ini. Apabila Pemasok menunjuk subpemroses sesuai dengan klausul 2(f) ini, pihaknya tetap bertanggung jawab atas tindakan dan kelalaian subpemroses;

g) memberikan bantuan yang wajar kepada GSK dengan (i) melaksanakan penilaian dampak perlindungan data dan/atau penilaian dampak pengalihan data yang diwajibkan secara hukum; (ii) mematuhi hak-hak subjek data; dan (iii) menanggapi permintaan dari otoritas pengawas sehubungan dengan Informasi Pribadi GSK;

h) memberi tahu GSK tanpa penundaan setelah mengetahui adanya pelanggaran data pribadi sehubungan dengan Informasi Pribadi GSK dan memberikan bantuan kepada GSK terkait dengan pelanggaran tersebut;

i) memberi tahu GSK tanpa penundaan jika menerima permintaan tertulis dari (i) subjek data untuk menggunakan haknya sehubungan dengan Informasi Pribadi GSK berdasarkan Undang-Undang Perlindungan Data; atau (ii) otoritas pengawas terkait dengan pemrosesan Informasi Pribadi GSK;

j) kecuali jika ditentukan lain dalam Perjanjian, mengembalikan atau memusnahkan semua Informasi Pribadi GSK yang dimilikinya atau di bawah kendalinya (termasuk Informasi Pribadi GSK yang diproses oleh subpemroses yang diizinkan) pada saat Perjanjian berakhir atau kedaluwarsa; dan

k) atas permintaan tertulis dari GSK, memberikan informasi wajar yang diperlukan GSK untuk menunjukkan kepatuhan terhadap Daftar ini, yang dapat mencakup laporan audit keamanan pihak ketiga yang tersedia.

Ketentuan Pengendali

Apabila pemasok bertindak sebagai pengendali Informasi Pribadi GSK berdasarkan Undang-Undang Perlindungan Data yang relevan, ketentuan berikut akan berlaku:

1. Masing-masing pihak bertindak sebagai pengendali independen dan harus mematuhi kewajibannya berdasarkan Undang-Undang Perlindungan Data yang berlaku. GSK dan Pemasok menyetujui bahwa, sehubungan dengan data pribadi yang diproses berdasarkan Daftar ini, untuk tujuan CCPA, bahwa tidak ada uang atau barang berharga lainnya yang diberikan oleh Pemasok kepada GSK sebagai imbalan atas Informasi Pribadi GSK dan oleh karena itu GSK tidak menjual Informasi Pribadi GSK kepada Pemasok sebagaimana ditentukan oleh CCPA.

2. Jika Pemasok menerima komunikasi dari otoritas pengawas yang berhubungan langsung atau tidak langsung dengan a) pemrosesan Informasi Pribadi GSK oleh Pemasok; atau (b) potensi kegagalan untuk mematuhi Undang-Undang Perlindungan Data sehubungan dengan pemrosesan Informasi Pribadi GSK, Pemasok harus, sejauh diizinkan oleh undang-undang yang berlaku, segera meneruskan komunikasi kepada GSK serta bekerja sama dan memberikan bantuan yang wajar kepada GSK terkait hal tersebut.

3. Jika subjek data membuat permintaan tertulis kepada salah satu pihak untuk menggunakan hak mereka berdasarkan Undang-Undang Perlindungan Data sehubungan dengan Informasi Pribadi GSK, pihak penerima harus menanggapi permintaan tersebut sesuai dengan Undang-Undang Perlindungan Data. Sejauh permintaan tersebut mengenai pemrosesan Informasi Pribadi GSK yang dilakukan oleh pihak lain, pihak penerima harus: (i) segera dan tanpa penundaan yang tidak semestinya menyampaikan permintaan tersebut kepada pihak lain; dan (ii) bekerja sama dan memberikan bantuan yang wajar sehubungan dengan permintaan tersebut agar pihak lain dapat memberikan tanggapan sesuai dengan Undang-Undang Perlindungan Data.

4. Tanpa membatasi setiap ketentuan dari Daftar Keamanan, setelah mengetahui adanya pelanggaran data pribadi yang memengaruhi Informasi Pribadi GSK, Pemasok harus (a) segera memberi tahu GSK dan memberikan deskripsi yang wajar tentang pelanggaran tersebut kepada GSK; dan (b) tidak memublikasikan komunikasi mengenai pelanggaran tersebut tanpa berkonsultasi terlebih dahulu dengan GSK, kecuali komunikasi tersebut dapat memberitahukan pelanggaran kepada otoritas pengawas sejauh diwajibkan oleh Undang-Undang Perlindungan Data yang berlaku.

Pengalihan Data Internasional

Apabila GSK, yang bertindak sebagai pengekspor data, mengalihkan Informasi Pribadi GSK kepada Pemasok, yang bertindak sebagai pengimpor data, dengan cara yang merupakan pengalihan data internasional terbatas berdasarkan Undang-Undang Perlindungan Data yang berlaku, kedua belah pihak dengan ini menandatangani dan akan mematuhi Klausul Model yang berlaku yang mencakup hubungan antara para pihak:

- Lampiran Keputusan Pelaksanaan Komisi tentang klausul kontrak standar untuk pengalihan data pribadi kepada negara-negara ketiga sesuai dengan Peraturan (UE) Nomor 679 Tahun 2016 dari Parlemen dan Dewan Eropa ("**Lampiran**") beserta MODUL SATU: Pengalihan pengendali ke pengendali (tersedia **di sini**) dan tercakup di sini melalui penyebuytan sebagaimana diperbarui, diubah, diganti, atau digantikan dari waktu ke waktu oleh Komisi Eropa; dan/atau (ii) perjanjian atau adendum pengalihan data internasional yang sesuai atau setara dengan Klausul Model yang digunakan oleh otoritas pengawas di Inggris Raya ("**Klausul Model C2C**");
- Lampiran beserta MODUL DUA: Pengalihan pengendali ke pemroses (tersedia **di sini**) dan tecakup di sini melalui penyebutan sebagaimana diperbarui, diubah, diganti, atau digantikan dari waktu ke waktu oleh Komisi Eropa; dan/atau (ii) perjanjian atau adendum pengalihan data internasional yang sesuai atau setara dengan Klausul Model yang digunakan oleh otoritas pengawas di Inggris Raya ("**Klausul Model C2P**");

"**Klausul Model**" berarti Lampiran beserta Klausul Model C2C dan Klausul Model C2P.

Untuk tujuan Klausul Model, para pihak menyetujui bahwa:

- Opsi dalam tanda kurung siku pada Klausul 11 "Ganti Rugi" tidak berlaku
- Opsi satu dipilih untuk Klausul 17 "Hukum yang Mengatur" dan hukum Irlandia akan berlaku.
- Pengadilan Irlandia akan memiliki yurisdiksi berdasarkan Klausul 18 "Pilihan Forum dan Yurisdiksi".

Untuk keperluan Klausul Model C2P dan Klausul Model C2C yang berlaku, harap perhatikan hal-hal berikut:

- Lampiran 1 (Pengekspor dan Pengimpor): GSK atau penerima layanan GSK yang relevan yang berlokasi di UE dan/atau Britania Raya berdasarkan perjanjian(-perjanjian) dengan Pemasok adalah Pengekspor Data sehubungan dengan Informasi Pribadi GSK. Pemasok adalah Pengimpor Data sehubungan dengan Informasi Pribadi GSK
- Lampiran 1 (Deskripsi Pengalihan): harap baca definisi Informasi Pribadi dan Layanan yang akan disediakan oleh Pengimpor. Data sensitif tidak dialihkan. Frekuensi pengalihan bersifat terus-menerus. Sifat kegiatan pemrosesan dan tujuan pengalihan ditetapkan dalam perjanjian(-perjanjian) dengan Pemasok. Data akan disimpan sesuai dengan kebijakan penyimpanan data Pengekspor Data.
- Lampiran 1 (Otoritas yang Berwenang): sebagaimana diatur dalam pasal 13 Klausul Model C2C dan Klausul Model C2P
- Lampiran 2 (Langkah-langkah Teknis dan Organisasi):: harap baca Langkah-langkah Keamanan yang ditetapkan di bawah ini

Para pihak menyetujui bahwa opsi 2 dari klausul 9 "Penggunaan Subpemroses" dari Klausul Model C-P akan berlaku apabila Pemasok menggunakan subpemroses dan Pemasok, serta subpemroses harus menyetujui untuk mematuhi **Klausul Model P-P**, yang berarti i) Lampiran beserta MODUL TIGA: Pengalihan pemroses ke pemroses (tersedia **di sini**) dan tercakup di sini melalui penyebutan sebagaimana diperbarui, diubah, diganti, atau digantikan dari waktu ke waktu oleh Komisi Eropa; dan/atau (ii) perjanjian atau adendum pengalihan data internasional yang sesuai atau setara dengan Klausul Model yang digunakan oleh otoritas pengawas di Inggris Raya;

Apabila Pemasok tidak yakin dapat memenuhi persyaratan sebagaimana ditetapkan secara wajar oleh GSK, Pemasok harus segera memberi tahu GSK tentang ketidakmampuannya dan GSK berhak mengakhiri Perjanjian.

Para Pihak menyetujui bahwa Klausul Model yang ditandatangani akan berlaku di negara-negara di luar Wilayah Ekonomi Eropa apabila: (i) ketentuannya diakui sebagai perlindungan yang sesuai sehubungan dengan pengalihan internasional Data Pribadi ke negara-negara dengan tingkat perlindungan yang tidak memadai atau (ii) Undang-undang Perlindungan Data mewajibkan adanya ketentuan kontrak untuk melindungi pengalihan internasional Informasi Pribadi. Dalam menafsirkan Klausul Model, di negara-negara tersebut, setiap penyebutan istilah "Negara Anggota tempat pengekspor data didirikan" akan ditafsirkan sebagai negara tempat entitas GSK didirikan; dan setiap penyebutan Peraturan (UE) Nomor 679 Tahun 2016 harus sesuai dengan undang-undang negara tempat GSK didirikan di luar EEA. Setiap penyebutan "Negara yang Memadai" berarti setiap negara yang dianggap menyediakan, atau yang menyediakan, tingkat perlindungan yang setara untuk tujuan Undang-Undang Perlindungan Data yang berlaku, di negara-negara di luar Wilayah Ekonomi Eropa di mana Klausul Model harus mencakup pengalihan Data Pribadi.

Langkah-langkah Keamanan

"Data GSK" berarti setiap data atau informasi yang diberikan oleh atau atas nama GSK atau diperoleh Pemasok atau Personel Pemasok sehubungan dengan negosiasi dan pelaksanaan Perjanjian atau pelaksanaan kewajiban Pemasok berdasarkan Perjanjian, termasuk data tersebut dan informasi yang: (i) dibuat, dihasilkan, dikumpulkan, atau diproses oleh Personel Pemasok dalam pelaksanaan kewajiban Pemasok berdasarkan Perjanjian, atau (ii) berada di atau diakses melalui sistem informasi GSK atau sistem informasi Pemasok, serta setiap data dan informasi yang diperoleh dari hal-hal tersebut di atas.

"**Pemrosesan**" berarti setiap operasi atau serangkaian operasi yang dilakukan pada informasi atau data apa pun, baik dengan cara otomatis maupun tidak, seperti pengumpulan, perekaman, pengorganisasian, penataan, penyimpanan, penyesuaian atau perubahan, pengambilan, konsultasi, penggunaan, pengungkapan melalui transmisi, penyebaran atau penyediaan dengan cara lain, penyelarasan atau penggabungan, pembatasan, penghapusan, atau pemusnahan.

"Lingkungan Pemasok" berarti kombinasi perangkat keras, perangkat lunak, sistem operasi, sistem basis data, alat, dan komponen jaringan yang digunakan oleh atau atas nama Pemasok untuk menerima, memelihara, Memproses, menyimpan, mengakses, atau mengirimkan Data GSK.

"Personel Pemasok" berarti setiap dan semua personil yang dilibatkan atau dipekerjakan oleh Pemasok dan Subkontraktornya untuk melaksanakan setiap bagian dari Layanan.

Daftar Keamanan ini merupakan bagian dari Perjanjian oleh dan antara GSK dan Pemasok. Apabila terjadi pertentangan sehubungan dengan keamanan siber antara ketentuan Daftar Keamanan ini dan ketentuan Perjanjian, Daftar Keamanan ini yang akan berlaku. Istilah-istilah dalam huruf besar yang tidak didefinisikan dalam Daftar Keamanan ini akan memiliki makna yang dianggap berasal dari istilah-istilah tersebut di bagian lain dari Perjanjian.

1. Tanggung Jawab. Pemasok akan: (a) menggunakan kontrol enkripsi yang kuat untuk melindungi semua Data GSK dari pengungkapan, akses, atau perubahan yang tidak sah saat transit masuk atau keluar dari Lingkungan Pemasok melalui jaringan pihak ketiga; (b) menjaga proses pengendalian sesuai dengan praktik terbaik industri untuk mendeteksi, mencegah, dan memulihkan dari malware, virus, dan spyware, termasuk memperbarui perangkat lunak antivirus, anti-malware, dan anti-spyware secara berkala; (c) menjaga kebijakan, prosedur, dan pengendalian teknis manajemen akses sesuai dengan praktik terbaik industri untuk memastikan semua akses ke Data GSK yang berada dalam kendalinya mendapatkan otorisasi yang sesuai.

2. Pelanggaran Keamanan. Pemasok akan melaporkan kepada GSK melalui email ke cstd@gsk.com tentang setiap penggunaan tidak disengaja, tidak sah, atau melanggar hukum, kehilangan, pemusnahan, pengungkapan, akses, kerusakan, modifikasi, penjualan, penyewaan, atau Pemrosesan Data GSK lainnya ("**Pelanggaran Keamanan**") dalam waktu dua puluh empat (24) jam setelah Pemasok memverifikasinya. Pemasok akan memastikan bahwa semua peristiwa keamanan yang melibatkan Data GSK dikelola sesuai dengan prosedur tanggap peristiwa yang sesuai, Pemasok akan bekerja sama dengan GSK dengan iktikad baik untuk mengidentifikasi penyebab utama dan memulihkan Pelanggaran Keamanan.

ACCORDO PRIVACY

TERMINI DI PROTEZIONE DEI DATI – INFORMAZIONI PERSONALI DI BASE

Per Affiliata coperta si intende ogni Affiliata di GSK che beneficia dei Servizi come terza parte (un elenco delle quali sarà fornito da GSK al Fornitore su richiesta). Un'Affiliata è un'entità che, in relazione a qualsiasi altra entità, è controllata da, soggetta a controllo comune con, o che controlla, tale altra entità. Per "Controllo" e i suoi derivati si intende la proprietà (diretta o indiretta) di una maggioranza delle azioni con diritto di voto di tale entità o la capacità (diretta o indiretta) di nominare una maggioranza degli amministratori di tale entità o l'autorità di orientare l'amministrazione o le politiche di tale entità, per contratto o altrimenti.

Per **"Leggi in materia di protezione dei dati"** si intendono: (a) il regolamento generale sulla protezione dei dati (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, nonché eventuali leggi e/o normative applicabili che attuano e/o esercitano deroghe in virtù dello stesso e/o lo sostituiscono o lo rimpiazzano (**GDPR**); (b) il GDPR adattato dalla legge britannica in materia di protezione dei dati del 2018; (c) la legge californiana sulla privacy dei consumatori del 2018 (codice civile della California 1798.100 – 1798.199) (**CCPA**); e (d) tutte le altre leggi riguardanti il trattamento dei dati personali.

Per **"Informazioni personali"** si intendono i dati personali che rientrano nella seguente categoria: nome e/o cognome, iniziali, dettagli del referente in ambito lavorativo, adesioni a gruppi, numero di identificazione della rete o dell'utente, credenziali di accesso, percorso e competenze professionali, sesso o titolo, partecipazione ad eventi dedicati a dipendenti e lavoratori complementari di GSK che usano i Servizi.

Per **"Informazioni personali di GSK"** si intendono tutte le Informazioni personali che: (i) siano fornite da o per conto di GSK al Fornitore (anche laddove il Fornitore abbia accesso alle Informazioni personali conservate da GSK o per suo conto) oppure che il Fornitore raccolga o generi per conto di GSK; (ii) siano trattate dal Fornitore ai sensi o in relazione all'Accordo; e (iii) per le quali GSK sia un titolare del trattamento o il proprietario (o equivalente).

Per **"Programma di sicurezza"** si intende *il programma di sicurezza informatica allegato al presente come Appendice 1.*

I termini **titolare del trattamento, valutazione d'impatto sulla protezione dei dati, interessato, dati personali, violazione dei dati personali, responsabile del trattamento, trattamento, fornitore di servizi** e **autorità di controllo** saranno definiti ai sensi delle Leggi sulla protezione dei dati pertinenti. Qualsiasi riferimento a GSK indicherà l'entità contraente GSK utilizzata nell'Accordo, nonché le Affiliate interessate.

Termini del Responsabile del trattamento

Nel caso in cui il Fornitore agisca in qualità di responsabile del trattamento delle Informazioni personali di GSK ai sensi delle Leggi sulla protezione dei dati pertinenti, si applicheranno i seguenti termini:

1. Ciascuna parte dovrà rispettare i propri obblighi ai sensi delle Leggi applicabili in materia di protezione dei dati. GSK e il Fornitore convengono che, in relazione alle Informazioni personali di GSK trattate ai sensi del presente Accordo, GSK sarà il titolare del trattamento e il Fornitore sarà il responsabile del trattamento. Ai fini del CCPA, il Fornitore è un fornitore di servizi per GSK e il trattamento delle Informazioni personali di GSK da parte del Fornitore deve essere intrapreso solo per le finalità di GSK in conformità al presente Programma, purché non venga corrisposto un corrispettivo monetario o di altro valore dal Fornitore a GSK e, pertanto, GSK non venda le proprie Informazioni personali al Fornitore come definito dal CCPA.

2. Il Fornitore dovrà rispettare quanto segue in relazione alle Informazioni personali di GSK:

a) Trattare le Informazioni personali di GSK solo in base alle legittime istruzioni scritte di GSK ed esclusivamente ai fini della fornitura di Servizi da parte del Fornitore a GSK ai sensi del presente Accordo, per la durata dell'Accordo o qualsiasi periodo aggiuntivo indicato nell'Accordo, se applicabile.

b) Né il Fornitore, né alcuno dei suoi dipendenti, agenti, consulenti o assegnatari avrà alcun diritto di trattare le Informazioni personali di GSK per un proprio beneficio commerciale, sotto qualsiasi forma.

c) Implementare e mantenere adeguate misure di sicurezza tecniche e organizzative, incluse, a titolo esemplificativo ma non esaustivo, le misure stabilite nel Programma di sicurezza. I riferimenti nel Programma di sicurezza a "Dati di GSK" includeranno le Informazioni personali di GSK.

d) Mantenere riservate le Informazioni personali di GSK in conformità ai termini del presente Programma e i riferimenti in questo Programma e nel Programma di sicurezza alle Informazioni riservate di GSK includeranno le Informazioni personali di GSK.

e) Imporre obblighi di riservatezza equivalenti agli obblighi stabiliti ai sensi dell'Accordo al personale competente con accesso alle Informazioni personali di GSK.

f) Non incaricare un altro responsabile del trattamento ("**sub-responsabile del trattamento**") senza la previa approvazione scritta di GSK (e per queste finalità GSK acconsente alle seguenti categorie di sub-responsabili del trattamento: fornitori di servizi per infrastrutture di hosting, l'incarico di singoli appaltatori e sub-responsabili del trattamento resi noti a GSK al momento della stipula dell'Accordo) e trasferire le Informazioni personali di GSK a tali sub-responsabili del trattamento autorizzati esclusivamente ai sensi di un contratto scritto che impone obblighi coerenti con quelli stabiliti nel presente Programma. Quando il Fornitore nomina un sub-responsabile del trattamento in linea con la presente clausola 2(f), rimane responsabile per gli atti e le omissioni del sub-responsabile del trattamento.

g) Prestare ragionevole assistenza a GSK (i) nell'esecuzione di eventuali valutazioni d'impatto sulla protezione dei dati e/o sul trasferimento dei dati; (ii) nel rispetto dei diritti degli interessati; e (iii) nella risposta alle richieste di qualsiasi autorità di controllo in relazione alle Informazioni personali di GSK.

h) Informare GSK tempestivamente dopo essere venuto a conoscenza di una violazione dei dati personali in relazione a qualsiasi Informazione personale di GSK e fornire assistenza a GSK in relazione a tale violazione.

i) Informare GSK senza indugio se riceve una richiesta scritta da (i) un interessato di esercitare uno qualsiasi dei propri diritti in relazione alle Informazioni personali di GSK ai sensi delle Leggi sulla protezione dei dati; o (ii) un'autorità di controllo in relazione al trattamento delle Informazioni personali di GSK.

j) Se non diversamente stabilito nell'Accordo, restituire o distruggere tutte le Informazioni personali di GSK in proprio possesso o sotto il proprio controllo (comprese quelle trattate da sub-responsabili del trattamento autorizzati) alla risoluzione o alla scadenza dell'Accordo; e

k) su richiesta scritta di GSK, fornirle le informazioni ragionevolmente necessarie per dimostrare la conformità al presente Programma, che possono includere eventuali rapporti di verifica della sicurezza di terze parti disponibili.

Termini del Titolare del trattamento

Nel caso in cui il Fornitore agisca in qualità di titolare del trattamento delle Informazioni personali di GSK ai sensi delle Leggi sulla protezione dei dati pertinenti, si applicheranno i seguenti termini:

1. Ciascuna parte agisce in qualità di titolare autonomo del trattamento e dovrà rispettare i propri obblighi ai sensi delle Leggi applicabili in materia di protezione dei dati. GSK e il Fornitore convengono che, in relazione ai dati personali trattati ai sensi del presente Programma, ai fini del CCPA, nessun corrispettivo monetario o di altro valore verrà corrisposto dal Fornitore a GSK in cambio delle Informazioni personali di GSK; pertanto, GSK non vende le proprie Informazioni personali al Fornitore come definito dal CCPA.

2. Se il Fornitore riceve una comunicazione da un'autorità di controllo che si riferisce direttamente o indirettamente a: (a) il trattamento delle Informazioni personali di GSK da parte del Fornitore; o (b) il potenziale inadempimento delle Leggi sulla protezione dei dati in relazione al trattamento delle Informazioni personali di GSK, il Fornitore dovrà, nella misura consentita dalle leggi applicabili, inoltrare tempestivamente la comunicazione a GSK e fornirle ragionevole collaborazione e assistenza in merito alla questione.

3. Se un interessato avanza una richiesta scritta a una delle parti, per esercitare uno qualsiasi dei propri diritti ai sensi delle Leggi sulla protezione dei dati in relazione alle Informazioni personali di GSK, la parte ricevente dovrà rispondere a tale richiesta in conformità alle Leggi sulla protezione dei dati. Nella misura in cui la richiesta riguardi il trattamento delle Informazioni personali di GSK effettuato dall'altra parte, la parte ricevente dovrà: (i) inoltrare tempestivamente e senza indebito ritardo la richiesta all'altra parte; e (ii) collaborare e fornire ragionevole assistenza in relazione a tale richiesta per consentire all'altra parte di rispondere in conformità alle Leggi sulla protezione dei dati.

4. Senza limitare alcuna disposizione del Programma di sicurezza, una volta venuto a conoscenza di una violazione dei dati personali che interessi le Informazioni personali di GSK, il Fornitore dovrà (a) informare tempestivamente GSK e fornirle una descrizione ragionevole della violazione; e (b) non pubblicare alcuna comunicazione riguardante la violazione senza prima consultare GSK, fermo restando che può notificare la violazione a un'autorità di controllo nella misura richiesta dalla Legge applicabile in materia di protezione dei dati.

Trasferimento internazionale dei dati

Laddove GSK, agendo in qualità di esportatore, trasferisca le proprie Informazioni personali al Fornitore, che agisce in qualità di importatore, in modo da costituire un trasferimento di dati internazionale limitato ai sensi delle Leggi sulla protezione dei dati applicabili, entrambe le parti avranno stipulato e rispetteranno le pertinenti Clausole tipo che disciplinano il rapporto tra le parti:

- Allegato alla decisione di esecuzione della Commissione sulle clausole contrattuali tipo per il trasferimento di dati personali verso Paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ("**Allegato**") insieme al MODULO UNO: Trasferimento da titolare del trattamento a titolare del trattamento (disponibile **qui**) e parte integrante del presente documento per rimando, come aggiornato, modificato, sostituito o integrato di volta in volta dalla Commissione europea; e/o (ii) qualsiasi accordo o clausola aggiuntiva sul trasferimento di dati internazionale corrispondente o equivalente alle Clausole tipo adottate dall'autorità di controllo nel Regno Unito ("**Clausole tipo C2C**").
- L'Allegato insieme al MODULO DUE: Trasferimento da titolare del trattamento a responsabile del trattamento (disponibile **qui**) e parte integrante del presente documento per rimando come aggiornato, emendato, sostituito o integrato di volta in volta dalla Commissione europea; e/o (ii) qualsiasi accordo o clausola aggiuntiva sul trasferimento di dati internazionale corrispondente o equivalente alle Clausole tipo adottate dall'autorità di controllo nel Regno Unito ("**Clausole tipo C2P**").

"**Clausole tipo**" indica l'Allegato insieme alle Clausole tipo C2C e alle Clausole tipo C2P.

Ai fini delle Clausole tipo, le parti convengono che:

- L'opzione tra parentesi quadre della Clausola 11 "Ricorso" non si applica.
- Per la Clausola 17 "Legge applicabile" si seleziona l'opzione uno e si applicherà la legge italiana.
- Gli organi giurisdizionali italiani avranno giurisdizione ai sensi della Clausola 18 "Foro competente e giurisdizione".

Ai fini delle Clausole tipo C2P e delle Clausole tipo C2C applicabili, si prega di notare quanto segue:

- Allegato 1 (Esportatore e Importatore): GSK o i pertinenti destinatari del servizio GSK situati nell'UE e/o nel Regno Unito, ai sensi dell'accordo o degli accordi con il Fornitore, è/sono Esportatore/i in relazione alle Informazioni personali di GSK. Il Fornitore è un importatore in relazione alle Informazioni personali di GSK.

- Allegato 1 (Descrizione dei trasferimenti): si veda la definizione di Informazioni personali e Servizi fornita dall'Importatore. Non vengono trasferiti dati sensibili. La frequenza del trasferimento è continua. La natura delle attività di trattamento e le finalità del trasferimento sono stabilite nell'accordo o negli accordi con il Fornitore. I dati saranno conservati in linea con le politiche di conservazione dei dati dell'Esportatore.
- Allegato 1 (Autorità competenti): come stabilito nella clausola 13 delle Clausole tipo C2C e Clausole tipo C2P.
- Allegato 2 (Misure tecniche e organizzative): si vedano le Misure di sicurezza indicate di seguito.

Le parti convengono che l'opzione 2 della clausola 9 "Ricorso ai Sub-responsabili del trattamento" delle Clausole tipo C-P si applicherà laddove il Fornitore incarichi un sub-responsabile del trattamento e il Fornitore e il sub-responsabile del trattamento si impegnino a rispettare le **Clausole tipo P-P**, ovvero i) l'Allegato insieme al MODULO TRE: Trasferimento da responsabile del trattamento a responsabile del trattamento (disponibile **qui**) e parte integrante del presente documento per rimando, come aggiornato, emendato, sostituito o integrato di volta in volta dalla Commissione europea; e/o (ii) qualsiasi accordo o clausola aggiuntiva sul trasferimento di dati internazionale corrispondente o equivalente alle Clausole tipo adottate dall'autorità di controllo nel Regno Unito.

Nel caso in cui il Fornitore non ritenga di poter soddisfare i requisiti ragionevolmente stabiliti da GSK, il Fornitore dovrà informare immediatamente GSK della sua incapacità e GSK avrà il diritto di risolvere l'Accordo.

Le Parti convengono che le Clausole tipo stipulate avranno effetto in Paesi al di fuori dello Spazio economico europeo dove: (i) le loro disposizioni sono riconosciute come una salvaguardia appropriata in relazione ai trasferimenti internazionali di Dati personali verso Paesi che non forniscono una protezione adeguata o (ii) le Leggi sulla protezione dei dati richiedono l'esistenza di disposizioni contrattuali volte a proteggere i trasferimenti internazionali di Informazioni personali. Nell'interpretazione delle Clausole tipo, in tali Paesi, qualsiasi riferimento all'espressione "Stato membro in cui l'esportatore ha sede" sarà interpretato come il Paese in cui ha sede l'entità GSK; e qualsiasi riferimento al Regolamento (UE) 2016/679 rimanderà alla legge del Paese in cui GSK ha sede al di fuori del SEE. Per "Paese adeguato" si intende qualsiasi Paese che sia ritenuto fornire, o che altrimenti fornisca, un livello equivalente di protezione ai fini delle Leggi applicabili in materia di protezione dei dati, in quei Paesi al di fuori dello Spazio economico europeo in cui le Clausole tipo si applicano ai trasferimenti di Dati personali.

Misure di sicurezza

Per **"Dati di GSK"** si intendono quei dati o quelle informazioni forniti da o per conto di GSK od ottenuti dal Fornitore o dal Personale del Fornitore in relazione alla negoziazione ed esecuzione dell'Accordo o all'adempimento degli obblighi del Fornitore ai sensi dell'Accordo, compresi quei dati e quelle informazioni che: (i) sono creati, generati, raccolti o trattati dal Personale del Fornitore nell'adempimento degli obblighi del Fornitore ai sensi dell'Accordo, o (ii) sono ubicati presso o sono accessibili attraverso i sistemi informativi di GSK o del Fornitore, nonché dati e informazioni derivati da quanto sopra.

Per "**Trattamento**" si intende qualsiasi operazione o serie di operazioni effettuate su qualsiasi informazione o dato, con l'ausilio di processi automatizzati o meno, quali, ad esempio, la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, l'allineamento o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Per **"Ambiente del Fornitore**" si intende la combinazione di hardware, software, sistemi operativi, sistemi di database, strumenti e componenti di rete utilizzati da o per conto del Fornitore per ricevere, mantenere, trattare, conservare, accedere o trasmettere i Dati di GSK.

Per **"Personale del Fornitore"** si intende tutto il personale incaricato o assunto dal Fornitore e dai suoi Subappaltatori per eseguire qualsiasi parte dei Servizi.

Il presente Programma di sicurezza fa parte dell'Accordo tra GSK e il Fornitore. In caso di conflitto in materia di sicurezza informatica tra i termini del presente Programma di sicurezza e i termini dell'Accordo, prevarrà il presente Programma di sicurezza. I termini in maiuscolo non definiti nel presente Programma di sicurezza avranno il significato loro attribuito in altre parti dell'Accordo.

1. Responsabilità. Il Fornitore dovrà: (a) avvalersi di severi controlli di crittografia al fine di tutelare tutti i Dati di GSK da divulgazione, accesso o modificazione non autorizzati in transito verso o dall'ambiente del Fornitore su reti di terzi; (b) mantenere processi di controllo in linea con la migliore prassi di settore al fine di rilevare, impedire e ripristinare dopo un attacco di malware, virus e spyware, anche tramite aggiornamenti periodici di software antivirus, anti-malware e anti-spyware; (c) e mantenere politiche, procedure e controlli tecnici di gestione degli accessi in linea con la migliore prassi di settore, per garantire che tutti gli accessi ai Dati di GSK sotto il proprio controllo siano debitamente autorizzati.

2. Violazione della sicurezza. Il Fornitore segnalerà a GSK, inviando un'e-mail all'indirizzo cstd@gsk.com, qualsiasi uso, perdita, distruzione, divulgazione, accesso, corruzione, modifica, vendita, noleggio o altro Trattamento di Dati di GSK (una "**Violazione della sicurezza**") accidentale, non autorizzato o illecito verificatosi, entro ventiquattro (24) ore dalla verifica del Fornitore. Il Fornitore farà in modo che tutti gli incidenti di sicurezza aventi a oggetto Dati di GSK siano gestiti in conformità ad adeguate procedure di risposta agli incidenti e collaborerà con GSK in buona fede per individuarne la causa determinante e sanare la Violazione della sicurezza.

別表

データ保護規約 - 基本個人情報

対象関連会社とは、第三者として本サービスの利益を享受するGSKの各関連会社（当該リストは要請に応じてGSKから本サプライヤーに提供される）をいいます。関連会社とは、他の事業体から支配を受けている事業体、他の事業体と共通の支配下にある事業体、または他の事業体を支配している事業体をいいます（他の事業体についてはいずれの事業体であるかを問わない）。「支配」およびその派生とは、当該事業体の株式の議決権のうち過半数を（直接的または間接的に）所有すること、当該事業体の取締役の過半数を（直接的または間接的に）指名できること、または契約その他により当該事業体の経営や政策について指示する権限があることをいいます。

データ保護法とは、(a)個人データの取り扱い、および当該データの自由な移転に関する自然人の保護を規定する一般データ保護規則（EU）2016/679、それに基づく修正を具体化および／もしくは執行する適用法規、ならびに／またはそれに代替しもしくはそれを廃止するもの（**GDPR**）、(b)2018年英国データ保護法によって修正されたGDPR、(c)2018年カリフォルニア州消費者プライバシー法（カリフォルニア州民法第1798.100条 - 第1798.199条）（**CCPA**）、ならびに(d)個人データの処理に関するその他すべての法をいいます。

個人情報とは、次の項目の範囲内の個人データをいいます。すなわち、名前および／または名字、頭文字、勤務先情報、所属組織、ネットワークまたはユーザー識別番号、ログイン資格、職歴と技能、性別もしくは敬称、本サービスを使用するGSKの従業員と臨時職員によるイベントの出席。

GSK個人情報とは、(i)GSKもしくはGSKの代理人がサプライヤーに提供する個人情報（GSKもしくはGSKの代理人の保有する個人情報に対するアクセス権をサプライヤーが有する場合を含む）、またはサプライヤーがGSKの代理人として収集もしくは生成する個人情報、(ii)サプライヤーが本契約に基づき、もしくは関連して処理する個人情報、および(iii)GSKが、関連する支配者または所有者（もしくはそれに相当する者）である個人情報をいいます。

セキュリティ別表とは、*本別表に付録1として添付されるサイバーセキュリティに関する別表*をいいます。

管理者、データ保護影響評価、データ主体、個人データ、個人データ侵害、処理者、処理、サービスプロバイダーおよび**監督当局**という用語については、関連するデータ保護法に基づいて定義されるところによります。GSKについての言及がある場合、それは本契約で使用され、GSKが契約している事業体、および対象関連会社を意味します。

処理者に関する規約

関連するデータ保護法に基づいてサプライヤーがGSK個人情報の処理者となる場合、次の規約が適用されるものとします。

1. 各当事者は、適用されるデータ保護法に基づき自らの義務を遵守するものとします。GSKおよびサプライヤーは、本契約に基づいて処理されるGSK個人情報に関し、GSKが管理者となり、サプライヤーが処理者となることに同意します。CCPAの趣旨から、サプライヤーは、GSKに対するサービスプロバイダーとなり、サプライヤーによるGSK個人情報の処理は、本別表に従い、GSKの目的のためにのみこれを引き受けるものとします。サプライヤーは、いかなる金銭その他有価約因もGSKに提供せず、それにしたがい、GSKは、CCPAの規定に則り、GSK個人情報をサプライヤーに売却しないものとします。

2. サプライヤーは、GSK個人情報に関し、次の事項を遵守するものとします。

   a) GSK個人情報を、GSKの適法な書面による指示によってのみ処理します。また、サプライヤーが、本契約に基づき、本契約期間または本契約に規定される追加の期間（該当する場合）にわたり、GSKに本サービスを提供する目的でのみ処理します。

   b) その形式を問わず、サプライヤー、およびその従業員、代理人、コンサルタント、もしくは譲受人は、自身の営業上の利益のためにGSK個人情報を処理する権利を有さないものとします。

   c) 適切な技術的および組織的なセキュリティ措置を講じ、維持します。これにはセキュリティ別表に規定する措置も含まれますが、これに限定されません。セキュリティ別表で言及される「GSKデータ」には、GSK個人情報が含まれるものとします。

   d) 本別表の条件に従い、GSK個人情報を機密として保持します。本別表およびセキュリティ別表で言及されるGSK機密情報には、GSK個人情報が含まれるものとします。

   e) GSK個人情報に対するアクセス権を有する関連職員に対し、本契約に規定する義務に相当する機密保持義務を課します。

   f) GSKの書面による事前の承認（また同趣旨から、インフラストラクチャサービスプロバイダーのホスティング、個人請負業者の利用、本契約の締結時点でGSKに認識されていた復処理者に対するGSKの同意）がない限り、他の処理者（「**復処理者**」）を関与させないものとします。また、書面による契約により本別表に規定する義務と一致する義務を課す場合にのみ、当該承認済みの復処理者にGSK個人情報を転送します。本条2(f)に従ってサプライヤーが復処理者を指名した場合、サプライヤーはそれ以降、復処理者の作為および不作為に対して責任を負います。

g) (i)法律によって求められるデータ保護影響評価および／またはデータ転送影響評価の実施、(ii)データ主体の権利の遵守、(iii)GSK個人情報に関する監督当局からの要請に対する対応のそれぞれについて、GSKに合理的な支援を行います。

h) GSK個人情報に関する個人データ侵害を認識した後、GSKに遅滞なく通知し、GSKに当該侵害に関する支援を行います。

i) (i)データ保護法に基づきGSK個人情報に関する自身の権利を行使するためのデータ主体からの書面による要請、または(ii)GSK個人情報の処理に関する監督当局からの書面による要請を受理した場合、GSKに遅滞なく通知します。

j) 本契約に特段の規定がある場合を除き、本契約の解除または期間満了があった場合、保有するまたは管理下にあるすべてのGSK個人情報（承認済み復処理者が保有するGSK個人情報を含む）を返却または破棄します。

k) GSKの書面による要請に基づき、本別表の遵守を明らかにする上で必要となる合理的な情報をGSKに提供します。これには入手可能な第三者によるセキュリティ監査報告書が含まれる場合があります。

管理者に関する規約

関連するデータ保護法に基づいてサプライヤーがGSK個人情報の管理者となる場合、次の規約が適用されるものとします。

1. 各当事者は、独立した管理者となり、適用されるデータ保護法に基づき自らの義務を遵守するものとします。GSKおよびサプライヤーは次の事項に同意します。サプライヤーは、CCPAの趣旨から、本別表に基づいて処理される個人データに関し、GSK個人情報と引き換えにいかなる金銭またはその他有価約因もGSKに提供せず、それにしたがい、GSKは、CCPAの規定に則り、GSK個人情報をサプライヤーに売却しないものとします。
2. サプライヤーが監督当局から(a)サプライヤーによるGSK個人情報の処理、または(b)GSK個人情報の処理に関するデータ保護法遵守違反の可能性に直接的または間接的に関連する連絡を受けた場合、サプライヤーは、適用法で認められる範囲で、速やかに当該連絡をGSKに転送し、同内容に関してGSKに合理的な協力および支援を行います。
3. データ主体が、GSK個人情報に関し、データ保護法に基づく権利を実行する旨をいずれかの当事者に書面で要請した場合、受領当事者は、データ保護法に従い当該要請に対応するものとします。他方当事者が請け負っているGSK個人情報の処理に当該要請が関連する範囲において、受領当事者は、(i)過度の遅滞なく速やかに当該要請を他方当事者に転送するものとし、(ii)他方当事者がデータ保護法に従った対応ができるよう、当該要請に関する協力と合理的な支援を提供するものとします。
4. セキュリティ別表の規定に限らず、GSK個人情報に影響する個人データ侵害を認識した場合、サプライヤーは(a)速やかにGSKに通知し、GSKに当該侵害についての合理的な説明を提供するものとします。また、(b)適用されるデータ保護法により要求される範囲において当該侵害について監督当局に通知する場合を除き、最初にGSKと協議することなく当該侵害についての情報を公開しないものとします。

国際的なデータ転送

適用されるデータ保護法に基づき、制限付き国際的データ転送を構成する方法でGSK（データ輸出者）がGSK個人情報をサプライヤー（データ輸入者）に転送する場合、両当事者は本別表に従い、両当事者間の関係を対象範囲として適用されるモデル条項を締結し、遵守するものとします。

- 欧州議会および理事会規則(EU)2016/679に基づく個人データの第三国への転送についての標準契約条項に関する委員会実施決定の付属書（「**付属書**」）およびモジュール1：管理者間の転送（こちらで閲覧可）であって、欧州委員会により随時更新、改訂、代替、廃止される資料によって本別表に組み込まれるもの、ならびに／または(ii)対応するもしくは相当する国際的なデータ転送契約または英国の監督当局が採択したモデル条項の補遺（「**C2Cモデル条項**」）。
- 付属書およびモジュール2：管理者・処理者間の転送（こちらで閲覧可）であって、欧州委員会により随時更新、改訂、代替、廃止される資料によって本別表に組み込まれるもの、ならびに／または(ii)対応するもしくは相当する国際的なデータ転送契約または英国の監督当局が採択したモデル条項の補遺（「C2Pモデル条項」）。

「**モデル条項**」とは、C2Cモデル条項およびC2Pモデル条項に付属書を併せたものをいいます。

モデル条項の趣旨から、両当事者は次の事項に合意します。

- 第11条「救済」における角括弧の選択肢は適用されない
- 第17条「準拠法」については選択肢1を選択し、アイルランド法が適用される
- アイルランドの裁判所は第18条「裁判地および法域の選択」に基づく管轄権を有する

適用されるC2Pモデル条項およびC2Cモデル条項の趣旨から、次の事項に留意してください。

- 付属書1(輸出者および輸入者):GSKまたは関連するGSKサービス受領者(サプライヤーとの本契約に基づく所在地がEUおよび/または英国である者)は、GSK個人情報に関するデータ輸出者です。サプライヤーは、GSK個人情報に関するデータ輸入者です。
- 付属書1(転送の説明):輸入者から提供される個人情報および本サービスの定義をご確認ください。機微情報は転送されません。転送の頻度は連続的です。処理活動の性質と転送の目的はサプライヤーとの契約に規定されています。データは、データ輸出者のデータ保持ポリシーに従って保持されます。
- 付属書1(管轄当局):C2Cモデル条項およびC2Pモデル条項の第13条の規定に従います。
- 付属書2(技術的および組織的措置):以下に規定するセキュリティ措置をご確認ください

両当事者は、サプライヤーが復処理者を関与させる場合、C2Pモデル条項の第9条「復処理者の使用」の選択肢2が適用されることに同意します。また、サプライヤーおよび復処理者は、**P2Pモデル条項**を遵守することに同意します。i) ここでP2Pモデル条項とは、付属書およびモジュール3:処理者間の転送(こちらで閲覧可)であって、欧州委員会により随時更新、改訂、代替、廃止される資料によって本別表に組み込まれるもの、ならびに/または(ii)対応するもしくは相当する国際的なデータ転送契約または英国の監督当局が採択したモデル条項の補遺をいいます。

サプライヤーがGSKが合理的な範囲で規定した要件を満たすことができないと判断した場合、サプライヤーは、その不能について直ちにGSKに通知するものとし、GSKは本契約を解除する権利を有するものとします。

両当事者は、(i)締結したモデル条項の規定が、十分性認定がない国への国際的な個人データの転送に関する適切な保護手段として認められている場合、または(ii)データ保護法が個人情報の国際的な転送を保護する契約上の規定の存在を要求している場合、締結したモデル条項が欧州経済地域外の国でも効力を有することに同意します。当該国でモデル条項を解釈する場合、「データ輸出者が設立されている加盟国」という用語についての言及があれば、それはGSK事業体が設立されている国を指すものと解釈します。規則(EU)2016/679についての言及があれば、それはGSKが設立されているEEA域外の国の法を指すものとします。「十分性認定国」についての言及があれば、それは個人データの転送にモデル条項の適用がある欧州経済地域外の国の中でも、適用されるデータ保護法の趣旨に照らして相当な水準の保護を提供する旨の規制がある国、または提供している国を指すものとします。

セキュリティ措置

「GSKデータ」とは、GSKもしくはGSKの代理人が提供するデータもしくは情報、またはサプライヤーもしくはサプライヤースタッフが本契約の交渉および締結または本契約に基づくサプライヤーの義務の履行に関連して取得したデータもしくは情報をいいます。これには当該データもしくは情報のうち、(i)本契約に基づくサプライヤーの義務の履行に際してサプライヤースタッフによって作成、生成、収集、処理されたもの、および(ii)GSKの情報システムもしくはサプライヤーの情報システムで保管され、これを通じてアクセスできるもの、ならびに上記から派生するあらゆるデータおよび情報も含まれます。

「**処理**」とは、収集、記録、整理、体系化、保存、適用もしくは変更、検索、相談、使用、送信による開示、流布、またはその他提供、連携もしくは組み合わせ、制限、消去もしくは破棄など、手段が自動化されているかどうかを問わず、情報またはデータについて実施されるあらゆる操作をいいます。

「**サプライヤー環境**」とは、GSKデータを受信、管理、処理、保存、送信もしくはこれにアクセスするために、サプライヤーまたはその代理人が使用するハードウェア、ソフトウェア、オペレーティングシステム、データベースシステム、ツール、およびネットワークコンポーネントの組み合わせをいいます。

「**サプライヤースタッフ**」とは、サプライヤーおよびその再委託業者が、本サービスのいずれかの部分を実行するために契約または雇用するあらゆる人員をいいます。

本セキュリティ別表は、GSKとサプライヤー間の本契約の一部を構成するものです。本セキュリティ別表の条項と本契約の条項との間でサイバーセキュリティに関して矛盾が認められる場合、本セキュリティ別表が優先するものとします。本セキュリティ別表において定義されていない大文字の用語については、本契約の他の部分で付与されている意味を有します。

1. **責任**。サプライヤーは、(a)強力な暗号化制御を使用して、第三者ネットワークを介したサプライヤー環境に対する未承認の開示、アクセス、または通信中の変更からすべてのGSKデータを保護し、(b)業界のベストプラクティスに則って制御プロセスを管理し、アンチウイルス、アンチマルウェア、アンチスパイウェアソフトウェアを定期的に更新するなどして、マルウェア、ウイルス、スパイウェアを発見、回避、除去し、(c)業界のベストプラクティスに則ってアクセス管理ポリシー、手続、および技術制御を管理し、制御下にあるGSKデータへのすべてのアクセスが適切に承認されていることを確認します。

2. **セキュリティ侵害**。GSKデータについて偶発的、未承認、または不適法な使用、紛失、破棄、開示、アクセス、変造、改変、売却、貸与、またはその他の処理(「**セキュリティ侵害**」)を確認した場合、サプライヤーは、当該確認から24時間以内に電子メール(cstd@gsk.com)でGSKに報告します。サプライヤーは、GSKデータに関連するすべてのセキュリティインシデントが適切なイ

ンシデント対応手続に則って管理されていることを確認し、GSKと連携して誠意をもって根本原因を突き止め、当該セキュリティ侵害を修正します。

ZAŁĄCZNIK

WARUNKI OCHRONY DANYCH – PODSTAWOWE DANE OSOBOWE

Objęta jednostka stowarzyszona oznacza: każdą jednostkę stowarzyszoną GSK, który korzysta z Usług jako podmiot zewnętrzny (lista zostanie przekazana Dostawcy przez GSK na żądanie). Jednostka stowarzyszona to każdy podmiot, który w odniesieniu do jakiegokolwiek innego podmiotu jest objęty przez niego Kontrolą, znajduje się pod wspólną Kontrolą albo obejmuje go Kontrolą. Kontrola i wyrazy pochodne oznaczają posiadanie (bezpośrednie albo pośrednie) większości akcji z prawem głosu takiego podmiotu albo zdolność (bezpośrednia albo pośrednia) do wyznaczenia większości członków zarządu takiego podmiotu albo uprawnienie do kierowania zarządzaniem albo politykami takiego podmiotu na podstawie umowy albo w inny sposób;

„Przepisy prawa dotyczące ochrony danych" oznaczają: (a) ogólne rozporządzenie o ochronie danych osobowych (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz wszelkie obowiązujące przepisy prawa i/lub regulacje, które wdrażają i/lub realizują zobowiązania z niego wynikające i/lub je zastępują (**RODO**); (b) brytyjskie rozporządzenie RODO dostosowane do brytyjskiej ustawy o ochronie danych z 2018 r. (c) ustawę o ochronie danych konsumentów z 2018 r. (kodeks cywilny stanu Kalifornia 1798.100–1798.199) (**CCPA**); oraz (d) wszystkie inne przepisy dotyczące przetwarzania danych osobowych.

„Dane osobowe" to dane osobowe obejmujące imię lub nazwisko, inicjały, służbowe dane kontaktowe, członkostwo w grupach, numer identyfikacyjny sieci lub użytkownika, dane logowania, historię zatrudnienia i umiejętności, płeć lub stanowisko, obecność na wydarzeniach pracowników firmy GSK i pracowników tymczasowych korzystających z Usług.

„Dane osobowe firmy GSK" oznaczają wszelkie Dane osobowe (i) dostarczane przez firmę GSK lub w jej imieniu na rzecz Dostawcy (w tym w przypadku, gdy Dostawca ma dostęp do Danych osobowych przechowywanych przez firmę GSK lub w jej imieniu) lub które Dostawca gromadzi bądź generuje w imieniu firmy GSK; (ii) które są przetwarzane przez Dostawcę na mocy Umowy lub w związku z Umową; oraz (iii) w odniesieniu do których firma GSK jest administratorem lub właścicielem (bądź jego odpowiednikiem).

Załącznik dotyczący bezpieczeństwa oznacza *załącznik dotyczący cyberbezpieczeństwa stanowiący Załącznik 1.*

Pojęcia **„administrator", „ocena skutków dla ochrony danych", „osoba, której dane dotyczą", „dane osobowe", „naruszenie ochrony danych osobowych", „podmiot przetwarzający", „przetwarzanie", „usługodawca"** i **„organ nadzorczy"** będą definiowane zgodnie z odpowiednimi Przepisami prawa dotyczącymi ochrony danych. Jakiekolwiek odniesienia do GSK oznaczają zamawiającego ze strony GSK wskazanego w Umowie, jak również Objęte jednostki stowarzyszone.

Warunki dotyczące podmiotu przetwarzającego

W przypadku, gdy dostawca działa jako podmiot przetwarzający Dane osobowe firmy GSK zgodnie z odpowiednimi Przepisami prawa dotyczącymi ochrony danych, zastosowanie mają następujące warunki:

1. Każda ze stron będzie wywiązywać się ze swoich obowiązków wynikających z obowiązujących Przepisów prawa o ochronie danych. GSK i Dostawca uzgadniają, że w odniesieniu do Danych osobowych firmy GSK przetwarzanych na podstawie niniejszej Umowy GSK będzie administratorem, a Dostawca podmiotem przetwarzającym. Na potrzeby ustawy CCPA Dostawca jest usługodawcą świadczącym usługi na rzecz GSK, a przetwarzanie Danych osobowych firmy GSK przez Dostawcę odbywa się wyłącznie do celów GSK zgodnie z niniejszym Załącznikiem, Dostawca nie przekazuje GSK żadnych świadczeń pieniężnych ani innych świadczeń wzajemnych, w związku z czym GSK nie sprzedaje Dostawcy Danych osobowych firmy GSK zgodnie z definicją CCPA.

2. Dostawca będzie przestrzegać następujących wymogów w odniesieniu do Danych osobowych firmy GSK:

a) będzie przetwarzać Dane osobowe firmy GSK tylko na podstawie zgodnych z prawem pisemnych instrukcji GSK i wyłącznie w celu świadczenia Usług przez Dostawcę na rzecz GSK na podstawie niniejszej Umowy przez okres obowiązywania Umowy albo dowolny dodatkowy okres wskazany w Umowie, jeśli ma to zastosowanie;

b) Dostawca ani żaden z jego pracowników, przedstawicieli, konsultantów czy cesjonariuszy nie będzie mieć żadnych praw odnośnie do przetwarzania Danych osobowych firmy GSK w celu osiągnięcia własnych korzyści gospodarczych w dowolnej postaci;

c) będzie wdrażać i utrzymywać odpowiednie techniczne i organizacyjne środki bezpieczeństwa, w tym w szczególności środki określone w Załączniku dotyczącym bezpieczeństwa. Odniesienia w Załączniku dotyczącym bezpieczeństwa do „Danych GSK" obejmują Dane osobowe firmy GSK;

d) będzie zachowywać poufność Danych osobowych firmy GSK zgodnie z warunkami niniejszego Załącznika oraz zawartymi w nim odniesieniami; Załącznik dotyczący bezpieczeństwa do Informacji poufnych firmy GSK obejmuje Dane osobowe firmy GSK;

e) nałoży na odpowiedni personel mający dostęp do Danych osobowych firmy GSK obowiązek zachowania poufności równoważny obowiązkom określonym w Umowie;

f) nie będzie angażować innego podmiotu przetwarzającego („podwykonawcy przetwarzania") bez uzyskania uprzedniej pisemnej zgody GSK (w tych celach GSK wyraża zgodę na angażowanie następujących kategorii podwykonawców przetwarzania: usługodawców infrastruktury hostingowej, korzystanie z usług poszczególnych wykonawców oraz podwykonawców przetwarzania znanych GSK w momencie zawarcia Umowy) i będzie przekazywać Dane osobowe firmy GSK takim zatwierdzonym podwykonawcom przetwarzania wyłącznie na podstawie pisemnej umowy, która nakłada obowiązki zgodne z tymi określonymi w niniejszym Załączniku. Gdy Dostawca wyznacza podwykonawcę przetwarzania zgodnie z niniejszym ustępem 2(f), pozostaje on odpowiedzialny za działania i zaniechania podwykonawcy przetwarzania;

g) będzie zapewniać GSK uzasadnioną pomoc w odniesieniu do (i) przeprowadzania wszelkich wymaganych na mocy przepisów prawa ocen skutków dla ochrony danych lub ocen skutków dla przekazywania danych; (ii) zachowania zgodności w zakresie praw osób, których dane dotyczą; oraz (iii) odpowiadania na żądania jakiegokolwiek organu nadzorczego w odniesieniu do Danych osobowych firmy GSK;

h) będzie niezwłocznie powiadamiać GSK po uzyskaniu informacji o naruszeniu ochrony danych osobowych w odniesieniu do jakichkolwiek Danych osobowych GSK i zapewniać GSK pomoc w związku z takim naruszeniem;

i) będzie niezwłocznie powiadamiać GSK, jeśli otrzyma pisemne żądanie od (i) osoby, której dane dotyczą, o skorzystanie ze swoich praw w odniesieniu do Danych osobowych firmy GSK na mocy Przepisów prawa dotyczących ochrony danych; albo (ii) organu nadzorczego w związku z przetwarzaniem Danych osobowych firmy GSK;

j) o ile Umowa nie stanowi inaczej, zwróci albo zniszczy wszystkie Dane osobowe firmy GSK znajdujące się w jego posiadaniu albo pod jego kontrolą (w tym wszelkie Dane osobowe firmy GSK przetwarzane przez upoważnionych podwykonawców przetwarzania) po rozwiązaniu albo wygaśnięciu Umowy; oraz

k) na pisemny wniosek GSK będzie przekazywać GSK uzasadnione informacje niezbędne do wykazania zgodności z niniejszym Załącznikiem, które mogą obejmować wszelkie dostępne sprawozdania z audytu bezpieczeństwa podmiotów zewnętrznych.

Warunki dotyczące administratora

W przypadku gdy dostawca działa jako administrator Danych osobowych firmy GSK zgodnie z odpowiednimi Przepisami prawa dotyczącymi ochrony danych, zastosowanie mają następujące warunki:

1. Każda ze stron działa jako niezależny administrator i będzie wywiązywać się ze swoich obowiązków wynikających z obowiązujących Przepisów prawa dotyczących ochrony danych. GSK i Dostawca uzgadniają, że w odniesieniu do danych osobowych przetwarzanych na podstawie niniejszego Załącznika dla celów CCPA, Dostawca nie przekazuje GSK żadnych świadczeń pieniężnych ani innych świadczeń wzajemnych w zamian za Dane osobowe firmy GSK, w związku z czym GSK nie sprzedaje Dostawcy Danych osobowych firmy GSK zgodnie z definicją CCPA.
2. Jeśli Dostawca otrzyma jakąkolwiek korespondencję od organu nadzorczego, która odnosi się bezpośrednio albo pośrednio do a) przetwarzania Danych osobowych firmy GSK przez Dostawcę; albo (b) potencjalnego nieprzestrzegania Przepisów prawa dotyczących ochrony danych w związku z przetwarzaniem Danych osobowych firmy GSK, Dostawca, w zakresie dozwolonym przepisami obowiązującego prawa, niezwłocznie przekaże korespondencję do GSK oraz będzie w uzasadnionym zakresie współpracować z firmą GSK i zapewni jej pomoc w tej kwestii.
3. Jeżeli osoba, której dane dotyczą, złoży pisemne żądanie do którejkolwiek ze stron o skorzystanie z któregokolwiek z jej praw wynikających z Przepisów prawa dotyczących ochrony danych w odniesieniu do Danych osobowych firmy GSK, strona odbierająca odpowie na to żądanie zgodnie z Przepisami prawa dotyczącymi ochrony danych. W zakresie, w jakim żądanie dotyczy przetwarzania Danych osobowych firmy GSK przez drugą stronę, strona otrzymująca: (i) przekaże żądanie drugiej stronie natychmiast i bez zbędnej zwłoki; oraz (ii) będzie współpracować i zapewniać uzasadnioną pomoc w związku z tym żądaniem, aby umożliwić drugiej stronie udzielenie odpowiedzi zgodnie z Przepisami prawa dotyczącymi ochrony danych.
4. Bez ograniczania jakiegokolwiek postanowienia Załącznika dotyczącego bezpieczeństwa, po uzyskaniu informacji o naruszeniu ochrony danych osobowych mającym wpływ na Dane osobowe firmy GSK, Dostawca (a) niezwłocznie powiadomi firmę GSK i przekaże jej opis naruszenia w uzasadnionym zakresie; oraz (b) nie będzie publikować żadnych komunikatów dotyczących naruszenia bez uprzedniej konsultacji z GSK, z zastrzeżeniem, że może zgłosić naruszenie do organu nadzorczego w zakresie wymaganym przez obowiązujące Przepisy prawa dotyczące ochrony danych.

Przesyłanie danych za granicę:

W przypadku, gdy GSK, działając jako podmiot przekazujący dane, przekazuje Dane osobowe firmy GSK Dostawcy, który działa jako podmiot odbierający dane, w sposób, który stanowi ograniczone międzynarodowe przekazywanie danych zgodne z obowiązującymi Przepisami prawa dotyczącymi ochrony danych, obie strony niniejszym przyjmują obowiązujące Standardowe klauzule umowne dotyczące stosunków między stronami i będą ich przestrzegać:

- Załącznik do Decyzji wykonawczej Komisji w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do krajów trzecich na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (**„Załącznik”**) wraz z MODUŁEM PIERWSZYM: Przekazywanie danych pomiędzy administratorami (dostępnymi **tutaj**), włączonym do niniejszego dokumentu przez odniesienie z uwzględnieniem okresowych aktualizacji, zmian, zniesienia albo zastąpienia przez Komisję Europejską; lub (ii) wszelkie odpowiadające albo równoważne umowy międzynarodowe o przekazywanie danych albo aneksy do Standardowych klauzul umownych przyjętych przez organ nadzorczy w Wielkiej Brytanii (**„Standardowe klauzule umowne C2C”**);
- Załącznik razem z MODUŁEM DRUGIM: Przekazywanie danych pomiędzy administratorem a podmiotem przetwarzającym (dostępnym **tutaj**), włączonym do niniejszego dokumentu przez odniesienie z uwzględnieniem okresowych aktualizacji, zmian, zniesienia albo zastąpienia przez Komisję Europejską; lub (ii) wszelkie odpowiadające albo równoważne umowy międzynarodowe o przekazywanie danych albo aneksy do Standardowych klauzul umownych przyjętych przez organ nadzorczy w Wielkiej Brytanii (**„Standardowe klauzule umowne C2P”**);

„Standardowe klauzule umowne” oznaczają Załącznik wraz ze Standardowymi klauzulami umownymi C2C i Standardowymi klauzulami umownymi C2P.

Na potrzeby Standardowych klauzul umownych strony uzgadniają, że:

- Opcja w nawiasie kwadratowym w Klauzuli 11 „Dochodzenie roszczeń" nie będzie miała zastosowania
- Dla Klauzuli 17 „Prawo właściwe" wybrano opcję pierwszą i zastosowanie będzie miało prawo Irlandii.
- Na mocy Klauzuli 18 „Wybór sądu właściwego i jurysdykcji" właściwymi miejscowo sądami będą sądy Irlandii.

Na potrzeby obowiązujących Standardowych klauzul umownych C2C i Standardowych klauzul umownych C2P należy zwrócić uwagę na następujące kwestie:

- Załącznik 1 (Podmiot przekazujący i Podmiot odbierający): GSK albo odpowiedni odbiorcy usług zlokalizowani na terytorium UE lub Wielkiej Brytanii na mocy umów zawartych z Dostawcą są Podmiotami przekazującymi dane w odniesieniu do Danych osobowych firmy GSK. Dostawca to Podmiot odbierający dane w odniesieniu do Danych osobowych firmy GSK.
- Załącznik 1 (Opis przekazywania): proszę odnieść się do definicji Danych osobowych i Usług świadczonych przez Podmiot odbierający dane. Dane wrażliwe nie są przekazywane. Częstotliwość przekazywania: ciągłe. Charakter czynności przetwarzania oraz cele przekazywania określono w umowach zawartych z Dostawcą. Dane będą przechowywane zgodnie z politykami dotyczącymi przechowywania danych Podmiotu przekazującego dane.
- Załącznik 1 (Organy właściwe): zgodnie z ustępem 13 Standardowych klauzul umownych C2C i Standardowych klauzul umownych C2P.
- Załącznik 2 (Środki techniczne i organizacyjne): proszę odnieść się do Środków bezpieczeństwa określonych poniżej

Strony zgadzają się, że opcja 2 ustępu 9 „Korzystanie z Podwykonawców przetwarzania" Standardowych klauzul umownych C-P będzie mieć zastosowanie w przypadku, gdy Dostawca zaangażuje podwykonawcę przetwarzania, zaś Dostawca i podwykonawca przetwarzania zgadzają się przestrzegać **Standardowych klauzul umownych P-P**, co oznacza i) Załącznik razem z MODUŁEM TRZECIM: Przekazywanie danych pomiędzy podmiotami przetwarzającymi (dostępnym **tutaj**), włączonym do niniejszego dokumentu przez odniesienie z uwzględnieniem okresowych aktualizacji, zmian, zniesienia albo zastąpienia przez Komisję Europejską; lub (ii) wszelkie odpowiadające albo równoważne umowy międzynarodowe o przekazywaniu danych albo aneksy do Standardowych klauzul umownych przyjęte przez organ nadzorczy w Wielkiej Brytanii;

Jeżeli Dostawca uzna, że nie może spełnić wymogów przedstawionych w uzasadniony sposób przez firmę GSK, Dostawca poinformuje o tym niezwłocznie firmę GSK, zaś firmie GSK będzie przysługiwać prawo do rozwiązania Umowy.

Strony zgadzają się, że zawierane Standardowe klauzule umowne będą miały zastosowanie w krajach poza Europejskim Obszarem Gospodarczym, gdzie: (i) ich postanowienia są uznawane za odpowiednie zabezpieczenie w związku z międzynarodowym przekazywaniem Danych osobowych do krajów niezapewniających odpowiedniego poziomu ochrony albo (ii) Przepisy prawa dotyczące ochrony danych wymagają, aby postanowienia umowne chroniły międzynarodowe przekazywanie Danych osobowych. Przy interpretowaniu Standardowych klauzul umownych w tych krajach wszelkie odniesienia do „państwa członkowskiego, w którym prowadzi działalność gospodarczą podmiot przekazujący dane" będą interpretowane jako kraj w którym podmiot GSK prowadzi działalność gospodarczą; zaś wszelkie odniesienia do Rozporządzenia (UE) 2016/679 będą oznaczać przepisy prawa kraju, w którym GSK prowadzi działalność poza EOG. Wszelkie odniesienia do „Kraju zapewniającego odpowiedni poziom ochrony" będą oznaczać kraj zapewniający odpowiedni poziom ochrony do celów obowiązujących Przepisów prawa dotyczących ochrony danych należący do krajów spoza Europejskiego Obszaru Gospodarczego, gdzie Standardowe klauzule umowne obejmują przekazywanie Danych osobowych.

Środki bezpieczeństwa

„Dane firmy GSK" oznaczają wszelkie dane albo informacje udostępniane przez firmę GSK albo w jej imieniu albo pozyskiwane przez Dostawcę albo Personel Dostawcy w związku z negocjowaniem i zawieraniem Umowy albo wywiązywaniem się przez Dostawcę z obowiązków wynikających z Umowy, w tym wszelkie dane i informacje, które: (i) są tworzone, generowane, gromadzone albo przetwarzane przez Personel Dostawcy w ramach wywiązywania się z obowiązków Dostawcy wynikających z Umowy, albo (ii) są przechowywane w systemach informatycznych GSK albo Dostawcy albo uzyskuje się do nich dostęp za pośrednictwem tych systemów, a także wszelkie uzyskiwane z nich dane i informacje.

„**Przetwarzanie**" oznacza każdą operację lub zestaw operacji, które są wykonywane na jakichkolwiek informacjach lub danych, w sposób zautomatyzowany lub nie, w tym zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub modyfikowanie, pobieranie, konsultowanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub udostępnianie w inny sposób, dostosowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

„Środowisko Dostawcy" oznacza połączenie sprzętu, oprogramowania, systemów operacyjnych, systemów baz danych, narzędzi i elementów sieciowych używanych przez Dostawcę albo w jego imieniu w celu pozyskiwania, utrzymywania, Przetwarzania, przechowywania, uzyskiwania dostępu albo przekazywania Danych firmy GSK.

„Personel Dostawcy" oznacza wszelki personel zaangażowany albo zatrudniony przez Dostawcę i jego Podwykonawców w celu realizacji jakiejkolwiek części Usług.

Niniejszy Załącznik dotyczący bezpieczeństwa stanowi część Umowy zawartej pomiędzy GSK i Dostawcą. W przypadku wystąpienia jakiejkolwiek sprzeczności w związku z cyberbezpieczeństwem między postanowieniami niniejszego Załącznika dotyczącego bezpieczeństwa a postanowieniami niniejszej Umowy, niniejszy Załącznik dotyczący bezpieczeństwa będzie miał znaczenie nadrzędne. Pojęcia pisane wielką literą niezdefiniowane w niniejszym Załączniku dotyczącym bezpieczeństwa będą miały znaczenie przypisane im w innych częściach Umowy.

1. Obowiązki. Dostawca będzie korzystać z mechanizmów szyfrujących AES 256 lub innych standardów branżowych w celu ochrony wszystkich Danych firmy GSK przed nieuprawnionym ujawnieniem, dostępem lub modyfikacją w trakcie przesyłania do lub ze środowiska Dostawcy za pośrednictwem sieci osób trzecich; będzie utrzymywać procesy kontroli zgodnie z najlepszymi praktykami branżowymi w celu wykrywania ataków, zapobiegania im, i odzyskiwania danych po ataku z użyciem złośliwego oprogramowania, wirusów i oprogramowania

szpiegującego, w tym poprzez aktualizowanie oprogramowania antywirusowego, oprogramowania chroniącego przed złośliwym i szpiegującym oprogramowaniem w regularnych odstępach czasu; i będzie utrzymywać zasady zarządzania dostępem, procedury oraz techniczne środki kontroli zgodne z najlepszymi praktykami branżowymi, aby zapewnić, że wszelki dostęp do danych firmy GSK, które są pod jego kontrolą, jest odpowiednio autoryzowany.

2. Naruszenie bezpieczeństwa. Dostawca zgłosi GSK za pośrednictwem poczty elektronicznej na adres cstd@gsk.com wszelkie zweryfikowane przypadkowe, nieuprawnione albo niezgodne z prawem przypadki wykorzystania, utraty, zniszczenia, ujawnienia, uzyskania dostępu, uszkodzenia, modyfikacji, sprzedaży, wynajęcia albo innego Przetwarzania wszelkich Danych firmy GSK („Naruszenia bezpieczeństwa") w ciągu 24 (dwudziestu czterech) godzin od ich zweryfikowania przez Dostawcę. Dostawca dopilnuje, aby wszystkie incydenty związane z bezpieczeństwem danych firmy GSK były zarządzane zgodnie z odpowiednimi procedurami reagowania na incydenty i będzie współpracować z firmą GSK w dobrej wierze w celu zidentyfikowania przyczyny źródłowej i usunięcia naruszenia bezpieczeństwa informacji.

ANEXO

TERMOS DE PROTEÇÃO DE DADOS – INFORMAÇÃO PESSOAL BÁSICA

Filial Abrangida refere-se a: cada Filial da GSK que tem o benefício dos Serviços como um terceiro (cuja lista será fornecida pela GSK ao Fornecedor, mediante pedido). Uma Filial é uma entidade que, em relação a outra, é controlada, controla ou está sob o controlo comum dessa outra parte. "Controlo" e respetivos termos derivados referem-se à titularidade (direta ou indiretamente) de uma maioria das ações com direito a voto dessa entidade, à capacidade (direta ou indiretamente) de nomear a maioria dos administradores da mesma ou à autoridade para dirigir a gestão ou as políticas dessa entidade, por contrato ou de outra forma.

Legislação sobre Proteção de Dados refere-se: (a) ao Regulamento Geral sobre a Proteção de Dados (UE) 2016/679 para a proteção de pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, assim como a outra legislação e/ou regulamentação aplicáveis, que implementem e/ou apliquem derrogações ao abrigo das mesmas e/ou as substituam ou suplantem (**RGPD**); (b) ao RGPD do Reino Unido adaptado pela Lei sobre Proteção de Dados inglesa (UK Data Protection Act) de 2018; (c) à Lei da Privacidade do Consumidor da Califórnia (California Consumer Privacy Act) (artigos 1798.100 – 1798.199 do Código Civil da Califórnia) (**CCPA**); e (d) a qualquer legislação relativa ao tratamento de dados pessoais.

Informação Pessoal refere-se aos dados pessoais, dentro do seguinte subconjunto: nome próprio e/ou apelido, iniciais, contactos profissionais, pertença a um grupo, rede ou número de identificação de utilizador, credenciais de início de sessão, histórico profissional e competências, género ou título, participação em eventos por parte de colaboradores e trabalhadores suplementares da GSK que utilizem os Serviços.

Informação Pessoal da GSK refere-se à Informação Pessoal: (i) facultada pela GSK ou em nome da mesma ao Fornecedor (incluindo quando este tem acesso à Informação Pessoal conservada pela GSK ou em nome da mesma) ou que este recolhe ou produz em nome desta; (ii) que são tratados pelo Fornecedor ao abrigo de ou em relação a este Contrato; e (iii) cuja responsabilidade pelo tratamento ou titularidade (ou equivalente) recaia sobre a GSK.

Programa de Segurança refere-se *ao programa de cibersegurança apenso ao presente documento como Anexo 1.*

Os termos **responsável pelo tratamento, avaliação do impacto sobre a proteção de dados, titular dos dados, dados pessoais, violação de dados pessoais, subcontratante, tratamento, prestador de serviços** e **autoridade de controlo** devem ser definidos de acordo com as Leis de Proteção de Dados relevantes. Qualquer referência à GSK deve ser entendida como a entidade contratante da GSK utilizada no Contrato, bem como as Filiais Abrangidas.

Termos do Subcontratante

No caso de o fornecedor estar a agir como subcontratante da Informação Pessoal da GSK, ao abrigo das Leis de Proteção de Dados relevantes, aplicam-se os seguintes termos:

1. Cada parte deve cumprir as suas obrigações previstas na Legislação aplicável sobre Proteção de Dados. A GSK e o Fornecedor acordam que, em relação à Informação Pessoal daquela tratada ao abrigo deste Contrato, a GSK será a responsável pelo tratamento e o Fornecedor será o subcontratante. Para efeitos da CCPA, o Fornecedor é um prestador de serviços da GSK e o tratamento da Informação Pessoal da mesma por parte daquele deve ser realizado apenas para os fins desta empresa, de acordo com este Anexo, que não está a ser fornecido contra qualquer contrapartida, monetária ou outra, pelo Fornecedor à GSK e, por conseguinte, esta não está a vender àquele a sua Informação Pessoal, conforme definido pela CCPA.

2. O Fornecedor deve cumprir o seguinte relativamente à Informação Pessoal da GSK:

a) tratar a Informação Pessoal da GSK apenas de acordo com as instruções escritas legais desta empresa e apenas para efeitos de prestação de Serviços pelo mesmo a esta entidade, ao abrigo do presente Contrato, durante a vigência ou qualquer período adicional indicado no mesmo, se aplicável;

b) nem o Fornecedor nem qualquer dos seus funcionários, agentes, consultores ou cessionários terão qualquer direito de tratar a Informação Pessoal da GSK para o seu próprio benefício comercial, sob qualquer forma;

c) implementar medidas técnicas e organizativas no domínio da segurança adequadas, incluindo, sem limitação, as medidas estabelecidas no Anexo relacionado com a Segurança. As referências no Anexo relacionado com a Segurança a "Dados da GSK" devem incluir Informação Pessoal da GSK;

d) manter a confidencialidade da Informação Pessoal da GSK, de acordo com os termos e referências neste Anexo, devendo o Anexo relacionado com a Segurança da Informação Confidencial da GSK incluir a Informação Pessoal desta empresa;

e) impor obrigações de confidencialidade, equivalentes às obrigações estabelecidas no Contrato, ao pessoal relevante com acesso à Informação Pessoal da GSK;

f) não contratar outro subcontratante ("**subcontratante ulterior**") sem a aprovação prévia por escrito da GSK (e, para estes efeitos, a GSK consente as seguintes categorias de subcontratante ulterior: prestadores de serviços de infraestrutura de alojamento, a utilização de contratantes individuais e subcontratantes ulteriores informados à GSK, na altura em que o Contrato é celebrado) e transferir a Informação Pessoal da GSK para os subcontratantes ulteriores aprovados apenas ao abrigo de um contrato escrito, que imponha obrigações consistentes com as estabelecidas neste Anexo. Quando o Fornecedor nomear um subcontratante ulterior em conformidade com o disposto nesta cláusula 2(f), permanece responsável pelos atos e omissões do mesmo;

g) prestar à GSK apoio razoável com (i) a realização de quaisquer avaliações de impacto sobre a proteção de dados, legalmente exigidas e/ou avaliações de impacto sobre a transferência de dados; (ii) o cumprimento dos direitos dos titulares dos dados; e (iii) a resposta a pedidos de qualquer autoridade de controlo, relativamente à Informação Pessoal da GSK;

h) notificar a GSK sem demora depois de tomar conhecimento de uma violação de dados pessoais, relativamente a qualquer Informação Pessoal da GSK e prestar apoio à mesma, relativamente a tal violação;

i) notificar a GSK sem demora se receber um pedido por escrito de (i) um titular de dados para exercer qualquer um dos seus direitos, em relação à Informação Pessoal da GSK, ao abrigo da Legislação sobre Proteção de Dados; ou (ii) uma autoridade de controlo, em relação ao tratamento da Informação Pessoal da GSK;

j) salvo disposição em contrário no Contrato, devolver ou destruir toda a Informação Pessoal da GSK na sua posse ou sob o seu controlo (incluindo a tratada por subcontratantes ulteriores autorizados) aquando da rescisão ou caducidade do Contrato; e

k) mediante pedido escrito da GSK, fornecer à mesma as informações razoáveis necessárias para demonstrar o cumprimento do preceituado neste Anexo, o que pode incluir relatórios de auditoria de segurança de terceiros disponíveis.

Termos para o Responsável pelo Tratamento de Dados:

No caso de o fornecedor estar a agir como responsável pelo tratamento da Informação Pessoal da GSK, ao abrigo das Leis de Proteção de Dados relevantes, aplicam-se os seguintes termos:

1. Cada parte deve cumprir as suas obrigações, como responsável independente pelo tratamento, previstas na Legislação aplicável sobre Proteção de Dados. Para efeitos da CCPA, a GSK e o Fornecedor acordam, em relação aos dados pessoais tratados ao abrigo deste Anexo, que não existe contra qualquer contrapartida, monetária ou outra, a ser realizada pelo Fornecedor à GSK em troca da Informação Pessoal da GSK e, por conseguinte, esta não está a vender àquele a sua Informação Pessoal, conforme definido pela CCPA.

2. Se o Fornecedor receber uma comunicação de uma autoridade de controlo relacionada direta ou indiretamente com: a) o tratamento de Informação Pessoal da GSK por parte do Fornecedor; ou (b) um potencial incumprimento das Leis de Proteção de Dados, em relação ao tratamento de Informação Pessoal da GSK, o Fornecedor deverá, na medida do permitido pelas leis aplicáveis, encaminhar prontamente a comunicação à GSK e oferecer-lhe cooperação e apoio razoáveis, em relação ao mesmo.

3. Se um titular de dados apresentar um pedido escrito a qualquer uma das partes para exercer qualquer um dos seus direitos, ao abrigo das Leis de Proteção de Dados, relativamente à Informação Pessoal da GSK, a parte recetora responderá a esse pedido, de acordo com as Leis de Proteção de Dados. Na medida em que o pedido diga respeito ao tratamento da Informação Pessoal da GSK realizado pela outra parte, a parte recetora deve: (i) prontamente e sem demora injustificada encaminhar o pedido para a outra parte; e (ii) cooperar e prestar apoio razoável, em relação a esse pedido, para permitir que a outra parte responda de acordo com as Leis de Proteção de Dados.

4. Sem limitar qualquer disposição do Anexo relacionado com a Segurança, ao tomar conhecimento de uma violação de dados pessoais, que afete a Informação Pessoal da GSK, o Fornecedor deve: (a) notificá-la imediatamente e fornecer-lhe uma descrição razoável da violação; e (b) não publicar qualquer comunicação relativa à violação, sem antes consultar a GSK, com a ressalva de que pode notificar uma violação a uma autoridade de controlo, na medida exigida pela Lei de Proteção de Dados aplicável.

Transferências internacionais de dados

Nos casos em que a GSK, na qualidade de exportadora de dados, transfira a sua Informação Pessoal para o Fornecedor, na qualidade de importador de dados, de uma forma que constitua uma transferência internacional de dados restrita, ao abrigo das Leis de Proteção de Dados aplicáveis, ambas as partes celebraram e irão cumprir as Cláusulas-Tipo aplicáveis, que abrangem a relação entre as partes:

- O Anexo à Decisão de Implementação da Comissão relativa a cláusulas contratuais-tipo para a transferência de dados pessoais para países terceiros, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ("**Anexo**") juntamente com o MÓDULO UM: transferência entre responsáveis pelo tratamento (disponível **aqui**) e incorporado aqui por referência tal como atualizado, alterado, substituído ou suplantado ocasionalmente pela Comissão Europeia; e/ou (ii) qualquer acordo ou adenda correspondente ou equivalente a uma cláusula-tipo de transferência de dados internacional às Cláusulas-Tipo adotadas pela autoridade de controlo no Reino Unido ("**Cláusulas-Tipo C2C**");
- O Anexo juntamente com o MÓDULO DOIS: transferência de responsável pelo tratamento para subcontratante (disponível **aqui**) e incorporado aqui por referência tal como atualizado, alterado, substituído ou suplantado ocasionalmente pela Comissão Europeia; e/ou (ii) qualquer contrato ou adenda correspondente ou equivalente a uma cláusula-tipo de transferência internacional de dados às Cláusulas-Tipo adotadas pela autoridade de controlo no Reino Unido ("**Cláusulas-Tipo C2P**");

"**Cláusulas-Tipo**" referem-se ao Anexo juntamente com as Cláusulas-Tipo C2C e Cláusulas-Tipo C2P.

Para efeitos das Cláusulas-Tipo, as partes acordam que:

- A opção entre parênteses retos da Cláusula 11 "Recurso" não é aplicável
- A opção um é selecionada para a Cláusula 17 "Direito Aplicável" e aplica-se o direito da Irlanda.
- Os tribunais da Irlanda terão jurisdição nos termos da Cláusula 18 "Eleição do Foro e Jurisdição".

Para efeitos das Cláusulas-Tipo C2P e Cláusulas-Tipo C2C aplicáveis, tenha, por favor, em consideração o seguinte:

- Annex1 (Exportador e Importador): a GSK ou os destinatários relevantes dos seus serviços localizados na UE e/ou no Reino Unido, ao abrigo do(s) acordo(s) com o Fornecedor, são o Exportador de Dados, em relação à Informação Pessoal da GSK. O Fornecedor é o Importador de Dados, em relação à Informação Pessoal da GSK
- Anexo 1 (Descrição das Transferências): consulte, por favor, a definição de Informação Pessoal e Serviços a prestar pelo Importador. Não são transferidos dados sensíveis. A frequência da transferência é contínua. A natureza das atividades de tratamento e as finalidades da transferência estão definidos no(s) contrato(s) celebrado(s) com o Fornecedor. Os dados serão conservados em conformidade com as políticas de conservação de dados do Exportador de Dados.
- Anexo 1 (Autoridades Competentes): conforme estabelecido na cláusula 13 das Cláusulas-Tipo C2C e Cláusulas-Tipo C2P
- Anexo 2 (Medidas Técnicas e de Organização): consulte, por favor, as Medidas de Segurança estabelecidas abaixo

As partes acordam que a opção 2 da cláusula 9 "Recurso a subcontratantes ulteriores" das Cláusulas-Tipo C-P é aplicável, quando o Fornecedor contrata um subcontratante ulterior, aceitando estes, por sua vez, cumprir as **Cláusulas-Tipo P-P**, o que significa i) o Anexo, juntamente com o MÓDULO TRÊS: transferência entre subcontratantes (disponível **aqui**) e incorporado aqui por referência tal como atualizado, alterado, substituído ou suplantado ocasionalmente pela Comissão Europeia; e/ou (ii) qualquer contrato ou adenda correspondente ou equivalente a uma cláusula-tipo de transferência internacional de dados às Cláusulas-Tipo adotadas pela autoridade de controlo no Reino Unido;

Caso o Fornecedor não acredite que possa satisfazer as exigências razoavelmente estabelecidas pela GSK, deverá notificá-la imediatamente acerca da sua incapacidade, tendo esta o direito de rescindir o Contrato.

As Partes acordam que as Cláusulas-Tipo celebradas produzirão efeitos em países fora do Espaço Económico Europeu, onde: (i) as suas disposições são reconhecidas como uma garantia adequada, em relação a transferências internacionais de Dados Pessoais para países não adequados; ou (ii) as Leis de Proteção de Dados exigem a existência de disposições contratuais para proteger as transferências internacionais de Informação Pessoal. Na interpretação das Cláusulas-Tipo, nesses países, qualquer referência ao termo "Estado-Membro no qual o exportador de dados está estabelecido" será interpretada como significando o país no qual a entidade da GSK está estabelecida; e qualquer referência ao Regulamento (UE) 2016/679 será interpretada como referência à lei do país onde a GSK está estabelecida fora do EEE. Qualquer referência a um "País Adequado" refere-se a qualquer país que seja considerado como proporcionando ou que de outra forma proporciona um nível equivalente de proteção, para efeitos das Leis de Proteção de Dados aplicáveis, nos países fora do Espaço Económico Europeu onde as Cláusulas-Tipo abrangem as transferências de Dados Pessoais.

Medidas de segurança

"**Dados da GSK**" referem-se a quaisquer dados ou informações que sejam fornecidos por ou em nome da GSK ou obtidos pelo Fornecedor ou pelo seu Pessoal, no âmbito da negociação e execução do Contrato ou do cumprimento das obrigações deste último, ao abrigo do Contrato, incluindo quaisquer dados e informações que: (i) sejam criados, gerados, recolhidos ou processados pelo Pessoal do Fornecedor, no cumprimento das obrigações deste previstas no Contrato; ou (ii) residam ou sejam acedidos através dos sistemas de informação da GSK ou sistemas de informação do Fornecedor, bem como quaisquer dados e informações derivados do atrás referido.

"**Tratamento de Dados Pessoais**" refere-se à operação ou conjunto de operações realizadas sobre qualquer informação ou dados, por meios automatizados ou não, como, por exemplo, recolha, registo, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou disponibilização, alinhamento ou combinação, limitação, apagamento ou destruição.

"**Ambiente do Fornecedor**" refere-se à combinação de *hardware*, *software*, sistemas operativos, sistemas de bases de dados, ferramentas e componentes de rede utilizados por ou em nome do Fornecedor, para receber, manter, Tratar, armazenar, aceder ou transmitir Dados da GSK.

"**Pessoal do Fornecedor**" refere-se a todo e qualquer pessoal empregado ou contratado pelo Fornecedor e pelos seus Subcontratantes, para executar qualquer parte dos Serviços.

Este Anexo relacionado com a Segurança faz parte do Contrato celebrado por e entre a GSK e o Fornecedor. Em caso de conflito, no que diz respeito à cibersegurança, entre os termos deste Anexo relacionado com a Segurança e os termos do Contrato, prevalecerão os primeiros. Os termos iniciados por maiúscula não definidos neste Anexo relacionado com a Segurança têm o significado que lhes é atribuído noutros locais no Contrato.

1. Responsabilidades. O Fornecedor deve: (a) utilizar controlos robustos de cifragem para proteger os Dados da GSK contra a divulgação, alteração ou acesso não autorizados, em trânsito ou fora do seu ambiente em redes de terceiros; (b) manter os procedimentos de controlo alinhados com as boas práticas do setor, para a deteção, prevenção e recuperação de programas maliciosos, vírus e programas espiões, incluindo a atualização de antivírus e combate aos programas maliciosos e espiões, em intervalos regulares; e (c) manter o acesso às políticas de gestão, procedimentos e mecanismos de controlo técnico alinhados com as boas práticas do setor, para garantir que o acesso total aos Dados da GSK sob o seu controlo é devidamente autorizado.

2. Violação de Segurança. O Fornecedor deve comunicar à GSK por *e-mail* para cstd@gsk.com qualquer utilização acidental, não autorizada ou ilegal, perda, destruição, divulgação, acesso, corrupção, modificação, venda, aluguer ou outro Tratamento de quaisquer Dados da GSK (uma "**Violação de Segurança**"), no prazo de vinte e quatro (24) horas após a verificação do Fornecedor. Deve ainda garantir que todos os incidentes relacionados com a segurança, que envolvam os Dados da GSK, são geridos em conformidade com os procedimentos adequados de resposta a incidentes e colaborar de boa-fé com a GSK, para identificar a origem do problema e remediar a Violação de Segurança.

ПРИЛОЖЕНИЕ

УСЛОВИЯ ЗАЩИТЫ ДАННЫХ. ОСНОВНАЯ ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ

«**Аффилированная компания, на которую распространяется действие Соглашения**» означает каждое из аффилированных лиц GSK, которое получает преимущества от Услуг в качестве третьей стороны (список которых будет предоставлен компанией GSK Поставщику по запросу). Аффилированное лицо — это любое юридическое лицо, которое (в отношении любого другого юридического лица) Контролируется, находится под общим Контролем или Контролирует такое другое юридическое лицо. «Контроль» и его производные означают либо право собственности (будь то прямо или косвенно) на большинство голосующих акций такого юридического лица, либо способность (будь то прямо или косвенно) назначать большинство директоров такого юридического лица, либо полномочия руководить управлением или политиками такого юридического лица по договору или иным образом.

«**Законодательство о защите данных**» означает: (а) Общий регламент по защите данных (ЕС) 2016/679 о защите физических лиц в отношении обработки персональных данных и свободного перемещения таких данных, а также любые применимые законы и (или) нормативные акты, которые реализуют и (или) осуществляют отступления в соответствии с ним и (или) заменяют его «**GDPR**»); (б) Общий регламент по защите данных, приведенный в соответствии с Законом Великобритании о защите данных от 2018 г.; (в) Закон Калифорнии о защите персональных данных потребителей от 2018 г. (Гражданский кодекс Калифорнии §1798. 117 - §98.199 («**CCPA**»); и (г) все другие законы, касающиеся обработки персональных данных.

«**Персональная информация**» означает персональную информацию в составе следующего подмножества: имя и (или) фамилия, инициалы, рабочие контактные данные, членство в группах, сетевой или идентификационный номер пользователя, данные для входа в учетную запись, опыт работы, навыки, пол и должность, посещение мероприятий сотрудниками GSK и дополнительными работниками, использующими Услуги.

«**Персональная информация GSK**» означает любую Персональную информацию: (i) которая предоставляется компанией GSK или от ее имени Поставщику (включая случаи, когда Поставщик имеет доступ к Персональной информации, хранящейся у компании GSK или от ее имени) либо собирается или генерируется Поставщиком от имени компании GSK; (ii) которая обрабатывается Поставщиком в соответствии или в связи с настоящим Соглашением; (iii) в отношении которой компания GSK является контролером или владельцем (или эквивалентом);

«Приложение об обеспечении безопасности» означает *приложение об обеспечении кибербезопасности, прилагаемое к настоящему документу в качестве Приложения № 1*.

Термины **«контролер», «оценка воздействия на защиту данных», «субъект данных», «персональные данные», «утечка персональных данных», «оператор», «обработка», «поставщик услуг»** и **«контролирующий орган»** должны соответствовать определению, данному в Применимом законодательстве о защите данных. Любая ссылка на компанию GSK означает контрактную организацию GSK, используемую в Соглашении, а также Аффилированные компании, на которые распространяется действие Соглашения.

Условия для оператора

В том случае, если Поставщик выступает в качестве оператора Персональной информации GSK в соответствии с Применимым законодательством о защите данных, применяются следующие условия:

1. Каждая из сторон обязуется соблюдать свои обязательства в соответствии с Применимым законодательством о защите данных. GSK и Поставщик соглашаются, что в отношении Персональной информации GSK, обрабатываемой в соответствии с настоящим Соглашением, GSK будет контролером, а Поставщик будет оператором. Для целей CCPA Поставщик является поставщиком услуг для GSK, и обработка Персональной информации GSK Поставщиком должна осуществляться только для целей GSK в соответствии с настоящим Приложением; Поставщик не предоставляет GSK никакого денежного или иного ценного вознаграждения, и, следовательно, GSK не продает Персональную информацию GSK Поставщику, как это определено в CCPA.

2. Поставщик обязуется соблюдать следующие требования в отношении Персональной информации GSK:

a) обрабатывать Персональную информацию GSK только в соответствии с законными письменными инструкциями GSK и исключительно в целях предоставления Услуг Поставщиком компании GSK в соответствии с настоящим Соглашением в течение срока действия Соглашения или любого дополнительного периода, указанного в Соглашении, если применимо;

b) ни Поставщик, ни его сотрудники, агенты, консультанты или цессионарии не имеют права обрабатывать Персональную информацию GSK в коммерческих целях в любой форме;

c) внедрить и поддерживать соответствующие технические и организационные меры обеспечения безопасности, включая, помимо прочего, меры, изложенные в Приложении об обеспечении безопасности. Ссылки на «Данные GSK» в Приложении об обеспечении безопасности включают Персональную информацию GSK;

d) обеспечивать конфиденциальность Персональной информации GSK в соответствии с условиями настоящего Приложения, при этом ссылки на Конфиденциальную информацию GSK, содержащиеся в настоящем Приложении и Приложении об обеспечении безопасности, должны включать Персональную информацию GSK;

e) налагать обязательства по соблюдению конфиденциальности, эквивалентные обязательствам, изложенным в Соглашении, на соответствующих сотрудников, имеющих доступ к Персональной информации GSK;

f) не привлекать другого оператора («**субподрядчика по обработке данных**») без предварительного письменного разрешения GSK (и для этих целей GSK соглашается на следующие категории субподрядчиков по обработке данных: поставщики услуг хостинга инфраструктуры, при этом использование индивидуальных подрядчиков и субподрядчиков по обработке данных должно доводиться до сведения компании GSK на момент заключения Соглашения), и передавать Персональную информацию компании GSK таким утвержденным субподрядчикам по обработке данных только по письменному договору, который налагает на них обязательства, согласующиеся с обязательствами, изложенными в настоящем Приложении. Когда Поставщик назначает субподрядчика по обработке данных в соответствии с настоящим пунктом 2(f), он несет ответственность за действия и бездействие субподрядчика по обработке данных;

g) оказывать GSK разумную помощь в отношении: (i) проведения любых предусмотренных законом оценок воздействия на защиту данных и (или) оценки влияния на передачу данных; (ii) соблюдения прав субъектов данных; (iii) ответа на запросы от любого надзорного органа в отношении Персональной информации GSK;

h) незамедлительно уведомлять компанию GSK после того, как ему станет известно об утечке персональных данных в отношении какой-либо Персональной информации GSK, и оказывать GSK помощь в отношении такой утечки;

i) незамедлительно уведомлять компанию GSK, если он получает письменный запрос от: (i) субъекта данных, осуществляющего свои права в отношении Персональной информации GSK в соответствии с Законодательством о защите данных; (ii) надзорного органа в отношении обработки Персональной информации GSK;

j) если иное не указано в Соглашении, вернуть или уничтожить всю Персональную информацию GSK, находящуюся в его распоряжении или под его контролем (включая любую Персональную информацию GSK, обрабатываемую разрешенными субподрядчиками по обработке данных) в случае расторжения или истечения срока действия Соглашения;

k) по письменному запросу GSK предоставлять GSK разумную информацию, необходимую для подтверждения соблюдения настоящего Приложения, что может включать любые доступные отчеты по аудиту безопасности третьих сторон.

Условия для контролера

В случае если поставщик действует в качестве контролера Персональной информации GSK в соответствии с Применимым законодательством о защите данных, применяются следующие условия:

1. Каждая сторона выступает в качестве независимого контролера и обязуется выполнять свои обязательства в соответствии с Применимым законодательством о защите данных. GSK и Поставщик соглашаются с тем, что в отношении персональных данных, обрабатываемых в соответствии с настоящим Приложением, в целях CCPA Поставщик не предоставляет GSK никакого денежного или иного ценного вознаграждения в обмен на Персональную информацию GSK, и, следовательно, GSK не продает Персональную информацию GSK Поставщику, как это определено CCPA.

2. Если Поставщик получает какое-либо сообщение от надзорного органа, которое прямо или косвенно связано с: а) обработкой Поставщиком Персональных данных GSK; (б) потенциальным несоблюдением Законодательства о защите данных в отношении обработки Персональных данных GSK, Поставщик обязуется (если это разрешено Применимым законодательством) незамедлительно перенаправить такое сообщение GSK и обеспечить разумное сотрудничество и помощь GSK в этой связи.

3. Если субъект данных подает письменный запрос любой из сторон на осуществление своих прав в соответствии с Законодательством о защите данных в отношении Персональной информации GSK, получающая сторона должна ответить на этот запрос в соответствии с Законодательством о защите данных. Если запрос касается обработки Персональной информации GSK, полученной другой стороной, получающая сторона должна: (i) незамедлительно и без неоправданной задержки переслать запрос другой стороне; (ii) сотрудничать и оказывать разумную помощь в отношении этого запроса таким образом, чтобы другая сторона могла ответить на него в соответствии с Законодательством о защите данных.

4. Не ограничивая какое-либо положение Приложения об обеспечении безопасности, после того, как станет известно об утечке персональных данных, влияющей на Персональную информацию GSK, Поставщик обязуется: (а) незамедлительно уведомить GSK и предоставить GSK описание нарушения в разумных пределах; (б) не публиковать сообщение об утечке без предварительной консультации с GSK, за исключением того, что он может уведомить об утечке надзорный орган в объеме, предусмотренном применимым Законодательством о защите данных.

Международная передача данных

В тех случаях, когда GSK, выступающая в качестве экспортера данных, передает Персональную информацию GSK Поставщику, действующему в качестве импортера данных, таким образом, который представляет собой ограниченную международную передачу данных в соответствии с Применимым законодательством о защите данных, обе стороны настоящим заключили и будут соблюдать применимые Типовые положения, охватывающие отношения между сторонами:

- Приложение к Исполнительному решению Комиссии о стандартных договорных положениях относительно передачи персональных данных третьим странам в соответствии с Регламентом (ЕС) 2016/679 Европейского парламента и Совета («**Приложение**») вместе с МОДУЛЕМ ПЕРВЫМ: передача данных от контролера контролеру (доступно **здесь**), которые включены в настоящий документ посредством ссылки, с учетом обновлений, изменений или замены каким бы то ни было образом, производимых в определенные периоды времени Европейской комиссией; (ii) любым соответствующим или эквивалентным международным соглашением о передаче данных либо приложением к Типовым положениям, принятым надзорным органом Великобритании («**Типовые положения передачи данных от контролера контролеру**»).

- Приложение вместе с МОДУЛЕМ ВТОРЫМ: передача данных от контролера оператору (доступно **здесь**), которые включены в настоящий документ посредством ссылки, с учетом обновлений, изменений или замены каким бы то ни было образом, производимых в определенные периоды времени Европейской комиссией; и (или) (ii) любым соответствующим или эквивалентным международным соглашением о передаче данных либо приложением к Типовым положениям, принятым надзорным органом Великобритании («**Типовые положения передачи данных от контролера оператору**»).

«**Типовые положения**» означает Приложение вместе с Типовыми положениями передачи данных от контролера контролеру и Типовыми положениями передачи данных от контролера оператору.

Стороны соглашаются, что для целей Типовых приложений:

- вариант, приведенный в квадратных скобках пункта 11 «Восстановление в правах», не применяется;
- для пункта 17 «Регулирующее законодательство» выбран вариант 1, при этом применяется законодательство Ирландии;
- суды Ирландии будут иметь юрисдикцию в соответствии с пунктом 18 «Выбор места рассмотрения споров и юрисдикции».

Для целей применимых Типовых положений передачи данных от контролера контролеру и Типовых положений передачи данных от контролера оператору обратите внимание на следующее:

- Приложение № 1 (Экспортер и Импортер): GSK или соответствующие получатели услуг GSK, расположенные в ЕС и (или) Великобритании в соответствии с соглашением(-ями) с Поставщиком, являются Экспортером данных в отношении Персональной информации GSK. Поставщик является Импортером данных в отношении Персональной информации GSK.
- Приложение № 1 (Описание передачи): см. определение Персональной информации и Услуг, предоставляемых Импортером. Никакие конфиденциальные данные не передаются. Частота передачи – непрерывный режим. Характер деятельности по обработке данных и цели передачи указаны в соглашении(-ях) с Поставщиком. Данные будут храниться в соответствии с политиками хранения данных Экспортера данных.
- Приложение № 1 (Компетентные органы): как указано в пункте 13 Типовых положений передачи данных от контролера контролеру и Типовых положений передачи данных от контролера оператору.
- Приложение № 2 (Технические и организационные меры): см. раздел «Меры обеспечения безопасности», приведенный ниже.

Стороны соглашаются с тем, что вариант 2 пункта 9 «Использование субподрядчиков по обработке данных» Типовых положений передачи данных от контролера оператору применяется в тех случаях, когда Поставщик привлекает субподрядчика по обработке данных, и Поставщик и субподрядчик по обработке данных соглашаются соблюдать **Типовые положения передачи данных от оператора оператору**, что означает использование: i) Приложения вместе с МОДУЛЕМ ТРЕТЬИМ: передача от оператора данных оператору данных (доступно **здесь**), которые включены в настоящий документ посредством ссылки, с учетом обновлений, изменений или замены каким бы то ни было образом, производимых в определенные периоды времени Европейской комиссией; (ii) любым соответствующим или эквивалентным международным соглашением о передаче данных либо приложением к Типовым положением, принятым надзорным органом Великобритании.

В случае если Поставщик считает, что он не может выполнить требования, установленные GSK, Поставщик обязуется немедленно уведомить GSK о своей неспособности, и GSK имеет право расторгнуть Соглашение.

Стороны соглашаются с тем, что принятые Типовые положения имеют силу в странах за пределами Европейской экономической зоны, где: (i) они признаются в качестве надлежащего средства защиты в отношении международной передачи Персональных данных в страны, не обеспечивающих должный уровень защиты; (ii) Законодательство о защите данных требует наличия договорных положений для защиты Персональных данных при международной передаче. При толковании Типовых положений в этих странах любая ссылка на термин «Страна-участник, в которой учрежден экспортер данных» будет истолковываться как ссылка на страну, в которой учреждена организация GSK, а любая ссылка на Регламент (ЕС) 2016/679 будет истолковываться как ссылка на законодательство страны, в которой учреждена организация GSK за пределами ЕЭЗ. Любая ссылка на «Страну, обеспечивающую должный уровень защиты» означает любую страну, которая, как считается, предоставляет или иным образом обеспечивает эквивалентный уровень защиты в целях применимого Законодательства о защите данных, в тех странах, которые находятся за пределами Европейской экономической зоны, где передача Персональных данных обеспечивается Типовыми положениями.

Меры обеспечения безопасности

«Данные GSK» означает любые данные или информацию, предоставленные компанией GSK или от ее имени или полученные Поставщиком или Персоналом Поставщика в связи с обсуждением условий и подписанием Соглашения или выполнением обязательств Поставщика по Соглашению, включая любые такие данные и информацию, которые: (i) создается, генерируются, собираются или обрабатываются Персоналом Поставщика при выполнении обязательств Поставщика по Соглашению; (ii) находятся или доступны в информационных системах GSK или информационных системах Поставщика, а также любые данные и информацию, полученные на основании вышеизложенного.

«**Обработка**» означает любую операцию или набор операций, которые выполняются с любой информацией или данными, например, сбор, запись, организация, в структурировании, хранении, адаптация или изменения, извлечение, консультация, использование, раскрытие путем передачи, распространение или предоставление иным образом, согласование или объединение, ограничение, удаление или уничтожение, независимо от того, осуществляются ли они автоматически или нет.

«Среда Поставщика» означает комбинацию аппаратного обеспечения, программного обеспечения, операционных систем, систем баз данных, инструментов и сетевых компонентов, используемых Поставщиком или от его имени для получения, обслуживания, обработки, хранения, доступа или передачи Данных GSK.

«Персонал Поставщика» означает любой и весь персонал, привлеченный или нанятый Поставщиком и его Субподрядчиками для выполнения какой-либо части Услуг.

Настоящее Приложение об обеспечении безопасности является частью Соглашения между GSK и Поставщиком. В случае любого противоречия в отношении кибербезопасности между условиями настоящего Приложения об обеспечении безопасности и условиями Соглашения, данное Приложение об обеспечении безопасности имеет преимущественную силу. Термины с заглавной буквы, не определенные в настоящем Приложении об обеспечении безопасности, имеют значения, присвоенные им в других частях Соглашения.

1. Ответственность. Поставщик будет: (а) использовать действенные средства шифрования для защиты всех Данных GSK от несанкционированного раскрытия, доступа или изменения при передаче в Среду Поставщика или из нее через сторонние сети; (б) поддерживать процедуры контроля в соответствии с передовыми отраслевыми практиками с целью обнаружения, предотвращения и восстановления от вредоносного ПО, вирусов и шпионских программ, включая обновление антивирусного программного обеспечения и программного обеспечения для защиты от вредоносных и шпионских программ через регулярные промежутки времени; (в) поддерживать политики управления доступом, процедуры, и технические средства контроля в соответствии с передовыми отраслевыми практиками с целью обеспечения надлежащего доступа ко всем Данным GSK, которые находятся в его распоряжении.

2. Нарушение безопасности. Поставщик обязуется сообщать компании GSK (по адресу электронной почты cstd@gsk.com) о любом подтвержденном случайном, несанкционированном или незаконном использовании, потере, уничтожении, раскрытии, доступе, искажении, модификации, продаже, аренде или другой обработке любых Данных GSK («**Нарушение безопасности**») в течение 24 (двадцати четырех) часов после подтверждения Поставщика. Поставщик обеспечит управление всеми инцидентами, связанными с Данными GSK, согласно соответствующим процедурам реагирования на инциденты и будет добросовестно работать с GSK для выявления первопричины и устранения Нарушения безопасности.

ANEXO

CONDICIONES DE PROTECCIÓN DE DATOS: INFORMACIÓN PERSONAL BÁSICA

Filial cubierta se refiere a cada Filial de GSK que tenga el beneficio de los Servicios como tercero (cuya lista GSK proporcionará al Proveedor previa solicitud). Una Filial es cualquier entidad que, con respecto a cualquier otra entidad, esté controlada por, bajo el control común, o que controle dicha otra entidad. "Control" y sus derivados se refieren a la titularidad (directa o indirectamente) de una mayoría de las acciones con derecho a voto de dicha entidad o la capacidad (directa o indirectamente) de nombrar a la mayoría de los consejeros de dicha entidad o la autoridad para dirigir la gestión o las políticas de dicha entidad, mediante contrato o de otro modo.

Legislación sobre protección de datos se refiere a: (a) el Reglamento General de Protección de Datos (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y cualesquiera leyes o reglamentos aplicables que implementen o ejecuten derogaciones en virtud del mismo o que lo sustituyan o reemplacen (**RGPD**); (b) el RGPD adaptado por la Ley de Protección de Datos del Reino Unido de 2018; (c) la Ley de Privacidad del Consumidor de California de 2018 (Código Civ. de California 1798.100 - 1798.199) (California Consumer Privacy Act, **CCPA**); y (d) todas las demás leyes relativas al tratamiento de datos personales.

Información personal se refiere a los siguientes datos personales: nombre o apellido(s), iniciales, datos de contacto laborales, pertenencia a grupos, número de identificación de red o usuario, credenciales de inicio de sesión, historial laboral y habilidades, género o cargo, asistencia a eventos de los empleados de GSK y trabajadores suplementarios que utilizan los Servicios.

Información personal de GSK se refiere a cualquier Información personal: (i) que sea suministrada por o en nombre de GSK al Proveedor (incluido cuando el Proveedor tenga acceso a la Información personal en poder de GSK o en su nombre), o que el Proveedor recoja o genere en nombre de GSK; (ii) que sea tratada por el Proveedor en virtud de o en relación con el Contrato; y (iii) con respecto a la cual GSK sea un responsable del tratamiento o titular (o equivalente).

Programa de seguridad se refiere *al programa de ciberseguridad adjunto al presente como Apéndice 1*.

Los términos **responsable del tratamiento, evaluación de impacto relativa a la protección de datos, interesado, datos personales, violación de la seguridad de los datos personales, encargado del tratamiento, tratamiento, proveedor de servicios y autoridad de control** se definirán con arreglo a la Legislación sobre protección de datos pertinente. Cualquier referencia a GSK se referirá a la entidad contratante de GSK utilizada en el Contrato, así como a las Filiales cubiertas.

Condiciones del encargado del tratamiento

En caso de que el proveedor actúe como encargado del tratamiento de la Información personal de GSK en virtud de la Legislación sobre protección de datos pertinente, se aplicarán los siguientes términos:

1. Cada parte cumplirá con sus obligaciones en virtud de la Legislación sobre protección de datos aplicable. GSK y el Proveedor acuerdan que, en relación con la Información personal de GSK tratada en virtud del presente Contrato, GSK será el responsable del tratamiento y el Proveedor será el encargado del tratamiento. A efectos de la CCPA, el Proveedor es un proveedor de servicios de GSK y el tratamiento de la Información personal de GSK por parte del Proveedor se llevará a cabo únicamente para los fines de GSK de conformidad con este Anexo; el Proveedor no proporciona a GSK ninguna contraprestación monetaria ni de valor y, por lo tanto, GSK no vende Información personal de GSK al Proveedor según se define en la CCPA.

2. El Proveedor deberá cumplir con lo siguiente con respecto a la Información personal de GSK:

a) Tratará la Información personal de GSK únicamente según las instrucciones legales escritas de GSK y únicamente para los fines de prestación de los Servicios por parte del Proveedor a GSK en virtud del presente Contrato durante la vigencia del Contrato o cualquier periodo adicional establecido en el mismo, si procede.

b) Ni el Proveedor, ni ninguno de sus empleados, agentes, consultores o cesionarios tendrán derecho a tratar la Información personal de GSK para su propio beneficio comercial de ninguna forma.

c) Implementará y mantendrá las medidas de seguridad técnicas y organizativas adecuadas, incluidas, entre otras, las medidas establecidas en el Programa de seguridad. Las referencias en el Programa de seguridad a "Datos de GSK" incluirán la Información personal de GSK.

d) Mantendrá de forma confidencial la Información personal de GSK de acuerdo con las condiciones de este Anexo y las referencias en este Anexo y el Programa de seguridad a la Información confidencial de GSK incluirán la Información personal de GSK.

e) Impondrá obligaciones de confidencialidad equivalentes a las obligaciones establecidas en el Contrato al personal pertinente que tenga acceso a la Información personal de GSK.

f) No contratará a otro encargado ("**subencargado del tratamiento**") sin la aprobación previa por escrito de GSK (y para estos fines, GSK consiente las siguientes categorías de subencargado: proveedores de servicios de infraestructura de alojamiento, el uso de contratistas individuales y subencargados del tratamiento informados a GSK en el momento en que se celebra el Contrato) y transferirá la Información personal de GSK a dichos subencargados del tratamiento aprobados únicamente en virtud de un contrato escrito que imponga obligaciones consistentes con las establecidas en este Anexo. Cuando el Proveedor nombre a un subencargado del tratamiento de acuerdo con esta cláusula 2(f), seguirá siendo responsable de los actos y omisiones del subencargado del tratamiento.

g) Proporcionará a GSK asistencia razonable (i) al llevar a cabo las evaluaciones de impacto de la protección de datos legalmente requeridas o las evaluaciones de impacto de la transferencia de datos; (ii) al cumplir con los derechos de los interesados; y (iii) al responder a las solicitudes de cualquier autoridad de control con respecto a la Información personal de GSK.

h) Notificará a GSK sin demora después de tener conocimiento de una violación de la seguridad de los datos personales con respecto a cualquier Información personal de GSK y prestará asistencia a GSK en relación con dicha violación.

i) Notificará a GSK sin demora si recibe una solicitud por escrito de (i) un interesado para ejercer cualquiera de sus derechos en relación con la Información personal de GSK de conformidad con la Legislación sobre protección de datos; o (ii) una autoridad de control en relación con el tratamiento de Información personal de GSK.

j) A menos que se establezca lo contrario en el Contrato, devolverá o destruirá toda la Información personal de GSK que obre en su posesión o esté bajo su control (incluida cualquier Información personal de GSK tratada por los subencargados del tratamiento autorizados) al resolverse o llegar a su vencimiento el Contrato.

k) A petición escrita de GSK, proporcionará a GSK la información razonable necesaria para demostrar el cumplimiento de este Anexo, lo que podrá incluir cualquier informe de auditoría de seguridad de terceros disponible.

Términos del responsable del tratamiento

En caso de que el proveedor actúe como responsable del tratamiento de la Información personal de GSK en virtud de la Legislación sobre protección de datos pertinente, se aplicarán las siguientes condiciones:

1. Cada una de las partes actúa como un responsable del tratamiento independiente y deberá cumplir con sus obligaciones en virtud de la Legislación sobre protección de datos aplicable. GSK y el Proveedor acuerdan que, en relación con los datos personales tratados en virtud de este Anexo, para los fines de la CCPA, el Proveedor no proporciona a GSK ninguna contraprestación monetaria ni de valor a cambio de la Información personal de GSK y, por lo tanto, GSK no vende la Información personal de GSK al Proveedor según lo definido por la CCPA.
2. Si el Proveedor recibe cualquier comunicación de una autoridad de control que esté relacionada directa o indirectamente con a) el tratamiento de la Información personal de GSK por parte del Proveedor; o (b) un incumplimiento potencial de la Legislación sobre protección de datos en relación con el tratamiento de la Información personal de GSK; el Proveedor, en la medida permitida por las leyes aplicables, deberá reenviar inmediatamente la comunicación a GSK y proporcionar cooperación y asistencia razonables a GSK en relación con la misma.
3. Si un interesado realiza una solicitud por escrito a cualquiera de las partes para ejercer cualquiera de sus derechos en virtud de la Legislación sobre protección de datos con respecto a la Información personal de GSK, la parte receptora deberá responder a dicha solicitud de conformidad con la Legislación sobre protección de datos. En la medida en que la solicitud se refiera al tratamiento de la Información personal de GSK realizado por la otra parte, la parte receptora: (i) inmediatamente y sin demora indebida, deberá reenviar la solicitud a la otra parte; y (ii) deberá cooperar y proporcionar asistencia razonable en relación con esa solicitud para permitir que la otra parte responda de conformidad con la Legislación sobre protección de datos.
4. Sin limitar ninguna disposición del Programa de seguridad, tras tener conocimiento de una violación de datos personales que afecte a la Información personal de GSK, el Proveedor (a) deberá notificar inmediatamente a GSK y proporcionar a GSK una descripción razonable de la violación; y (b) no deberá publicar ninguna comunicación relativa a la violación sin consultar primero a GSK, salvo que se notifique una violación a una autoridad de control en la medida requerida por la Legislación sobre protección de datos aplicable.

Transferencia internacional de datos

Cuando GSK, actuando como exportador de datos, transfiera la Información personal de GSK al Proveedor, actuando como importador de datos, de manera que constituya una transferencia de datos internacional restringida en virtud de la Legislación sobre protección de datos aplicable, ambas partes por el presente han celebrado y cumplirán las Cláusulas tipo aplicables que abarcan la relación entre las partes:

- El Anexo a la Decisión de aplicación de la Comisión de las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ("**Anexo**") junto con el MÓDULO UNO: Transferencia responsable del tratamiento a responsable del tratamiento (disponible **aquí**) e incorporados al presente mediante referencia según se actualicen, modifiquen, reemplacen o sustituyan de forma oportuna por la Comisión Europea; o (ii) cualquier acuerdo de transferencia internacional de datos correspondiente o equivalente, o adenda a las Cláusulas tipo, adoptados por la autoridad de control en el Reino Unido ("**Cláusulas tipo C2C**").
- El Anexo junto con el MÓDULO DOS: Transferencia responsable del tratamiento a encargado del tratamiento (disponible **aquí**) e incorporados al presente mediante referencia según se actualicen, modifiquen, reemplacen o sustituyan de forma oportuna por la Comisión Europea; o (ii) cualquier acuerdo de transferencia internacional de datos correspondiente o equivalente, o adenda a las Cláusulas tipo, adoptados por la autoridad de control en el Reino Unido ("**Cláusulas tipo C2P**").

"**Cláusulas tipo**" se refiere al Anexo junto con las Cláusulas tipo C2C (controller to controller) y las Cláusulas tipo C2P (controller to processor).

A los efectos de las Cláusulas tipo, las partes acuerdan cuanto sigue:

- La opción entre corchetes de la Cláusula 11 "Reparación" no se aplicará.
- La opción uno se selecciona para la cláusula 17 "Legislación aplicable" y se aplicará la legislación de Irlanda.
- Los tribunales de Irlanda tendrán la competencia en virtud de la cláusula 18 "Elección de foro y jurisdicción".

A efectos de las Cláusulas tipo C2P y C2C aplicables, tener en cuenta lo siguiente:

- Anexo 1 (Exportador e importador): GSK o el correspondiente destinatario de los servicios de GSK ubicado en la UE o el Reino Unido en virtud del acuerdo o acuerdos con el Proveedor, es un Exportador de datos en relación con la Información personal de GSK. El Proveedor es un Importador de datos en relación con la Información personal de GSK.
- Anexo 1 (Descripción de las Transferencias): consultar la definición de Información personal y Servicios que debe proporcionar el Importador. No se transfieren datos confidenciales. La frecuencia de la transferencia es continua. La naturaleza de las actividades de tratamiento y los fines de la transferencia se establecen en el acuerdo o acuerdos con el Proveedor. Los datos se conservarán de acuerdo con las políticas de conservación de datos del Exportador de datos.
- Anexo 1 (Autoridades competentes): según se establece en la cláusula 13 de las Cláusulas tipo C2C y las Cláusulas tipo C2P.
- Anexo 2 (Medidas técnicas y organizativas): consulte las Medidas de seguridad que se exponen a continuación.

Las partes acuerdan que la opción 2 de la cláusula 9 "Uso de Subencargados del tratamiento" de las Cláusulas tipo C-P deberá aplicarse cuando el Proveedor contrate a un subencargado del tratamiento y el Proveedor y el subencargado del tratamiento deberán acordar cumplir las **Cláusulas tipo P-P**, lo que significa i) el Anexo junto con el MÓDULO TRES: Transferencia encargado del tratamiento a encargado del tratamiento (disponible **aquí**) e incorporados al presente mediante referencia según se actualicen, modifiquen, remplacen o sustituyan de forma oportuna por la Comisión Europea; o (ii) cualquier acuerdo de transferencia internacional de datos correspondiente o equivalente, o adenda a las Cláusulas tipo adoptados por la autoridad de control en el Reino Unido.

En caso de que el Proveedor crea que no puede cumplir los requisitos establecidos razonablemente por GSK, el Proveedor deberá notificar a GSK inmediatamente su incapacidad y GSK tendrá derecho a resolver el Contrato.

Las Partes acuerdan que las Cláusulas tipo suscritas tendrán efecto en países fuera del Espacio Económico Europeo donde: (i) sus disposiciones se reconocen como una salvaguarda adecuada en relación con las transferencias internacionales de Datos personales a países no adecuados o (ii) la Legislación sobre protección de datos requiere la existencia de disposiciones contractuales para proteger las transferencias internacionales de Información personal. Al interpretar las Cláusulas tipo, en esos países, cualquier referencia al término "Estado miembro en el que esté establecido el exportador de datos" se interpretará que hace referencia al país en el que esté establecida la entidad de GSK; y cualquier referencia al Reglamento (UE) 2016/679 se referirá a la legislación del país en el que GSK esté establecida fuera del EEE. Cualquier referencia a un "País adecuado" se referirá a cualquier país que se considere que proporciona, o que proporcione de otro modo, un nivel equivalente de protección para los fines de la Legislación sobre de protección de datos aplicable, en los países fuera del Espacio Económico Europeo donde las Cláusulas tipo deberán abarcar las transferencias de Datos personales.

Medidas de seguridad

"Datos de GSK" se refiere a cualesquiera datos o información que sean proporcionados por GSK o en nombre de GSK u obtenido por el Proveedor o el Personal del Proveedor en relación con la negociación y ejecución del Contrato o el cumplimiento de las obligaciones del Proveedor en virtud del Contrato, incluidos aquellos datos e información que: (i) o bien sean creados, generados, recopilados o tratados por el Personal del Proveedor en el cumplimiento de las obligaciones del Proveedor en virtud del Contrato, (ii) o bien residan en, o se acceda a ellos a través de, los sistemas de información de GSK o los sistemas de información del Proveedor, así como cualesquiera datos e información derivados de los anteriores.

"**Tratamiento**" se refiere a toda operación o conjunto de operaciones efectuadas sobre una información o un dato, por medios automatizados o no, tales como la recogida, el registro, la organización, la estructuración, el almacenamiento, la adaptación o la modificación, la recuperación, la consulta, la utilización, la divulgación por transmisión, la difusión o cualquier otra forma de puesta a disposición, la alineación o la combinación, la limitación, el borrado o la destrucción.

"Entorno del Proveedor" se refiere a la combinación de hardware, software, sistemas operativos, sistemas de bases de datos, herramientas y componentes de red utilizados por o en nombre del Proveedor para recibir, mantener, tratar, almacenar, acceder o transmitir Datos de GSK.

"Personal del Proveedor" se refiere a todo el personal contratado o empleado por el Proveedor y sus Subcontratistas para llevar a cabo cualquier parte de los Servicios.

Este Programa de seguridad forma parte del Contrato entre GSK y el Proveedor. En caso de cualquier conflicto con respecto a la ciberseguridad entre las condiciones de este Programa de seguridad y las condiciones del Contrato, prevalecerá este Programa de seguridad. Los términos en mayúsculas que no se definan en este Programa de seguridad tendrán el significado que se les atribuya en otras partes del Contrato.

1. Responsabilidades. El Proveedor: (a) utilizará controles de encriptación fuertes para proteger todos los Datos de GSK frente a la divulgación, el acceso o la alteración no autorizados en tránsito hacia o desde el Entorno del Proveedor a través de redes de terceros; (b) mantendrá procesos de control en línea con las mejores prácticas del sector para detectar, prevenir y recuperarse de cualquier malware, virus y spyware, incluidos la actualización del software antivirus, antimalware y antispyware a intervalos regulares; (c) mantendrá políticas de gestión del acceso, procedimientos y controles técnicos en línea con las mejores prácticas del sector para garantizar que todo acceso a los datos de GSK bajo su control sea debidamente autorizado.

2. Violación de la seguridad. El Proveedor informará a GSK por correo electrónico a cstd@gsk.com de cualquier uso, pérdida, destrucción, divulgación, acceso, corrupción, modificación, venta, alquiler u otro Tratamiento de cualesquiera Datos de GSK (una "**Violación de la seguridad**"), accidental, no autorizado o ilegal y verificado, en un plazo de veinticuatro (24) horas desde la verificación del Proveedor. El Proveedor se asegurará de que todos los incidentes de seguridad que afecten a los Datos de GSK se gestionen de acuerdo con los

procedimientos adecuados de respuesta a incidentes y trabajará de buena fe con GSK para identificar la causa raíz y subsanar la Violación de la seguridad.

ตาราง

ข้อกำหนดการคุ้มครองข้อมูล – ข้อมูลส่วนบุคคลพื้นฐาน

บริษัทในเครือที่ครอบคลุม หมายถึง บริษัทในเครือแต่ละแห่งของ GSK ที่มีผลประโยชน์จากบริการในฐานะบุคคลที่สาม (รายชื่อที่ GSK จะจัดเตรียมให้ซัพพลายเออร์ตามคำร้องขอ) บริษัทในเครือคือนิติบุคคลใด ๆ ที่อยู่ภายใต้การควบคุม การควบคุมร่วมกัน หรือที่ควบคุมนิติบุคคลอื่น ๆ ดังกล่าว ในส่วนที่เกี่ยวกับนิติบุคคลอื่นใด "การควบคุม" และสิ่งที่ได้มาจากสิ่งนั้นจะหมายถึงความเป็นเจ้าของ (โดยตรงหรือโดยอ้อม) ของหุ้นที่มีสิทธิออกเสียงข้างมากของนิติบุคคลดังกล่าว หรือเป็นความสามารถ (โดยตรงหรือโดยอ้อม) เพื่อแต่งตั้งกรรมการเสียงข้างมากของนิติบุคคลดังกล่าวหรืออำนาจเพื่อสั่งการฝ่ายบริหารหรือนโยบายของนิติบุคคลดังกล่าว โดยสัญญาหรืออย่างอื่น

"กฎหมายการคุ้มครองข้อมูล" หมายถึง (ก) ข้อระเบียบการคุ้มครองข้อมูลทั่วไป (สหภาพยุโรป (EU)) 2016/679 ว่าด้วยการคุ้มครองบุคคลธรรมดาที่เกี่ยวกับการประมวลผลข้อมูลส่วนตัวและการเคลื่อนย้ายข้อมูลดังกล่าวโดยเสรี และกฎหมายและ/หรือระเบียบข้อบังคับที่บังคับใช้ซึ่งนำมาใช้และ/หรือเพิกถอนสิทธิ์ภายใต้กฎหมายนั้นและ/หรือแทนที่หรือมีผลมากกว่ากฎหมายนั้น (**GDPR**) และ (ข) GDPR ตามพระราชบัญญัติการคุ้มครองข้อมูลของสหราชอาณาจักร ปี 2018 (ค) กฎหมายว่าด้วยความเป็นส่วนตัวของผู้บริโภคของมลรัฐแคลิฟอร์เนีย ปี 2018 (Cal. Civ. Code 1798.100 - 1798.199) (**CCPA**) และ (ง) กฎหมายอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนตัว

"ข้อมูลส่วนบุคคล" หมายถึงข้อมูลส่วนตัวภายในชุดข้อมูลดังต่อไปนี้: ชื่อและ/หรือนามสกุล อักษรย่อ รายละเอียดการติดต่อที่ทำงาน การเป็นสมาชิกกลุ่ม หมายเลขเครือข่ายหรือหมายเลขประจำตัวผู้ใช้ ข้อมูลประจำตัวเพื่อเข้าสู่ระบบ ประวัติการทำงานและทักษะ เพศหรือคำนำหน้านาม การเข้าร่วมกิจกรรมของพนักงาน GSK และพนักงานเสริมที่ใช้บริการ

ข้อมูลส่วนบุคคลของ GSK หมายถึงข้อมูลส่วนบุคคลใด ๆ (1) ที่จัดหาโดยหรือในนามของ GSK ให้กับซัพพลายเออร์ (ซึ่งรวมถึงในกรณีที่ซัพพลายเออร์สามารถเข้าถึงข้อมูลส่วนตัวที่ GSK ถือครองหรือในนามของตน) หรือที่ซัพพลายเออร์เก็บรวบรวมหรือสร้างขึ้นในนามของ GSK (2) ที่ซัพพลายเออร์ประมวลผลภายใต้หรือที่เกี่ยวข้องกับข้อตกลงนี้ และ (3) ในส่วนที่ GSK เป็นผู้ควบคุมหรือเจ้าของ (หรือเทียบเท่า)

ตารางความปลอดภัย หมายถึง*ตารางการรักษาความปลอดภัยทางไซเบอร์ที่แนบมานี้ตามภาคผนวก 1*

คำว่า **ผู้ควบคุม การประเมินผลกระทบต่อการคุ้มครองข้อมูล เจ้าของข้อมูล ข้อมูลส่วนตัว การละเมิดข้อมูลส่วนตัว ผู้ประมวลผล การประมวลผล ผู้ให้บริการ** และ **หน่วยงานกำกับดูแล** จะเป็นไปตามที่กำหนดไว้ภายใต้กฎหมายการคุ้มครองข้อมูลที่เกี่ยวข้อง การอ้างอิงใด ๆ ถึง GSK จะหมายถึงนิติบุคคลที่ทำสัญญา GSK ที่ใช้ในข้อตกลงนี้ เช่นเดียวกับบริษัทในเครือที่ครอบคลุม

<u>ข้อกำหนดของผู้ประมวลผล</u>

<u>ในกรณีที่ซัพพลายเออร์ทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลของ GSK ภายใต้กฎหมายการคุ้มครองข้อมูลที่เกี่ยวข้อง ข้อกำหนดต่อไปนี้จะมีผลบังคับใช้:</u>

1. คู่สัญญาแต่ละฝ่ายจะต้องปฏิบัติตามภาระผูกพันภายใต้กฎหมายการคุ้มครองข้อมูลที่บังคับใช้ GSK และซัพพลายเออร์ตกลงกันว่าในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK ที่ประมวลผลภายใต้ข้อตกลงนี้ GSK จะเป็นผู้ควบคุมและซัพพลายเออร์จะเป็นผู้ประมวลผล สำหรับวัตถุประสงค์ของ CCPA ซัพพลายเออร์เป็นผู้ให้บริการแก่ GSK และการประมวลผลข้อมูลส่วนบุคคลของ GSK โดยซัพพลายเออร์จะดำเนินการเฉพาะเพื่อวัตถุประสงค์ของ GSK ตามตารางนี้เท่านั้น โดยจะไม่มีการตอบแทนทางการเงินหรือสิ่งมีมูลค่าอื่นใดโดยซัพพลายเออร์ให้กับ GSK และดังนั้น GSK จะไม่ขายข้อมูลส่วนบุคคลของ GSK ให้กับซัพพลายเออร์ตามที่ CCPA ได้กำหนด

2. ซัพพลายเออร์จะต้องปฏิบัติตามสิ่งต่อไปนี้ในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK

a) ประมวลผลข้อมูลส่วนบุคคลของ GSK ตามคำสั่งเป็นลายลักษณ์อักษรที่ชอบด้วยกฎหมายของ GSK เท่านั้นและเพียงเพื่อวัตถุประสงค์ในการจัดหาบริการโดยซัพพลายเออร์ให้กับ GSK ภายใต้ข้อตกลงนี้สำหรับระยะเวลาของข้อตกลงหรือระยะเวลาเพิ่มเติมใด ๆ ที่ระบุไว้ในข้อตกลง (หากมี)

b) ทั้งซัพพลายเออร์ หรือพนักงาน ตัวแทน ที่ปรึกษา หรือผู้รับโอนสิทธิ์ของตนใด ๆ จะไม่มีสิทธิ์ที่จะประมวลผลข้อมูลส่วนบุคคลของ GSK เพื่อประโยชน์เชิงพาณิชย์ของตนเองในรูปแบบใด ๆ

c) ดำเนินการและคงไว้ซึ่งมาตรการทางเทคนิคและความปลอดภัยขององค์กรที่เหมาะสม ซึ่งรวมถึงแต่ไม่จำกัดเพียงมาตรการที่กำหนดไว้ในตารางการรักษาความปลอดภัย การอ้างอิงในตารางการรักษาความปลอดภัยถึง "ข้อมูลของ GSK" จะรวมถึงข้อมูลส่วนบุคคลของ GSK

d) รักษาข้อมูลส่วนบุคคลของ GSK ไว้เป็นความลับตามข้อกำหนดของตารางนี้และการอ้างอิงในตารางนี้และตารางความปลอดภัยแก่ข้อมูลที่เป็นความลับของ GSK จะรวมถึงข้อมูลส่วนบุคคลของ GSK

e) กำหนดภาระผูกพันในการรักษาความลับเทียบเท่ากับภาระผูกพันที่กำหนดไว้ภายใต้ข้อตกลงที่เกี่ยวกับบุคลากรที่เกี่ยวข้องที่สามารถเข้าถึงข้อมูลส่วนบุคคลของ GSK

f) ไม่มีส่วนร่วมกับผู้ประมวลผลรายอื่น (“**ผู้ประมวลผลรายย่อย**”) โดยไม่ได้รับการอนุมัติเป็นลายลักษณ์อักษรล่วงหน้าจาก GSK (และเพื่อวัตถุประสงค์เหล่านี้ GSK ยินยอมให้ผู้ประมวลผลรายย่อยในหมวดหมู่ต่อไปนี้: ผู้ให้บริการโครงสร้างพื้นฐานเพื่อโฮสต์การใช้งานของผู้รับจ้างแต่ละราย และผู้ประมวลผลรายย่อยที่ทำให้ GSK ทราบในเวลาที่เข้าทำข้อตกลง) และถ่ายโอนข้อมูลส่วนบุคคลของ GSK ไปยังผู้ประมวลผลรายย่อยที่ได้รับอนุมัติดังกล่าวภายใต้สัญญาที่เป็นลายลักษณ์อักษรซึ่งกำหนดภาระผูกพันที่สอดคล้องกับที่กำหนดไว้ในตารางนี้เท่านั้น เมื่อซัพพลายเออร์แต่งตั้งผู้ประมวลผลรายย่อยตามข้อ 2(ฉ) นี้ จะยังคงต้องรับผิดต่อการกระทำและการละเว้นการกระทำของผู้ประมวลผลรายย่อย

g) ให้ความช่วยเหลือตามสมควรแก่ GSK โดย (1) ดำเนินการประเมินผลกระทบต่อการคุ้มครองข้อมูลที่จำเป็นตามกฎหมายและ/หรือการประเมินผลกระทบต่อการถ่ายโอนข้อมูล (2) ปฏิบัติตามสิทธิ์ของเจ้าของข้อมูล และ (3) ตอบสนองต่อคำร้องขอจากหน่วยงานกำกับดูแลในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK

h) แจ้งให้ GSK ทราบโดยทันทีเมื่อได้รับทราบถึงการละเมิดข้อมูลส่วนตัวในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลของ GSK และให้ความช่วยเหลือ GSK เกี่ยวกับการละเมิดดังกล่าว

i) แจ้งให้ GSK ทราบโดยทันทีหากได้รับคำร้องขอเป็นลายลักษณ์อักษรจาก (1) เจ้าของข้อมูลเพื่อใช้สิทธิ์ใด ๆ ของตนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK ภายใต้กฎหมายการคุ้มครองข้อมูล หรือ (2) หน่วยงานกำกับดูแลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ GSK

j) เว้นแต่จะกำหนดไว้เป็นอย่างอื่นในข้อตกลง ไม่ว่าจะส่งคืนหรือทำลายข้อมูลส่วนบุคคลของ GSK ทั้งหมดที่อยู่ในความครอบครองของตนหรืออยู่ภายใต้การควบคุมของตน (ซึ่งรวมถึงข้อมูลส่วนบุคคลของ GSK ที่ประมวลผลโดยผู้ประมวลผลรายย่อยที่ได้รับอนุญาต) ในการยุติหรือสิ้นสุดข้อตกลง และ

k) ตามคำร้องขอเป็นลายลักษณ์อักษรของ GSK ให้ข้อมูลที่เหมาะสมแก่ GSK ที่จำเป็นเพื่อแสดงความร่วมมือในการปฏิบัติตามตารางนี้ ซึ่งอาจรวมถึงรายงานการตรวจสอบความปลอดภัยของบุคคลที่สามที่มีอยู่

ข้อกำหนดของผู้ควบคุม

ในกรณีที่ซัพพลายเออร์ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลของ GSK ภายใต้กฎหมายการคุ้มครองข้อมูลที่เกี่ยวข้อง ข้อกำหนดต่อไปนี้จะมีผลบังคับใช้:

1. คู่สัญญาแต่ละฝ่ายทำหน้าที่เป็นผู้ควบคุมอิสระและจะต้องปฏิบัติตามภาระผูกพันของตนภายใต้กฎหมายการคุ้มครองข้อมูลที่บังคับใช้ GSK และซัพพลายเออร์ตกลงกันว่า ในส่วนที่เกี่ยวกับข้อมูลส่วนตัวที่ประมวลผลภายใต้ตารางนี้ เพื่อวัตถุประสงค์ของ CCPA ว่าไม่มีการตอบแทนทางการเงินหรือการตอบแทนที่มีมูลค่าอื่น ๆ จากซัพพลายเออร์ให้กับ GSK เพื่อแลกกับข้อมูลส่วนบุคคลของ GSK ดังนั้น GSK จะไม่ขายข้อมูลส่วนบุคคลของ GSK แก่ซัพพลายเออร์ตามที่ CCPA กำหนด

2. หากซัพพลายเออร์ได้รับการติดต่อสื่อสารใด ๆ จากหน่วยงานกำกับดูแลที่เกี่ยวข้องโดยตรงหรือโดยอ้อมกับ ก) การประมวลผลข้อมูลส่วนบุคคลของ GSK ของซัพพลายเออร์ หรือ (ข) การไม่ปฏิบัติตามกฎหมายการคุ้มครองข้อมูลที่อาจเกิดขึ้นที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ GSK ซัพพลายเออร์จะต้องส่งต่อการติดต่อสื่อสารไปยัง GSK โดยทันทีและให้ความร่วมมือและความช่วยเหลือตามสมควรแก่ GSK ที่เกี่ยวข้องกับสิ่งเดียวกัน ตามขอบเขตที่กฎหมายที่บังคับใช้อนุญาต

3. หากเจ้าของข้อมูลร้องขอเป็นลายลักษณ์อักษรให้ฝ่ายใดฝ่ายหนึ่งเพื่อใช้สิทธิ์ของตนภายใต้กฎหมายการคุ้มครองข้อมูลในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK ฝ่ายที่ได้รับจะต้องตอบสนองต่อคำร้องขอนั้นตามกฎหมายการคุ้มครองข้อมูลในขอบเขตที่คำร้องขอเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ GSK ที่ดำเนินการโดยอีกฝ่ายหนึ่ง ฝ่ายที่ได้รับจะต้อง: (1) ส่งต่อคำร้องขอไปยังอีกฝ่ายโดยทันทีและโดยไม่ชักช้า และ (2) ให้ความร่วมมือและให้ความช่วยเหลือตามสมควรที่เกี่ยวข้องกับคำร้องขอนั้นเพื่อให้อีกฝ่ายหนึ่งสามารถตอบสนองตามกฎหมายการคุ้มครองข้อมูล

4. โดยไม่จำกัดข้อกำหนดใด ๆ ของตารางการรักษาความปลอดภัย เมื่อทราบถึงการละเมิดข้อมูลส่วนตัวที่ส่งผลต่อข้อมูลส่วนบุคคลของ GSK ซัพพลายเออร์จะต้อง (ก) แจ้งให้ GSK ทราบโดยทันทีและให้คำอธิบายที่เหมาะสมแก่ GSK เกี่ยวกับการละเมิดนั้น และ (ข) ไม่เผยแพร่การติดต่อสื่อสารใด ๆ เกี่ยวกับการละเมิดโดยปราศจากการปรึกษากับ GSK ก่อน เว้นแต่ว่าอาจแจ้งการละเมิดต่อหน่วยงานกำกับดูแลในขอบเขตที่กฎหมายการคุ้มครองข้อมูลที่บังคับใช้กำหนด

การถ่ายโอนข้อมูลระหว่างประเทศ

ในกรณีที่ GSK ซึ่งทำหน้าที่เป็นผู้ส่งออกข้อมูล ได้ถ่ายโอนข้อมูลส่วนบุคคลของ GSK ไปยังซัพพลายเออร์ ซึ่งทำหน้าที่เป็นผู้นำเข้าข้อมูลในลักษณะที่ก่อให้เกิดการถ่ายโอนข้อมูลระหว่างประเทศที่จำกัดภายใต้กฎหมายการคุ้มครองข้อมูลที่บังคับใช้
คู่สัญญาทั้งสองฝ่ายได้ทำขึ้นร่วมกันในที่นี้และจะปฏิบัติตามข้อบทต้นแบบที่เกี่ยวข้องที่ครอบคลุมความสัมพันธ์ระหว่างคู่สัญญา:

- ภาคผนวกของคณะกรรมาธิการการดำเนินการตัดสินใจเกี่ยวกับข้อสัญญามาตรฐานสำหรับการถ่ายโอนข้อมูลส่วนตัวไปยังประเทศที่สามตามข้อระเบียบสหภาพยุโรป (EU) 2016/679 ของรัฐสภายุโรปและสภายุโรป (“**ภาคผนวก**”) พร้อมกับโมดูลที่หนึ่ง: ถ่ายโอนผู้ควบคุมไปยังผู้ควบคุม (มีให้บริการ **ที่นี่**) และรวมอยู่ในที่นี้โดยการอ้างอิงตามที่คณะกรรมาธิการยุโรปได้ปรับปรุง แก้ไข แทนที่

หรือมีผลมากกว่าเป็นครั้งคราว และ/หรือ (2)
ข้อตกลงการถ่ายโอนข้อมูลระหว่างประเทศที่เกี่ยวข้องหรือเทียบเท่าหรือภาคผนวกของข้อบทต้นแบบที่นำมาใช้โดยหน่วยงานกำกับดูแลในสหราชอาณาจักร ("**ข้อบทต้นแบบ C2C**")

- ภาคผนวกพร้อมกับโมดูลที่สอง: ถ่ายโอนผู้ควบคุมไปยังผู้ประมวลผล (มีให้บริการ **ที่นี่**)
และรวมอยู่ในที่นี้โดยการอ้างอิงตามที่คณะกรรมาธิการยุโรปได้ปรับปรุง แก้ไข แทนที่ หรือมีผลมากกว่าเป็นครั้งคราว และ/หรือ (2)
ข้อตกลงการถ่ายโอนข้อมูลระหว่างประเทศที่เกี่ยวข้องหรือเทียบเท่าหรือภาคผนวกของข้อบทต้นแบบที่นำมาใช้โดยหน่วยงานกำกับดูแลในสหราชอาณาจักร ("**ข้อบทต้นแบบ C2P**")

"**ข้อบทต้นแบบ**" หมายถึงภาคผนวกพร้อมกับข้อบทต้นแบบ C2C และข้อบทต้นแบบ C2P

เพื่อวัตถุประสงค์ของข้อบทต้นแบบ คู่สัญญาทั้งสองฝ่ายตกลงกันว่า:

- ตัวเลือกในวงเล็บเหลี่ยมของข้อ 11 "การชดใช้" จะไม่นำมาใช้
- ตัวเลือกที่หนึ่งถูกเลือกสำหรับข้อ 17 "กฎหมายที่ใช้บังคับ" และกฎหมายของไอร์แลนด์จะมีผลบังคับใช้
- ศาลของไอร์แลนด์จะมีเขตอำนาจศาลภายใต้ข้อ 18 "ตัวเลือกของสถานที่ตัดสินและเขตอำนาจศาล"

สำหรับวัตถุประสงค์ของข้อบทต้นแบบ C2P และข้อบทต้นแบบ C2C ที่บังคับใช้ โปรดทราบถึงสิ่งต่อไปนี้:

- ภาคผนวก 1 (ผู้ส่งออกและผู้นำเข้า): GSK หรือผู้รับบริการของ GSK ที่เกี่ยวข้องซึ่งตั้งอยู่ในสหภาพยุโรปและ/หรือสหราชอาณาจักรภายใต้ข้อตกลงกับซัพพลายเออร์จะเป็นผู้ส่งออกข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK ซัพพลายเออร์จะเป็นผู้นำเข้าข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ GSK
- ภาคผนวก 1 (คำอธิบายของการโอน): โปรดดูคำจำกัดความของข้อมูลส่วนบุคคลและบริการที่ผู้นำเข้าจัดเตรียมให้ จะไม่มีการถ่ายโอนข้อมูลที่ละเอียดอ่อน ความถี่ของการถ่ายโอนเป็นแบบต่อเนื่อง ลักษณะของกิจกรรมการประมวลผลและวัตถุประสงค์ของการถ่ายโอนจะระบุไว้ในข้อตกลงกับซัพพลายเออร์ ข้อมูลจะถูกเก็บรักษาตามนโยบายการเก็บรักษาข้อมูลของผู้ส่งออกข้อมูล
- ภาคผนวก 1 (หน่วยงานผู้มีอำนาจ): ตามที่กำหนดไว้ในข้อ 13 ของข้อบทต้นแบบ C2C และข้อบทต้นแบบ C2P
- ภาคผนวก 2 (มาตรการทางเทคนิคและองค์กร): โปรดดูที่มาตรการรักษาความปลอดภัยที่กำหนดไว้ด้านล่าง

คู่สัญญาตกลงว่าตัวเลือกที่ 2 ของข้อ 9 "การใช้ผู้ประมวลผลรายย่อย" ของข้อบทต้นแบบ C-P จะใช้บังคับในกรณีที่ซัพพลายเออร์ว่าจ้างผู้ประมวลผลรายย่อย และซัพพลายเออร์และผู้ประมวลผลรายย่อยต้องตกลงที่จะปฏิบัติตาม**ข้อบทต้นแบบ P-P** ซึ่งหมายความว่า 1) ภาคผนวกพร้อมกับโมดูลที่สาม: ถ่ายโอนผู้ประมวลผลไปยังผู้ประมวลผล (มีให้บริการ **ที่นี่** และรวมอยู่ในที่นี้โดยอ้างอิงตามที่คณะกรรมาธิการยุโรปได้ปรับปรุง แก้ไข แทนที่ หรือมีผลมากกว่าเป็นครั้งคราว และ/หรือ (2) ข้อตกลงการถ่ายโอนข้อมูลระหว่างประเทศที่เกี่ยวข้องหรือเทียบเท่าหรือภาคผนวกของข้อบทต้นแบบที่นำมาใช้โดยหน่วยงานกำกับดูแลในสหราชอาณาจักร

ในกรณีที่ซัพพลายเออร์ไม่เชื่อว่าจะสามารถปฏิบัติตามข้อกำหนดตามที่ GSK ได้กำหนดไว้อย่างสมเหตุสมผล ซัพพลายเออร์จะต้องแจ้งให้ GSK ทราบโดยทันทีเกี่ยวกับการไร้ความสามารถของตน และ GSK จะมีสิทธิ์ยุติข้อตกลง

คู่สัญญาตกลงว่าข้อบทต้นแบบที่ทำขึ้นจะมีผลในประเทศนอกเขตเศรษฐกิจยุโรป โดยที่: (1) บทบัญญัติของตนได้รับการยอมรับว่าเป็นมาตรการป้องกันที่เหมาะสมที่เกี่ยวข้องกับการถ่ายโอนข้อมูลส่วนตัวระหว่างประเทศไปยังประเทศที่มีไม่เพียงพอ หรือ (2) กฎหมายการคุ้มครองข้อมูลกำหนดให้มีบทบัญญัติตามสัญญาเพื่อป้องกันการถ่ายโอนข้อมูลส่วนบุคคลระหว่างประเทศ เพื่อตีความข้อบทต้นแบบในประเทศเหล่านั้น การอ้างอิงใด ๆ ถึงคำว่า "รัฐสมาชิกซึ่งมีการจัดตั้งผู้ส่งออกข้อมูล" จะถูกตีความให้หมายถึงประเทศที่จัดตั้งนิติบุคคลของ GSK และการอ้างอิงถึงข้อระเบียบสหภาพยุโรป (EU) 2016/679 ให้เป็นไปตามกฎหมายของประเทศที่ GSK จัดตั้งขึ้นนอก EEA การอ้างอิงถึง "ประเทศที่มีเพียงพอ" จะหมายถึงประเทศใด ๆ ที่จัดให้มีหรือมอบระดับการคุ้มครองที่เท่าเทียมกันสำหรับวัตถุประสงค์ของกฎหมายการคุ้มครองข้อมูลที่บังคับใช้ในประเทศเหล่านั้นนอกเขตเศรษฐกิจยุโรปที่ข้อบทต้นแบบจะครอบคลุมการถ่ายโอนข้อมูลส่วนตัว

มาตรการความปลอดภัย

"**ข้อมูลของ GSK**" หมายถึงข้อมูลใด ๆ ที่จัดหาให้โดยหรือในนามของ GSK หรือซัพพลายเออร์หรือบุคลากรของซัพพลายเออร์ได้รับที่เกี่ยวข้องกับการเจรจาและการลงนามข้อตกลงหรือการปฏิบัติตามภาระผูกพันของซัพพลายเออร์ภายใต้ข้อตกลง ซึ่งรวมถึงข้อมูลดังกล่าวที่: (1) ถูกสร้างขึ้น ผลิต เก็บรวบรวม หรือประมวลผลโดยบุคลากรของซัพพลายเออร์ในการปฏิบัติตามภาระผูกพันของซัพพลายเออร์ภายใต้ข้อตกลง หรือ (2) อยู่ในหรือเข้าถึงได้ผ่านระบบข้อมูลของ GSK หรือระบบข้อมูลซัพพลายเออร์ ตลอดจนข้อมูลใด ๆ ที่ได้มาจากสิ่งข้างต้น

"**การประมวลผล**" หมายถึง การดำเนินการหรือชุดของการดำเนินการใด ๆ ที่ดำเนินการกับสารสนเทศหรือข้อมูลใด ๆ ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ก็ตาม เช่น การรวบรวม การบันทึก การจัดระเบียบ การจัดโครงสร้าง การจัดเก็บ การปรับหรือการเปลี่ยนแปลง

การดึงข้อมูล การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ หรือทำให้พร้อมใช้งาน การจัดตำแหน่งหรือการรวมกัน การจำกัด การลบออก หรือการทำลาย

"สภาพแวดล้อมของซัพพลายเออร์" หมายถึงการรวมกันของฮาร์ดแวร์ ซอฟต์แวร์ ระบบปฏิบัติการ ระบบฐานข้อมูล เครื่องมือและส่วนประกอบเครือข่ายที่ใช้โดยหรือในนามของซัพพลายเออร์เพื่อรับ บำรุงรักษา ประมวลผล จัดเก็บ เข้าถึง หรือส่งข้อมูลของ GSK

"บุคลากรของซัพพลายเออร์" หมายถึง บุคลากรใด ๆ และทุกคนที่ซัพพลายเออร์และผู้รับเหมาช่วงของตนว่าจ้างหรือจ้างเพื่อดำเนินการส่วนใดส่วนหนึ่งของบริการ

ตารางการรักษาความปลอดภัยนี้เป็นส่วนหนึ่งของข้อตกลงโดยและระหว่าง GSK และซัพพลายเออร์
ในกรณีที่มีข้อขัดแย้งเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ระหว่างข้อกำหนดของตารางการรักษาความปลอดภัยนี้กับข้อกำหนดของข้อตกลง ตารางการรักษาความปลอดภัยนี้จะมีผลบังคับ
คำที่ใช้อักษรตัวพิมพ์ใหญ่ที่ไม่ได้กำหนดไว้ในตารางการรักษาความปลอดภัยนี้จะมีความหมายตามที่กำหนดไว้ในส่วนอื่น ๆ ของข้อตกลง

1. **ความรับผิดชอบ** ซัพพลายเออร์จะ: (ก) ใช้การควบคุมการเข้ารหัสที่แข็งแรงเพื่อปกป้องข้อมูลของ GSK ทั้งหมดจากการเปิดเผย การเข้าถึง หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
ในระหว่างการส่งผ่านเข้าหรือออกจากสภาพแวดล้อมของซัพพลายเออร์ผ่านเครือข่ายของบุคคลที่สาม (ข)
รักษากระบวนการควบคุมให้สอดคล้องกับแนวปฏิบัติที่ดีที่สุดของอุตสาหกรรมในการตรวจจับ ป้องกัน และกู้คืนจากมัลแวร์ ไวรัส และสปายแวร์ รวมถึงการอัพเดตซอฟต์แวร์ การป้องกันไวรัส ซอฟต์แวร์ป้องกันมัลแวร์และสปายแวร์ตามช่วงเวลาเป็นประจำ (ค)
รักษานโยบายการจัดการการเข้าถึง ขั้นตอน และการควบคุมทางเทคนิคให้สอดคล้องกับแนวปฏิบัติที่ดีที่สุดของอุตสาหกรรม
เพื่อให้แน่ใจว่าการเข้าถึงข้อมูล GSK ทั้งหมดในการควบคุมนั้นได้รับอนุญาตอย่างเหมาะสม

2. **การละเมิดความปลอดภัย** ซัพพลายเออร์จะรายงานต่อ GSK ทางอีเมลไปที่ cstd@gsk.com ถึงการใช้งาน การสูญเสีย การทำลาย การเปิดเผย การเข้าถึง การทุจริต การปรับเปลี่ยน การขาย การเช่า หรือการประมวลผลข้อมูล GSK ใด ๆ โดยไม่ได้ตั้งใจ ไม่ได้รับอนุญาต หรือมิชอบด้วยกฎหมายที่ตรวจสอบแล้ว (**"การละเมิดความปลอดภัย"**) ภายในยี่สิบสี่ (24) ชั่วโมงของการตรวจสอบจากซัพพลายเออร์
ซัพพลายเออร์จะตรวจสอบให้แน่ใจว่าเหตุการณ์ด้านความปลอดภัยทั้งหมดที่เกี่ยวข้องกับข้อมูลของ GSK ได้รับการจัดการตามขั้นตอนการตอบสนองต่อเหตุการณ์ที่เหมาะสม โดยซัพพลายเออร์จะทำงานร่วมกับ GSK โดยสุจริตเพื่อระบุสาเหตุที่แท้จริงและแก้ไขการละเมิดความปลอดภัย

PROGRAM

VERİ KORUMA KOŞULLARI – TEMEL KİŞİSEL BİLGİ

Kapsamdaki Bağlı Kuruluş, üçüncü bir taraf olarak Hizmetlerden yararlanan her GSK Bağlı Kuruluşu demektir (bunların listesi istek üzerine GSK tarafından Tedarikçiye sağlanacaktır). Bir Bağlı Kuruluş, başka bir tüzel kişi bakımından, söz konusu tüzel kişi tarafından Kontrol Edilen, onun ile ortak Kontrol altında bulunan veya onu Kontrol Eden tüzel kişi demektir. "Kontrol" ve bunun türevleri, sözleşme yolu ile veya başka bir şekilde, söz konusu tüzel kişinin oy hakkına sahip hisselerinin çoğunluğunun mülkiyeti (doğrudan veya dolaylı olarak) veya söz konusu tüzel kişinin yönetim kurulu üyelerinin çoğunluğunu atama yeteneği (doğrudan veya dolaylı olarak) veya söz konusu tüzel kişinin yönetimini veya politikalarını yönetme yetkisi demektir;

Veri Koruma Yasaları şu demektir: (a) kişisel bilgilerin işlenmesi ile ilgili olarak gerçek kişilerin korunması konusunda ve söz konusu verilerin serbest dolaşımı konusunda Genel Veri Koruma Düzenlemesi (AB) 2016/679 ve onun altında istisnalar uygulayan ve/veya yürürlüğe koyan ve/veya onun yerini alan veya onu hükümsüz kılan tüm geçerli yasalar ve/veya düzenlemeler (**GDPR**) ve (b) 2018 Birleşik Krallık Veri Koruma Yasası tarafından uyarlanan GDPR; (c) 2018 Kaliforniya Tüketici Gizliliği Yasası (Kal. Medeni Kanunu 1798.100 – 1798.199) (**CCPA**) ve (d) kişisel veri işlemeyi ilgilendiren diğer tüm yasalar;

Kişisel Bilgi şu küme içindeki kişisel veriler demektir: Hizmetleri kullanan GSK çalışanlarının ve tamamlayıcı personelin adı ve/veya soyadı, adın baş harfleri, iş iletişim bilgileri, grup üyelikleri, ağ veya kullanıcı tanımlama numarası, oturum açma bilgileri, iş geçmişi veya becerileri, cinsiyet veya unvan, etkinlik katılımı

GSK Kişisel Bilgisi: (i) GSK tarafından veya onun adına Tedarikçiye sağlanan (Tedarikçinin GSK tarafından veya onun adına tutulan Kişisel Bilgilere erişimi olan durumlar dâhil) veya Tedarikçinin GSK adına topladığı veya ürettiği; (ii) bu Sözleşme uyarınca veya ona bağlı olarak Tedarikçi tarafından işlenen ve (iii) GSK'nin sorumlusu veya sahibi (veya dengi) olduğu herhangi bir Kişisel Bilgi demektir;

Güvenlik Programı, *bu belgeye Ek 1 olarak eklenmiş olan siber güvenlik programı demektir*.

Sorumlu, veri koruma etki değerlendirmesi, veri sahibi, kişisel veriler, kişisel veri ihlali, işleyici, işleme, hizmet sağlayıcısı ve **denetleme makamı** terimleri ilgili Veri Koruma Yasaları Kapsamında tanımlandığı gibi olacaktır. GSK'ye verilen herhangi bir referans Sözleşmede kullanılan GSK sözleşme tarafının yanı sıra GSK Bağlı Kuruluşları demek olacaktır.

İşleyici Koşulları

Tedarikçinin ilgili Veri Koruma Yasaları kapsamında GSK Kişisel Bilgileri için bir işleyici olarak hareket ediyor olması durumunda aşağıdaki koşullar geçerli olacaktır:

1. Tarafların her birisi Geçerli Veri Koruma Yasaları kapsamındaki yükümlülüklerine uyacaktır. Bu Sözleşme kapsamında işlenen GSK Kişisel Bilgileri ile ilgili olarak GSK'nin sorumlu ve Tedarikçinin işleyici olacağı konusunda GSK ve Tedarikçi anlaşmaya varmaktadır. CCPA'nın amaçları için, Tedarikçi GSK'ye bir hizmet sağlayıcıdır ve GSK Kişisel Bilgilerinin Tedarikçi tarafından işlenmesi yanızca bu Programa uygun şekilde GSK'nin amaçları için yapılacaktır, Tedarikçi tarafından GSK'ye hiçbir parasal veya başka bir değerli karşılık sağlanmamaktadır ve bu yüzden GSK Tedarikçiye CCPA tarafından tanımlanan şekilde Kişisel Bilgi satmamaktadır.

2. Tedarikçi, GSK Kişisel Bilgileri ile ilgili aşağıdakiler ile uyumlu olacaktır:

a) GSK'nin Kişisel Bilgilerini yalnızca GSK'nin yasal yazılı talimatlarına göre ve yalnızca bu Sözleşme kapsamında Sözleşmenin süresi veya geçerli ise Sözleşmede belirtilen herhangi bir ilave dönem boyunca Tedarikçi tarafından GSK'ye Hizmetler sağlanmasının amaçları için işlemek;

b) ne Tedarikçi ne de onun herhangi bir çalışanı, temsilcisi, danışmanı veya vekili GSK Kişisel Bilgilerini kendi ticari çıkarı için herhangi bir şekilde işlemek için hiçbir hakkı olmayacaktır;

c) bir sınırlandırma olmasızın Güvenlik Programında belirtilen önlemler dâhil olmak üzere uygun teknik ve kurumsal güvenlik önlemlerini uygulamak ve sürdürmek. Güvenlik Programında "GSK Verileri" için verilen referanslar GSK Kişisel Bilgilerini içerecektir;

d) GSK Kişisel Bilgilerini bu Programın koşullarına uygun şekilde gizli tutmak ve bu Programda ve Güvenlik Programında GSK Gizli Bilgileri için verilen referanslar GSK Kişisel Bilgilerini içerecektir;

e) GSK Kişisel Bilgilerine erişimi olan ilgili personel için, Sözleşme kapsamında belirtilen yükümlülüklere denk gizlilik yükümlülüklerini zorunlu tutmak;

f) GSK'nin önceden yazılı onayı oılmadan başka bir işleyici ("**alt işleyici"**) görevlendirmemek (ve bu amaçlar için GSK şu alt işleyici kategorilerine olur vermektedir: barındırma altyapı hizmeti sağlayıcıları ve Sözleşme yapıldığı zaman GSK'ye bildirilen münferit yükleniciler ve alt işleyiciler kullanılması) ve GSK Kişisel Bilgilerini bu gibi onanmış alt işleyicilere yalnızca bu Programda belirtilenler ile tutarlı olan yükümlülükleri zorunlu tutan yazılı bir sözleşme kapsamında aktarmak. Tedarikçi bu madde 2(f) ile uyumlu bir alt işleyici atadığı zaman alt işleyicinin davranışlarından ve ihmallerinden sorumlu durumda kalır;

g) şunlar için GSK'ye makul yardım sağlamak: (i) yasal olarak gerekli olan herhangi bir veri koruma etki değerlendirmesinin ve/veya veri aktarma etki değerlendirmesinin yapılması; (ii) veri sahibi haklarına uyulması ve (iii) GSK Kişisel Bilgileri ile ilgili olarak herhangi bir denetleme makamından gelen taleplere yanıt verilmesi;

h) herhangi bir GSK Kişisel Bilgisi ile ilgili bir kişisel veri ihlalinin farkına vardıktan sonra gecikmeden GSK'yi bilgilendirmek ve söz konusu ihlal ile ilgili olarak GSK'ye yardımda bulunmak;

i) (i) bir veri sahibinden Veri Koruma Yasaları kapsamında GSK Kişisel Bilgileri ile ilgili haklarının herhangi birisini kullanmak için veya (ii) bir denetleme makamından GSK Kişisel Bilgilerinin işlenmesi ile ilgili olarak yazılı bir talep alması durumunda gecikmeden GSK'yi bilgilendirmek;

j) Sözleşmede başka türlü belirtilmediği sürece, Sözleşmenin feshedilmesi veya süresinin bitmesi üzerine elinde veya kontrolü altında bulunan GSK Kişisel Bilgilerini (izin verilmiş alt işleyiciler tarafından işlenen GSK Kişisel Bilgileri dâhil olmak üzere) ya iade etmek ya da imha etmek ve

k) GSK'nin yazılı isteği üzerine, bu Programa uyumluluğu kanıtlamak için gerekli olan makul bilgileri GSK'ye sağlamak ve bunlar, mevcut olabilecek herhangi bir üçüncü taraf güvenlik yoklaması raporunu içerebilir.

Sorumlu Koşulları

Tedarikçinin ilgili Veri Koruma Yasaları kapsamında GSK Kişisel Bilgileri için bir sorumlu olarak hareket ediyor olması durumunda aşağıdaki koşullar geçerli olacaktır:

1. Tarafların her birisi bağımsız bir sorumlu olarak hareket etmektedir ve Geçerli Veri Koruma Yasaları kapsamındaki yükümlülüklerine uyacaktır. CCPA'nın amaçları için bu Program kapsamında işlenen kişisel veriler ile ilgili olarak, GSK Kişisel Bilgileri karşılığında Tedarikçi tarafından GSK'ye hiçbir parasal veya başka bir değerli karşılık sağlanmamakta olduğu ve bu yüzden GSK'nın Tedarikçiye CCPA tarafından tanımlanan şekilde Kişisel Bilgi satmakta olmadığı konusunda GSK ve Tedarikçi mutabakata varmaktadır.
2. Tedarikçi, bir denetleme makamından a) Tedarikçinin GSK Kişisel Bilgilerini işlemesi veya (b) GSK Kişisel Bilgilerinin işlenmesi ile ilgili olarak Veri Koruma Yasalarına potansiyel olarak herhangi bir şekilde uyulmaması ile doğrudan veya dolaylı şekilde ilgili herhangi bir iletişim aldığı takdirde Tedarikçi geçerli yasalar tarafından izin verilen ölçüde bu iletişimi hemen GSK'ye iletecek ve bunun ile ilgili olarak GSK'ye makul bir iş birliği ve yardım sağlayacaktır.
3. Bir veri sahibi GSK Kişisel Bilgileri bakımından Veri Koruma Yasaları kapsamındaki haklarından herhangi birisini kullanmak için taraflardan herhangi birisine yazılı bir talep ilettiği takdirde alıcı taraf bu isteğe Veri Koruma Yasalarına uygun şekilde yanıt verecektir. Bu istek GSK Kişisel Bilgilerinin diğer tarafça işlenmesini ilgilendirdiği takdirde alıcı taraf: (i) isteği hemen ve gereksiz bir gecikme olmadan diğer tarafa iletecek ve (ii) diğer tarafın Veri Koruma Yasalarına uygun şekilde yanıt verebilmesini sağlamak için istek ile ilgili olarak iş birliği yapacak ve makul şekilde yardım edecektir.
4. Güvenlik Programının hiçbir hükmünü sınırlandırmaksızın, Tedarikçi, GSK Kişisel Bilgilerini etkileyen herhangi bir kişisel veri ihlalinin farkına varması üzerine (a) hemen GSK'ye bildirim verecek ve GSK'ye ihlalin makul bir açıklamasını sağlayacaktır ve (b) önce GSK'ye danışmadan ihlal hakkında hiçbir iletişim yayınlamayacaktır ancak geçerli Veri Koruma Yasası tarafından gerekli tutulduğu ölçüde bir ihlali bir denetleme makamına bildirebilir.

Uluslararası Veri Aktarımı

GSK'nin bir veri ihracatçısı olarak hareket ederek veri ithalatçısı olarak hareket eden Tedarikçiye geçerli Veri Koruma Yasaları kapsamında kısıtlamalı uluslararası veri aktarımı oluşturan bir tarzda GSK Kişisel Bilgilerini aktarması durumu için her iki taraf, tarafların arasındaki ilişkiyi kapsayan geçerli Model Maddeleri bu belge ile imzalamaktadır ve bunlara uyacaktır:

- Avrupa Parlamentosunun ve Konseyinin (EU) 2016/679 Düzenlemesi uyarınca üçüncü ülkelere kişisel verilerin aktarımı için standart sözleşme maddeleri hakkında Komisyon Uydulama Kararına Ek ("**Ek**") ve yanı sıra MODÜL BİR: Aktarma sorumludan sorumluya (**burada** mevcuttur) ve Avrupa Komisyonu tarafından zaman zaman güncellenmiş, tadil edilmiş, değiştirilmiş veya yerine başka şey konmuş şekli ile referans yolu ile bu belgeye dâhil edilmiştir ve/veya (ii) Birleşik Krallık'ta denetleme makamı tarafından benimsenmiş olarak herhangi bir ilgili veya eşdeğer uluslararası veri aktarımı sözleşmesi veya Model Maddelere yapılan bir ek ("**C2C Model Maddeleri**");
- Ek ve yanı sıra MODÜL İKİ: Aktarma sorumludan işleyiciye (**burada** mevcuttur) ve Avrupa Komisyonu tarafından zaman zaman güncellenmiş, tadil edilmiş, değiştirilmiş veya yerine başka şey konmuş şekli ile referans yolu ile bu belgeye dâhil edilmiştir ve/veya (ii) Birleşik Krallık'ta denetleme makamı tarafından benimsenmiş olarak herhangi bir ilgili veya eşdeğer uluslararası veri aktarımı sözleşmesi veya Model Maddelere yapılan bir ek ("**C2P Model Maddeleri**");

"**Model Maddeler**", C2C Model Maddeleri ve C2P Model Maddeleri ile birlikte Ek demek olacaktır.

Taraflar, Model Maddelerin amaçları için şu şekilde anlaşmaya varmaktadır:

- Madde 11 "Telafi" içindeki köşeli parantez içindeki seçenek geçerli olmayacaktır
- Madde 17 "Geçerli Hukuk" için seçenek bir seçilmiştir ve İrlanda hukuku geçerli olacaktır.
- Madde 18 "Mahkeme ve Yargılama Yeri Tercihi" kapsamında İrlanda mahkemeleri yargı yetkisine sahip olacaktır.

Geçerli C2C Model Maddelerinin ve C2P Model Maddelerinin amaçları için lütfen şunlara dikkat edin:

- Ek 1 (İhracatçıdan İthalatçıya): Tedarikçi ile sözleşme(ler) kapsamında AB ve/veya Birleşik Krallık içinde yerleşik olan GSK veya ilgili GSK hizmet alıcıları, GSK Kişisel Bilgileri ile ilgili olarak bir Veri İhracatçısıdır. Tedarikçi, GSK Kişisel Bilgileri ile ilgili olarak bir Veri İthalatçısıdır
- Ek 1 (Aktarmaların Açıklaması): lütfen Kişisel Bilginin ve İthalatçı tarafından sağlanacak olan Hizmetlerin tanımına bakın. Duyarlı bilgi aktarılmamaktadır. Aktarımın sıklığı sürekli şekildedir. İşleme faaliyetlerinin özelliği ve aktarımın amaçları Tedarikçi ile Sözleşme(ler)de belirtilmiştir. Veriler Veri İhracatçısının veri saklama politikalarına uygun şekilde saklanacaktır.
- Ek 1 (Yetkili Makamlar): C2C Model Maddeleri ve C2P Model Maddeleri içinde madde 13'te belirtildiği gibidir

- Ek 2 (Teknik ve Kurumsal Önlemler): lütfen aşağıda belirtilen Güvenlik Önlemlerine bakın

Tedarikçi bir alt işleyici görevlendirdiği zaman C-P Model Maddelerindeki madde 9 "Alt İşleyiciler Kullanılması" içindeki seçenek 2'nin geçerli olacağı ve Tedarikçinin ve alt işleyicinin **P-P Model Maddelerine** uymak konusunda anlaşmaya varacağı hakkında taraflar mutabakata varmaktadır ve bu da şu anlama gelmektedir: i) Ek ve yanı sıra MODÜL ÜÇ: Aktarma işleyiciden işleyiciye (**burada** mevcuttur) ve Avrupa Komisyonu tarafından zaman zaman güncellenmiş, tadil edilmiş, değiştirilmiş veya yerine başka şey konmuş şekli ile referans yolu ile bu belgeye dâhil edilmiştir ve/veya (ii) Birleşik Krallık'ta denetleme makamı tarafından benimsenmiş olarak herhangi bir ilgili veya eşdeğer uluslararası veri aktarımı sözleşmesi veya Model Maddelere yapılan bir ek;

Tedarikçi, GSK tarafından makul şekilde belirtilen gereksinimleri karşılayabileceğine inanmadığı takdirde Tedarikçi bu olanaksızlığını hemen GSK'ye bildirecektir ve GSK Sözleşmeyi feshetme hakkına sahip olacaktır.

Taraflar, imzalanan Model Maddelerin, Avrupa Ekonomik Alanı dışında bulunan ve: (i) uygun olmayan ülkelere uluslararası Kişisel Veri aktarımları ile ilgili olarak Model Maddelerin hükümlerinin uygun bir koruma önlemi olarak görüldüğü veya (ii) uluslararası Kişisel Bilgi aktarımlarını korumak için Veri Koruma Yasalarının sözleşmeye dayalı hükümlerin var olmasını gerektirdiği ülkelerde geçerli olacağını kabul etmektedir. Bu ülkelerde Model Maddeler yorumlanırken "Veri ihracatçısının kurulu olduğu Üye Devlet" terimine verilen tüm referanslar GSK kuruluşunun kurulu olduğu ülke anlamına gelecek şekilde yorumlanacaktır ve (EU) 2016/679 Düzenlemesine yapılan tüm atıflar GSK'nin AEA dışında kurulu olduğu ülkenin yasasına yapılan atıf olacaktır. Bir "Uygun Ülke" için verilen tüm referanslar, Model Maddelerin Kişisel Veri aktarımlarını kapsayacağı Avrupa Ekonomik Alanı dışındaki ülkelerde, geçerli Veri Koruma Yasalarının amaçları için denk bir koruma düzeyi sağladığı kabul edilen veya sağlayan herhangi bir ülke demek olacaktır.

Güvenlik Önlemleri

"GSK Verileri", GSK tarafından veya onun adına sağlanan veya Sözleşmenin görüşülmesi veya imzalanması veya Tedarikçinin Sözleşme kapsamındaki yükümlülüklerinin yerine getirilmesi ile bağlantılı olarak Tedarikçi veya Tedarikçi personeli tarafından elde edilen herhangi bir veri veya bilgi demektir ve şu gibi tüm verileri içerir: (i) Tedarikçinin Sözleşme kapsamındaki yükümlülüklerinin yerine getirilmesi sırasında yaratılan, üretilen, toplanan veya işlenen veriler veya (ii) GSK'nin bilgi sistemlerinde veya Tedarikçi bilgi sistemlerinde bulunan veya bunlar üzerinden erişilen veriler ve ayrıca bunlardan türetilen tüm veriler ve bilgiler.

"**İşleme**", toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, kullanma, aktarım ile açıklama, yayma veya başka türlü sağlama, uygun duruma getirme veya birleştirme, kısıtlama, silme veya imha etme gibi, otomatik yollarla olsun veya olmasın, herhangi bir bilgi veya veri üzerine gerçekleştirilen herhangi bir operasyon veya bir dizi operasyon anlamına gelir.

"Tedarikçi Ortamı", GSK Verilerini almak, muhafaza etmek, İşlemek, depolamak, erişmek veya iletmek için Tedarikçi tarafından veya onun adına kullanılan donanım, yazılım, işletim sistemleri, veri tabanı sistemleri, araçlar ve ağ bileşenleri bileşimi demektir.

"Tedarikçi personeli", Hizmetlerin herhangi bir bölümünü yerine getirmek için Tedarikçi ve onun Taşeronları tarafından görevlendirilen veya istihdam edilen tüm personel demektir.

Bu Güvenlilik Programı GSK ile Tedarikçi arasındaki Sözleşmenin bir bölümünü oluşturur. Bu Güvenlik Programının terimleri ile Sözleşmenin terimleri arasında siber güvenlik bakımından herhangi bir çelişki olması durumunda bu Güvenlik Programı geçerli olacaktır. Bu Güvenlik Programında tanımlanmış olmayan büyük harf ile başlayan terimler onlara Sözleşmenin diğer bölümlerinde verilen anlamlara sahip olacaktır.

1. Sorumluluklar. Tedarikçi: (a) tüm GSK Verilerini üçüncü taraf ağları üzerinden Tedarikçi Ortamının içine veya dışına aktarırken yetkisiz açıklama, erişim veya değiştirmeden korumak için güçlü şifreleme kontrolleri kullanacaktır; (b) virüsten, kötü amaçlı yazılımdan ve casus yazılımdan koruma yazılımlarını düzenli aralıklarla güncelleme dâhil kötü amaçlı yazılımları, virüsleri ve casus yazılımları algılamak, önlemek ve bunlardan kurtarmak için sektördeki en iyi uygulamalarla uyumlu kontrol süreçleri bulunduracaktır; (c) kontrolündeki GSK Verilerine tüm erişimin uygun şekilde yetkili olmasını sağlamak üzere sektördeki en iyi uygulamalarla uyumlu erişim yönetimi politikaları, prosedürleri ve teknik kontrolleri bulunduracaktır.

2. Güvenlik İhlali. Tedarikçi herhangi bir GSK Verisinin doğrulanmış olan kaza sonucu, yetkisiz veya yasa dışı şekilde herhangi bir kullanımını, kaybolmasını, imha olmasını, açıklanmasını, erişilmesini, bozulmasını, değiştirilmesini, satılmasını, kiralanmasını veya başka bir şekilde İşlenmesini (bir "**Güvenlik İhlali**") Tedarikçinin doğrulamasının ardından yirmi dört (24) saat içinde cstd@gsk.com adresinden GSK'ye e-posta ile bildirecektir. Tedarikçi, GSK Verilerini içeren tüm güvenlik vakalarının, uygun vaka müdahale prosedürlerine uygun şekilde yönetilmesini sağlayacaktır Tedarikçi temel nedeni belirlemek ve Güvenlik İhlalini düzeltmek üzere GSK ile iyi niyetli bir şekilde çalışacaktır.

ДОДАТОК

УМОВИ ЗАХИСТУ ДАНИХ. ОСНОВНА ПЕРСОНАЛЬНА ІНФОРМАЦІЯ

Афілійована особа, що підпадає під дію цього додатка, означає кожну Афілійовану особу компанії ГСК, яка отримує вигоду від Послуг як третя сторона (перелік яких компанія ГСК надає на вимогу Постачальника). Афілійована особа — це будь-яка юридична особа, яка (стосовно будь-якої іншої юридичної особи) Контролюється такою іншою юридичною особою, перебуває під спільним контролем із такою юридичною особою або Контролює її. «Контроль» та похідні цього терміну означають володіння (безпосередньо чи опосередковано) більшістю голосуючих акцій такої юридичної особи, можливість (безпосередньо чи опосередковано) призначати більшу частину директорів такої юридичної особи або повноваження керувати діяльністю чи політикою такої юридичної особи в силу договору або іншим чином.

«Законодавство про захист даних» означає: (а) Загальний регламент про захист даних (ЄС) 2016/679 про захист фізичних осіб щодо обробки їхніх персональних даних і вільного переміщення таких даних, і (або) будь-які застосовні закони та (або) нормативно-правові акти, які впроваджують та (або) частково обмежують їх, і (або) заміняють або скасовують їх (**GDPR**); (б) GDPR, що відповідає вимогам Закону Великої Британії про захист даних 2018 року; (в) Закон штату Каліфорнія про захист персональних даних споживачів (ЦК штату Каліфорнія 1798.100 – 1798.199) (**CCPA**); (г) усі інші закони щодо обробки персональних даних.

«Персональна інформація» означає такі персональні дані: ім'я та (або) прізвище, ініціали, робочі контактні дані, членство в групі, ідентифікаційний номер мережі або користувача, дані для входу в обліковий запис, досвід роботи та навички, гендер або форму звертання, присутність працівників компанії ГСК і позаштатних працівників, які користуються Послугами.

«Персональна інформація компанії ГСК» означає будь-яку Персональну інформацію: (i) яка надається компанією ГСК або від імені компанії ГСК Постачальнику (у тому числі, коли Постачальник має доступ до Персональної інформації, що зберігається компанією ГСК або від її імені), або яку Постачальник збирає або створює від імені компанії ГСК; (ii) яка обробляється Постачальником відповідно до цього Договору або у зв'язку з ним; (iii) щодо якої компанія ГСК є розпорядником або власником (або особою з еквівалентними функціями).

«Додаток про безпеку» означає додаток про кібербезпеку*, що додається до цього документа як Додаток № 1*.

Терміни **«контролер», «оцінка впливу на захист даних», «суб'єкт даних», «персональні дані», «порушення захисту персональних даних», «обробник», «обробка», «постачальник»** та **«контролюючий орган**» мають визначення, наведені у відповідному Законодавстві про захист даних. Будь-яке посилання на компанію ГСК означає юридичну особу, що зазначена в Договорі, а також Афілійованих осіб, що підпадають під дію цього додатка.

Умови для обробника

Якщо постачальник діє як обробник Персональної інформації компанії ГСК відповідно до відповідних Законодавства про захист даних, застосовуються такі умови:

1. Кожна сторона дотримуватиметься своїх зобов'язань відповідно до застосовних Законів про захист даних. Компанія ГСК та Постачальник погоджуються, що стосовно Персональної інформації ГСК, яка обробляється відповідно до цього Договору, компанія ГСК буде контролером, а Постачальник буде обробником. Для цілей CCPA Постачальник є постачальником послуг для компанії ГСК, а обробка Персональної інформації ГСК Постачальником здійснюється лише для цілей компанії ГСК відповідно до цього Додатка, і Постачальник не надає компанії ГСК жодної грошової або іншої цінної винагороди, і тому компанія ГСК не продає Персональну інформацію компанії ГСК Постачальнику, як визначено CCPA.

2. Постачальник зобов'язаний дотримуватися наведених далі вимог щодо Персональної інформації компанії ГСК:

a) обробляти Персональну інформацію компанії ГСК лише відповідно до законних письмових вказівок компанії ГСК і виключно з метою надання Послуг Постачальником компанії ГСК відповідно до цього Договору протягом терміну дії Договору, або будь-якого додаткового періоду, зазначеного в Договорі, якщо застосовно;

b) ні Постачальник, ні будь-хто з його працівників, агентів, консультантів або цесіонаріїв не має права обробляти Персональну інформацію компанії ГСК для отримання власної комерційної вигоди в будь-якій формі;

c) вживати відповідних технічних та організаційних заходів безпеки, зокрема заходів, викладених у Додатка про безпеки. посилання у Додатку про безпеку на «дані компанії ГСК» включають Персональну інформацію компанії ГСК;

d) забезпечувати конфіденційність Персональної інформації компанії ГСК відповідно до умов цього Додатка, а посилання у цьому Додатку і Додатку про безпеку на Конфіденційну інформацію компанії ГСК включають Персональну інформацію компанії ГСК;

e) накладати зобов'язання щодо конфіденційності, еквівалентні зобов'язанням, викладеним у Договорі, на відповідний персонал, який має доступ до Персональної інформації компанії ГСК;

f) не залучати іншого обробника («**субобробника**») без попередньої письмової згоди компанії ГСК (і для цих цілей компанія ГСК погоджується з такими категоріями субобробників: постачальники послуг хостингової інфраструктури, використання окремих підрядників і субобробників, які стали відомі компанії ГСК на момент укладання Договору) та передавати Персональну інформацію компанії ГСК таким затвердженим субобробникам лише за письмовим договором, який встановлює зобов'язання, що відповідають положенням, викладеним у цьому Додатку. Коли Постачальник призначає субобробника відповідно до цього пункту 2(f), він залишається відповідальним за дії та бездіяльність субобробника;

g) надавати компанії ГСК обґрунтовану допомогу у: (i) проведенні будь-яких оцінок впливу на захист даних та (або) передачу даних; (ii) дотриманні прав суб'єктів даних; (iii) відповіді на запити будь-якого контролюючого органу щодо Персональної інформації компанії ГСК;

h) негайно повідомляти компанію ГСК, якщо йому стане відомо про порушення безпеки персональних даних, що стосується будь-якої Персональної інформації компанії ГСК, та надавати допомогу компанії ГСК у зв'язку з таким порушенням;

i) негайно повідомляти компанію ГСК, якщо він отримає письмовий запит від: (i) суб'єкта даних щодо здійснення будь-яких його (її) прав стосовно Персональної інформації компанії ГСК відповідно до Законодавства про захист даних; (ii) контролюючого органу щодо обробки Персональної інформації компанії ГСК;

j) якщо інше не передбачено в Договорі, повернути або знищити всю Персональну інформацію компанії ГСК, яка перебуває у його розпорядженні або під його контролем (включно з будь-якою Персональною інформацією компанії ГСК, яка обробляється уповноваженими субобробниками), після припинення або закінчення строку дії Договору;

k) на письмовий запит компанії ГСК надати компанії ГСК достатню інформацію, необхідну для підтвердження дотримання цього Додатку, що може включати будь-які доступні звіти про аудит безпеки третіх сторін.

Умови для контролера

Якщо постачальник діє як контролер Персональної інформації компанії ГСК відповідно до відповідного Законодавства про захист даних, застосовуються такі умови:

1. Кожна сторона діє як незалежний контролер і виконує свої зобов'язання відповідно до чинного Законодавства про захист даних. Компанія ГСК та Постачальник погоджуються з тим, що стосовно персональних даних, які обробляються відповідно до цього Додатка, для цілей CCPA, Постачальник не надає жодної грошової чи іншої цінної винагороди компанії ГСК в обмін на Персональну інформацію компанії ГСК, і тому компанія ГСК не продає Персональну інформацію компанії ГСК Постачальнику, як визначено у CCPA.
2. Якщо Постачальник отримує будь-яке повідомлення від контролюючого органу, яке прямо чи опосередковано пов'язане з а) обробкою Постачальником Персональної інформації компанії ГСК або (б) можливим порушенням Законодавства про захист даних стосовно обробки Персональної інформації компанії ГСК, Постачальник зобов'язаний у межах, дозволених застосовним законодавством, негайно передати інформацію компанії ГСК та надати обґрунтовану співпрацю та допомогу компанії ГСК у зв'язку з цим.
3. Якщо суб'єкт даних подає письмовий запит будь-якій зі сторін щодо здійснення будь-яких його (її) прав відповідно до Законодавства про захист даних щодо Персональної інформації компанії ГСК, сторона, яка отримує запит, повинна відповісти на такий запит відповідно до Законодавства про захист даних. Якщо запит стосується обробки Персональної інформації компанії ГСК, яку проводить інша сторона, сторона, яка отримує запит, зобов'язана: (i) негайно та без невиправданої затримки надіслати запит іншій стороні; (ii) співпрацювати та надавати обґрунтовану допомогу у зв'язку з цим запитом, щоб дати можливість іншій стороні відповісти на нього відповідно до Законодавства про захист даних.
4. Не обмежуючи будь-яке положення Додатка про безпеку, дізнавшись про порушення безпеки персональних даних, що впливають на Персональну інформацію компанії ГСК, Постачальник повинен: (а) негайно повідомити компанію ГСК та надати компанії ГСК обґрунтований опис порушення; (б) не публікувати інформацію щодо порушення без попередньої консультації з компанією ГСК, за винятком того, що він може повідомити про порушення контролюючий орган в обсязі, необхідному відповідно до застосовного Законодавства про захист даних.

Міжнародна передача даних

Якщо компанія ГСК, діючи як експортер даних, передає Персональну інформацію компанії ГСК Постачальнику, діючи як імпортер даних, у спосіб, що становить обмежену міжнародну передачу даних відповідно до чинного Законодавства про захист даних, обидві сторони цим укладають та зобов'язуються дотримуватись застосовних Типових положень, що стосуються відносин між сторонами:

- Додаток до Імплементуючого рішення Комісії щодо стандартних договірних положень про передачу персональних даних до третіх країн відповідно до Регламенту (ЄС) 2016/679 Європейського парламенту та Ради (далі — «**Додаток**») разом із МОДУЛЕМ ОДИН: Передача від контролера до контролера (доступний **тут**), включений у цей документ за допомогою посилання як оновлений, змінений або замінений Європейською комісією; (ii) будь-який відповідний або еквівалентний міжнародний договір про передачу даних або додаток до Типових положень, прийнятих контролюючим органом у Великій Британії (далі — «**Типові положення C2C**»);
- Додаток і МОДУЛЬ ДВА: Передача від контролера до обробника (доступний **тут**), включений у цей документ за допомогою посилання як оновлений, змінений або замінений Європейською комісією; (ii) будь-який відповідний або еквівалентний міжнародний договір про передачу даних або додаток до Типових положень, прийнятих контролюючим органом у Великій Британії (далі — «**Типові положення C2P**»).

«**Типові положення**» означають Додаток разом із Типовими положеннями C2C та Типовими положеннями C2P.

Для цілей Типових положень сторони погоджуються, що:

- Варіант статті 11 «Відновлення у правах» у квадратних дужках не застосовується.
- Варіант один вибирається для пункту 17 «Законодавство, що регулює», і застосовується законодавство Ірландії.

- Суди Ірландії мають юрисдикцію відповідно до статті 18 «Вибір місця розгляду спорів та юрисдикції».

Для цілей застосовних Типових положень C2P та Типових положень C2C, зверніть увагу на таке:

- Додаток № 1 (експортер і імпортер). Компанія ГСК або відповідні одержувачі послуг компанії ГСК, розташовані в ЄС та (або) Великій Британії, згідно з угодою(-ами) з Постачальником є Експортером даних стосовно Персональної інформації компанії ГСК. Постачальник є імпортером даних стосовно Персональної інформації компанії ГСК
- Додаток № 1 (Опис передачі). Див. визначення Персональної інформації та Послуг, які надаватиме імпортер. Жодні конфіденційні дані не передаються. Частота передачі даних є безперервною. Характер діяльності з обробки та цілі передачі визначені в угоді(-ах) із Постачальником. Дані зберігатимуться відповідно до політики зберігання даних Експортера даних.
- Додаток № 1 (Уповноважені органи). Як зазначено в положенні 13 Типових положень C2C та Типових положень C2P.
- Додаток № 2 (Технічні та організаційні заходи). Див. заходи безпеки, викладені нижче.

Сторони погоджуються, що варіант 2 положення 9 «Використання субобробників» Типових положень C-P застосовуватиметься, якщо Постачальник залучатиме субобробника, і Постачальник і Субобробник погоджуються дотримуватися Типових положень **P-P**, а це означає і) Додаток разом із МОДУЛЕМ ТРИ: Передача від обробника до обробника (доступний **тут**), включений у цей документ за допомогою посилання як оновлений, змінений або замінений Європейською комісією; (ii) будь-який відповідний або еквівалентний міжнародний договір про передачу даних або додаток до Типових положень, прийнятих контролюючим органом у Великій Британії.

Якщо Постачальник вважає, що він не може виконати вимоги, які обґрунтовано встановлені компанією ГСК, Постачальник повинен негайно повідомити компанію ГСК про свою неспроможність, а компанія ГСК матиме право припинити Договір.

Сторони погоджуються з тим, що укладені Типові положення діють у країнах за межами Європейської економічної зони, якщо: (i) їхні положення визнаються як належні заходи захисту у зв'язку з міжнародною передачею Персональних даних до країн, що не забезпечують належного захисту; (ii) Законодавство про захист даних вимагає наявності договірних положень для захисту Персональної інформації під час міжнародної передачі. Під час тлумачення Типових положень у цих країнах будь-яке посилання на термін «країна-учасниця, в якій створено експортера даних», буде тлумачитись як країна, в якій засновано юридичну особу ГСК, а будь-яке посилання на Регламент (ЄС) 2016/679 є посиланням на законодавство країни, якщо компанія ГСК створена за межами ЄЕЗ. Будь-яке згадування поняття «Країна, що забезпечує належний захист» означає будь-яку країну, яка, як вважається, забезпечує еквівалентний рівень захисту для цілей застосовного Законодавства про захист даних, у тих країнах за межами Європейської економічної зони, де Типові положення охоплюють передачу Персональних даних.

Заходи безпеки

«Дані компанії ГСК» означають будь-які дані або інформацію, які надаються компанією ГСК або від імені компанії ГСК, чи отримуються Постачальником або Персоналом Постачальника у зв'язку з обговоренням умов і виконанням Договору або виконанням зобов'язань Постачальника за цим Договором, зокрема будь-які дані та інформація, які: (i) створені, згенеровані, зібрані або оброблені Персоналом Постачальника під час виконання зобов'язань Постачальника за цим Договором; (ii) перебувають в інформаційних системах компанії ГСК або інформаційних системах Постачальника або доступ до яких здійснюється через ці системи, а також будь-які дані та інформація, отримані з вищевикладеного.

«**Обробка**» означає будь-яку операцію або набір операцій, які виконуються щодо будь-якої інформації або даних, як-от збирання, реєстрація, упорядкування, структурування, зберігання, адаптування або зміна, отримання, консультування, використання, розкриття шляхом передачі, поширення або іншого надання доступу, узгодження або поєднання, обмеження, видалення або знищення.

«Середовище постачальника» означає поєднання обладнання, програмного забезпечення, операційних систем, систем баз даних, інструментів і мережевих елементів, які використовуються Постачальником або від його імені для отримання, обробки, зберігання, доступу або передачі Даних компанії ГСК.

«Персонал Постачальника» означає будь-який персонал, залучений Постачальником та його Субпідрядниками для виконання будь-якої частини Послуг.

Цей Додаток про безпеку є частиною Договору між компанією ГСК та Постачальником. У разі будь-якого протиріччя щодо кібербезпеки між умовами цього Додатка про безпеку та умовами Договору, цей Додаток про безпеку переважає. Терміни з великої літери, не визначені в цьому Додатку про безпеку, мають значення, визначені для них в інших частинах Договору.

1. Обов'язки. Постачальник зобов'язується: (а) використовувати надійні засоби шифрування відповідно до промислового стандарту для захисту всіх Даних компанії ГСК від несанкціонованого розкриття, доступу або зміни під час передачі в Середовище Постачальника або з нього через сторонні мережі; (б) підтримувати процеси контролю відповідно до найкращих у галузі методів виявлення шкідливих програм, вірусів і шпигунського програмного забезпечення, запобігання їм і відновлення після їх дії, зокрема регулярно оновлювати антивірусні програми, програмне забезпечення для захисту від шкідливих і шпигунських програм; (в) підтримувати політики, процедури та технічні засоби контролю для управління доступом відповідно до передової галузевої практики, щоб увесь доступ до даних компанії ГСК, що перебувають під його контролем, здійснювався після належної авторизації.

2. Порушення безпеки. Постачальник повідомить компанію ГСК електронною поштою на адресу cstd@gsk.com про будь-яке підтверджене випадкове, несанкціоноване або незаконне використання, втрату, знищення, розкриття, доступ, псування, зміну, продаж, оренду або іншу Обробку будь-яких Даних компанії ГСК («**Порушення безпеки**») протягом 24 (двадцяти чотирьох) годин після перевірки Постачальника. Постачальник зобов'язаний забезпечувати управління всіма інцидентами безпеки, пов'язаними з Даними компанії ГСК,

відповідно до належних процедур реагування на інциденти. Постачальник зобов'язаний сумлінно співпрацювати з компанією ГСК для виявлення першопричини та усунення Порушень безпеки.

BẢN PHỤ LỤC

CÁC ĐIỀU KHOẢN BẢO VỆ DỮ LIỆU – THÔNG TIN CÁ NHÂN CƠ BẢN

Đơn vị Liên kết được Bảo hiểm có nghĩa là: mỗi Đơn vị liên kết của GSK có quyền lợi của Dịch vụ với tư cách là bên thứ ba (danh sách quyền lợi sẽ được GSK cung cấp cho Nhà cung cấp theo yêu cầu). Đơn vị liên kết là bất kỳ pháp nhân nào được Kiểm soát bởi, dưới Quyền kiểm soát chung hoặc Kiểm soát bởi pháp nhân tương ứng. "Quyền kiểm soát" và các công cụ phái sinh của nó có nghĩa là quyền sở hữu (trực tiếp hoặc gián tiếp) đối với đa số cổ phần có quyền biểu quyết của pháp nhân đó hoặc là khả năng (trực tiếp hoặc gián tiếp) bổ nhiệm đa số giám đốc của đơn vị đó hoặc quyền chỉ đạo đội ngũ quản lý hoặc các chính sách của pháp nhân đó, theo hợp đồng hoặc theo cách khác;

Luật Bảo vệ Dữ liệu có nghĩa là: (a) Quy định Chung về Bảo vệ Dữ liệu (General Data Protection Regulation, GDPR) (EU) 2016/679 về bảo vệ thể nhân liên quan đến việc xử lý dữ liệu cá nhân và tự do di chuyển dữ liệu đó cũng như bất kỳ luật và/hoặc quy định hiện hành nào mà triển khai và/hoặc thực thi biện pháp khắc phục vi phạm theo đó và/hoặc thay thế luật đó (**GDPR**); và (b) UK GDPR được điều chỉnh bởi Đạo luật Bảo vệ Dữ liệu của Vương quốc Anh năm 2018; (c) Đạo luật về Quyền riêng tư của Người tiêu dùng California năm 2018 (Bộ luật Dân sự California 1798.100 - 1798.199) (California Consumer Privacy Act, **CCPA**); và (d) tất cả các luật khác liên quan đến việc xử lý dữ liệu cá nhân;

Thông tin Cá nhân nghĩa là dữ liệu cá nhân nằm trong tập hợp thông tin sau: tên và/hoặc họ, tên viết tắt, chi tiết liên hệ công việc, tư cách thành viên nhóm, số định danh mạng lưới hoặc người dùng, thông tin đăng nhập, tiểu sử làm việc và kỹ năng , giới tính hoặc chức danh, tình trạng tham dự sự kiện của nhân viên của GSK và người lao động bổ sung sử dụng Dịch vụ

Thông tin Cá nhân GSK có nghĩa là bất kỳ Thông tin Cá nhân nào: (i) được cung cấp bởi hoặc thay mặt GSK cho Nhà cung cấp (bao gồm cả trường hợp Nhà cung cấp có quyền truy cập vào Thông tin Cá nhân do GSK trực tiếp hoặc nhân danh Nhà cung cấp nắm giữ), hoặc Nhà cung cấp thu thập hoặc tạo ra thay mặt GSK; (ii) được xử lý bởi Nhà cung cấp theo hoặc liên quan đến Thỏa thuận này; và (iii) GSK là bên kiểm soát hoặc bên sở hữu (hoặc tương đương);

Bản phụ lục về Bảo mật có nghĩa là *bản phụ lục về an ninh mạng được đính kèm dưới đây như là Phụ lục 1*.

Các thuật ngữ **bên kiểm soát, đánh giá tác động bảo vệ dữ liệu, đối tượng dữ liệu, dữ liệu cá nhân, vi phạm dữ liệu cá nhân, bên xử lý, xử lý, nhà cung cấp dịch vụ** và **cơ quan giám sát** sẽ được xác định theo Luật Bảo vệ Dữ liệu liên quan. Bất kỳ thông tin tham chiếu nào đến GSK sẽ có nghĩa là pháp nhân theo hợp đồng của GSK được sử dụng trong Thỏa thuận, cũng như các Đơn vị liên kết được Bảo hiểm.

Các Điều khoản của Bên xử lý

Trong trường hợp nhà cung cấp đóng vai trò là bên xử lý Thông tin Cá nhân GSK theo Luật Bảo vệ Dữ liệu liên quan, các điều khoản sau sẽ được áp dụng:

1. Mỗi bên sẽ tuân thủ các nghĩa vụ của mình theo Luật Bảo vệ Dữ liệu hiện hành. GSK và Nhà cung cấp đồng ý rằng liên quan đến Thông tin Cá nhân GSK được xử lý theo Thỏa thuận này, GSK sẽ là bên kiểm soát và Nhà cung cấp sẽ là bên xử lý. Đối với các mục đích của CCPA, Nhà cung cấp là nhà cung cấp dịch vụ cho GSK và việc xử lý Thông tin Cá nhân GSK của Nhà cung cấp sẽ chỉ được thực hiện vì các mục đích của GSK theo Bản phụ lục này, và Nhà cung cấp không cung cấp thông tin tài chính hoặc thông tin có giá trị nào khác cho GSK và do đó GSK không bán Thông tin Cá nhân GSK cho Nhà cung cấp như CCPA định nghĩa.

2. Nhà cung cấp phải tuân thủ những điều sau đối với Thông tin Cá nhân GSK:

a) chỉ xử lý Thông tin cá nhân GSK dựa trên các hướng dẫn bằng văn bản hợp pháp của GSK và chỉ vì các mục đích cung cấp Dịch vụ của Nhà cung cấp cho GSK theo Thỏa thuận này trong thời hạn của Thỏa thuận hoặc bất kỳ khoảng thời gian bổ sung nào nêu trong Thỏa thuận, nếu có;

b) Nhà cung cấp cũng như bất kỳ nhân viên, đại lý, chuyên gia tư vấn hoặc người được quyền thừa hưởng nào của Nhà cung cấp đều không có quyền xử lý Thông tin Cá nhân GSK vì lợi ích thương mại của riêng họ dưới bất kỳ hình thức nào;

c) thực hiện và duy trì các biện pháp bảo mật kỹ thuật và tổ chức thích hợp, bao gồm nhưng không giới hạn, các biện pháp được nêu trong Bản phụ lục về Bảo mật. Các thông tin tham chiếu trong Bản phụ lục về Bảo mật tới "Dữ liệu GSK" sẽ bao gồm Thông tin Cá nhân GSK;

d) giữ bí mật Thông tin Cá nhân GSK theo các điều khoản của Bản phụ lục này và các thông tin tham chiếu trong Bản phụ lục này và Bản phụ lục về Bảo mật tới Thông tin Bảo mật của GSK sẽ bao gồm Thông tin Cá nhân GSK;

e) áp đặt các nghĩa vụ về tính bảo mật tương đương với các nghĩa vụ được quy định trong Thỏa thuận về việc các nhân viên liên quan có quyền truy cập vào Thông tin Cá nhân GSK;

f) không thuê một bên xử lý khác ("**bên xử lý phụ**") mà không có sự chấp thuận trước bằng văn bản của GSK (và vì những mục đích này, GSK đồng ý với các danh mục bên xử lý phụ sau: nhà cung cấp dịch vụ cơ sở hạ tầng lưu trữ, sử dụng các nhà thầu riêng lẻ và các bên xử lý phụ được giới thiệu với GSK vào thời điểm Thỏa thuận được ký kết) và chỉ truyền Thông tin Cá nhân GSK cho các bên xử lý phụ đã được phê duyệt như vậy theo một hợp đồng bằng văn bản áp đặt các nghĩa vụ phù hợp với những nghĩa vụ được nêu trong Bản phụ lục này. Khi Nhà cung cấp chỉ định một bên xử lý phụ phù hợp với điều khoản 2(f) này, thì nhà cung cấp vẫn phải chịu trách nhiệm về các hành vi và thiếu sót của bên xử lý phụ;

g) cung cấp sự hỗ trợ hợp lý cho GSK bằng cách (i) thực hiện bất kỳ đánh giá tác động bảo vệ dữ liệu được yêu cầu hợp pháp nào và/hoặc đánh giá tác động truyền dữ liệu; (ii) tuân thủ các quyền của đối tượng dữ liệu; và (iii) phản hồi các yêu cầu từ bất kỳ cơ quan giám sát nào liên quan đến Thông tin Cá nhân GSK;

h) thông báo cho GSK ngay lập tức sau khi biết được vi phạm dữ liệu cá nhân đối với bất kỳ Thông tin Cá nhân GSK nào và cung cấp hỗ trợ cho GSK liên quan đến vi phạm đó;

i) thông báo cho GSK ngay lập tức nếu nhận được yêu cầu bằng văn bản từ (i) chủ thể dữ liệu để thực hiện bất kỳ quyền nào của họ liên quan đến Thông tin Cá nhân GSK theo Luật Bảo vệ Dữ liệu; hoặc (ii) cơ quan giám sát liên quan đến việc xử lý Thông tin Cá nhân GSK;

j) trừ khi có quy định khác trong Thỏa thuận, trả lại hoặc tiêu hủy tất cả Thông tin Cá nhân GSK thuộc quyền sở hữu hoặc nằm dưới sự kiểm soát của họ (bao gồm bất kỳ Thông tin Cá nhân GSK nào do bên xử lý phụ được cho phép xử lý) khi chấm dứt hoặc hết thời hạn Thỏa thuận; và

k) theo yêu cầu bằng văn bản của GSK, cung cấp cho GSK thông tin hợp lý cần thiết để chứng minh sự tuân thủ với Bản phụ lục này, thông tin này có thể bao gồm bất kỳ báo cáo kiểm tra độ an toàn nào có sẵn của bên thứ ba.

Điều khoản Bên kiểm soát

Trong trường hợp nhà cung cấp đóng vai trò là bên kiểm soát Thông tin Cá nhân GSK theo Luật Bảo vệ Dữ liệu liên quan, các điều khoản sau sẽ được áp dụng:

1. Mỗi bên đóng vai trò là bên kiểm soát độc lập và phải tuân thủ các nghĩa vụ của mình theo Luật Bảo vệ Dữ liệu hiện hành. GSK và Nhà cung cấp đồng ý rằng, liên quan đến dữ liệu cá nhân được xử lý theo Bản phụ lục này, vì các mục đích của CCPA, rằng Nhà cung cấp không cung cấp các khoản thanh toán bằng tiền hoặc có giá trị nào khác cho GSK để đổi lấy Thông tin Cá nhân GSK và do đó GSK không bán Thông tin Cá nhân GSK cho Nhà cung cấp theo định nghĩa của CCPA.
2. Nếu Nhà cung cấp nhận được bất kỳ thông tin liên lạc nào từ cơ quan giám sát có liên quan trực tiếp hoặc gián tiếp đến a) Quá trình xử lý Thông tin Cá nhân GSK của Nhà cung cấp; hoặc (b) khả năng không tuân thủ Luật Bảo vệ Dữ liệu liên quan đến việc xử lý Thông tin Cá nhân GSK, Nhà cung cấp, trong phạm vi được luật hiện hành cho phép, nhanh chóng chuyển thông tin liên lạc này đến GSK và cung cấp sự hợp tác và hỗ trợ hợp lý cho GSK về cùng vấn đề này.
3. Nếu một đối tượng dữ liệu đưa ra một văn bản yêu cầu một trong hai bên thực hiện bất kỳ quyền nào của họ theo Luật Bảo vệ Dữ liệu đối với Thông tin Cá nhân GSK, thì bên nhận được yêu cầu sẽ phản hồi yêu cầu đó theo Luật Bảo vệ Dữ liệu. Trong phạm vi yêu cầu liên quan đến việc xử lý Thông tin Cá nhân GSK do bên kia thực hiện, bên nhận được yêu cầu phải: (i) chuyển yêu cầu cho bên kia ngay lập tức và không chậm trễ quá mức; và (ii) hợp tác và cung cấp hỗ trợ hợp lý liên quan đến yêu cầu đó để cho phép bên kia phản hồi theo Luật Bảo vệ Dữ liệu.
4. Không giới hạn bất kỳ điều khoản nào của Bản phụ lục về Bảo mật, khi biết được vi phạm dữ liệu cá nhân ảnh hưởng đến Thông tin Cá nhân GSK, Nhà cung cấp phải (a) thông báo ngay cho GSK và cung cấp cho GSK mô tả hợp lý về vi phạm; và (b) không công bố bất kỳ thông tin nào liên quan đến vi phạm mà không hỏi ý kiến GSK trước, lưu ý rằng Nhà cung cấp có thể thông báo vi phạm cho cơ quan giám sát trong phạm vi yêu cầu của Luật Bảo vệ Dữ liệu hiện hành.

Truyền Dữ liệu Quốc tế

Trong trường hợp GSK, trong vai trò là bên xuất dữ liệu, truyền Thông tin Cá nhân GSK cho Nhà cung cấp, trong vai trò là bên nhập dữ liệu, theo cách cấu thành việc truyền dữ liệu quốc tế bị hạn chế theo Luật Bảo vệ Dữ liệu hiện hành, cả hai bên tham gia và sẽ tuân theo Các điều khoản Mẫu được áp dụng về mối quan hệ giữa các bên:

- Phụ lục của Quyết định Thi hành Mệnh lệnh về các điều khoản hợp đồng tiêu chuẩn đối với việc truyền dữ liệu cá nhân sang các nước thứ ba theo Quy định (EU) 2016/679 của Nghị viện và Hội đồng Châu Âu ("**Phụ lục**") cùng với MODULE MỘT: Truyền dữ liệu từ bên kiểm soát cho bên kiểm soát (có sẵn **tại đây**) và đôi khi được đưa vào tài liệu này theo thông tin tham chiếu như được cập nhật, sửa đổi, thay thế hoặc thế bởi Ủy ban Châu Âu; và/hoặc (ii) bất kỳ thỏa thuận hoặc phụ lục truyền dữ liệu quốc tế tương ứng hoặc tương đương nào đối với Điều khoản Mẫu được cơ quan giám sát tại Vương quốc Anh thông qua ("**Điều khoản Mẫu C2C**");
- Phụ lục cùng với MODULE HAI: Truyền dữ liệu từ bên kiểm soát cho bên xử lý (có sẵn **tại đây**) và đôi khi được đưa vào tài liệu này theo thông tin tham chiếu như được cập nhật, sửa đổi, thay thế hoặc thế bởi Ủy ban Châu Âu; và/hoặc (ii) bất kỳ thỏa thuận hoặc phụ lục truyền dữ liệu quốc tế tương ứng hoặc tương đương nào đối với Điều khoản Mẫu được cơ quan giám sát tại Vương quốc Anh thông qua ("**Điều khoản Mẫu C2P**");

"**Điều khoản Mẫu**" có nghĩa là Phụ lục cùng với Điều khoản Mẫu C2C và Điều khoản Mẫu C2P.

Vì mục đích của Điều khoản Mẫu, các bên đồng ý rằng:

- Không áp dụng tùy chọn trong ngoặc vuông của Khoản 11 "Cải chính"
- Tùy chọn một được chọn cho Điều khoản 17 "Luật Điều chỉnh" và luật pháp Ireland sẽ được áp dụng.

- Các tòa án của Ireland sẽ có quyền tài phán theo Điều khoản 18 "Lựa chọn Tòa án và Quyền tài phán".

Đối với mục đích của Điều khoản Mẫu C2P và Điều khoản Mẫu C2C hiện hành, vui lòng lưu ý những điều sau:

- Phụ lục1 (Bên xuất và Bên nhập): GSK hoặc bên nhận dịch vụ GSK có liên quan ở EU và/hoặc Vương quốc Anh theo (các) thỏa thuận với Nhà cung cấp là Bên xuất Dữ liệu liên quan đến Thông tin Cá nhân GSK. Nhà cung cấp là Bên nhập Dữ liệu liên quan đến Thông tin Cá nhân của GSK
- Phụ lục 1 (Mô tả về Hoạt động truyền): vui lòng xem định nghĩa về Thông tin Cá nhân và Dịch vụ do Bên nhập cung cấp. Không được truyền dữ liệu nhạy cảm. Tần số truyền là liên tục. Bản chất của các hoạt động xử lý và mục đích của hoạt động truyền được quy định trong (các) thỏa thuận với Nhà cung cấp. Dữ liệu sẽ được lưu giữ theo chính sách lưu giữ dữ liệu của Bên xuất Dữ liệu.
- Phụ lục 1 (Cơ quan có Thẩm quyền): như được nêu trong khoản 13 của Điều khoản Mẫu C2C và Điều khoản Mẫu C2P
- Phụ lục 2 (Các biện pháp Tổ chức và Kỹ thuật): vui lòng xem Biện pháp Bảo mật nêu dưới đây

Các bên đồng ý rằng tùy chọn 2 của khoản 9 "Sử dụng Bên xử lý phụ" của Điều khoản Mẫu CP sẽ được áp dụng khi Nhà cung cấp thuê bên xử lý phụ và Nhà cung cấp và bên xử lý phụ sẽ đồng ý tuân theo **Điều khoản mẫu P-P**, có nghĩa là i), Phụ lục cùng với MODULE BA: Truyền dữ liệu từ bên xử lý cho bên xử lý (có sẵn **tại đây**) và đôi khi được đưa vào tài liệu này theo thông tin tham chiếu như được cập nhật, sửa đổi, thay thế hoặc thế bởi Ủy ban Châu Âu; và/hoặc (ii) bất kỳ thỏa thuận hoặc phụ lục truyền dữ liệu quốc tế tương ứng hoặc tương đương nào đối với Điều khoản Mẫu được cơ quan giám sát tại Vương quốc Anh thông qua;

Trong trường hợp Nhà cung cấp không cho rằng mình có thể đáp ứng các yêu cầu do GSK đưa ra một cách hợp lý, Nhà cung cấp phải thông báo cho GSK ngay lập tức về tình trạng không đủ khả năng của mình và GSK sẽ có quyền chấm dứt Thỏa thuận.

Các bên đồng ý rằng các Điều khoản Mẫu được ký kết sẽ có hiệu lực ở các quốc gia bên ngoài Khu vực Kinh tế Châu Âu, nơi: (i) các điều khoản của Các bên được công nhận là biện pháp bảo vệ thích hợp liên quan đến hoạt động truyền Dữ liệu Cá nhân quốc tế tới các quốc gia không thỏa đáng hoặc (ii) Luật Bảo vệ Dữ liệu yêu cầu có các điều khoản hợp đồng để bảo vệ việc truyền Thông tin Cá nhân quốc tế. Khi giải thích các Điều khoản Mẫu, ở những quốc gia đó, bất kỳ thông tin tham chiếu nào đến thuật ngữ "Quốc gia Thành viên mà bên xuất dữ liệu được thành lập" sẽ được hiểu là quốc gia mà tổ chức GSK được thành lập; và mọi thông tin tham chiếu đến Quy định (EU) 2016/679 phải tuân theo luật của quốc gia nơi GSK được thành lập bên ngoài EEA. Bất kỳ thông tin tham chiếu nào đến "Quốc gia Thỏa đáng" sẽ có nghĩa là bất kỳ quốc gia nào đã quyết định cung cấp, hoặc cung cấp, mức độ bảo vệ tương đương vì các mục đích của Luật Bảo vệ Dữ liệu hiện hành, ở những quốc gia bên ngoài Khu vực kinh tế Châu Âu nơi Điều khoản Mẫu sẽ bao gồm hoạt động truyền Dữ liệu Cá nhân.

Biện pháp Bảo mật

"Dữ liệu GSK" có nghĩa là bất kỳ dữ liệu hoặc thông tin nào được cung cấp bởi hoặc thay mặt cho SK hoặc được Nhà cung cấp hoặc Nhân viên của Nhà cung cấp có được liên quan đến việc đàm phán và thực hiện Thỏa thuận hoặc việc thực hiện các điều khoản của Nhà cung cấp theo Thỏa thuận, bao gồm bất kỳ dữ liệu và thông tin nào như vậy mà: (i) do Nhân viên của Nhà cung cấp tạo ra ra, đưa ra, thu thập hoặc xử lý để thực hiện nghĩa vụ của Nhà cung cấp theo Thỏa thuận, hoặc (ii) nằm ở trong hoặc được truy cập thông qua hệ thống thông tin của GSK hoặc hệ thống thông tin của Nhà cung cấp, cũng như bất kỳ dữ liệu nào và thông tin thu được từ việc đã đề cập trước đó.

"**Xử lý**" có nghĩa là bất kỳ thao tác hoặc nhóm thao tác nào được thực hiện trên bất kỳ thông tin hoặc dữ liệu nào, dù có hay không bằng phương tiện tự động, chẳng hạn như thu thập, ghi chép, tổ chức, cấu trúc, lưu trữ, điều chỉnh hoặc thay đổi, truy xuất, tham vấn, sử dụng, tiết lộ bằng hình thức truyền tải, phổ biến hoặc cung cấp sẵn, liên kết hoặc kết hợp, hạn chế, tẩy xóa hoặc phá hủy.

"Môi trường Nhà cung cấp" có nghĩa là sự kết hợp của phần cứng, phần mềm, hệ điều hành, hệ thống cơ sở dữ liệu, công cụ và các thành phần mạng được sử dụng bởi hoặc thay mặt cho Nhà cung cấp để nhận, duy trì, xử lý, lưu trữ, truy cập hoặc truyền Dữ liệu GSK.

"Nhân sự Nhà cung cấp" có nghĩa là bất kỳ và tất cả nhân sự do Nhà cung cấp và các Nhà thầu phụ của Nhà cung cấp tham gia hoặc được thuê để thực hiện bất kỳ phần nào của Dịch vụ.

Bản phụ lục Bảo mật này là một phần của Thỏa thuận giữa GSK và Nhà cung cấp. Trong trường hợp có bất kỳ xung đột nào liên quan đến an ninh mạng giữa các điều khoản của Bản phụ lục Bảo mật này và các điều khoản của Thỏa thuận, thì Bản phụ lục Bảo mật này sẽ có hiệu lực ưu tiên. Các thuật ngữ viết hoa không được định nghĩa trong Bản phụ lục Bảo mật này sẽ có nghĩa như được nêu trong các phần khác của Thỏa thuận.

1. Trách nhiệm. Nhà cung cấp phải: (a) sử dụng các biện pháp kiểm soát mã hóa mạnh để bảo vệ tất cả Dữ liệu của GSK khỏi bị tiết lộ, truy cập hoặc thay đổi trái phép khi chuyển vào hoặc ra khỏi Môi trường của Nhà cung cấp qua mạng của bên thứ ba; (b) duy trì các quy trình kiểm soát phù hợp với thông lệ tốt nhất trong ngành để phát hiện, ngăn chặn và khôi phục trước phần mềm độc hại, vi rút và phần mềm gián điệp, bao gồm cập nhật phần mềm chống vi rút, phần mềm chống phần mềm độc hại và phần mềm chống phần mềm gián điệp theo định kỳ; (c) duy trì các chính sách, thủ tục và biện pháp kiểm soát kỹ thuật về quản lý truy cập phù hợp với thông lệ tốt nhất trong ngành để đảm bảo tất cả quyền truy cập vào Dữ liệu GSK trong phạm vi kiểm soát của họ đều được ủy quyền thích hợp.

2. Vi phạm Bảo mật. Nhà cung cấp sẽ báo cáo cho GSK bằng email đến địa chỉ cstd@gsk.com bất kỳ việc sử dụng ngẫu nhiên, trái phép hoặc bất hợp pháp nào đã được xác minh, mất mát, phá hủy, tiết lộ, truy cập, sai hỏng, sửa đổi, bán, cho thuê hoặc các Quá trình Xử lý bất kỳ Dữ liệu GSK nào ("**Vi phạm Bảo mật**") trong vòng hai mươi bốn (24) giờ kể từ khi Nhà cung cấp xác minh. Nhà cung cấp sẽ đảm bảo rằng tất

cả các sự cố bảo mật liên quan đến Dữ liệu của GSK được quản lý theo các quy trình ứng phó sự cố thích hợp, Nhà cung cấp phải làm việc thiện chí với GSK để xác định nguyên nhân gốc rễ và khắc phục Vi phạm Bảo mật.