**DATA PROCESSING ADDENDUM**

**REVISION DATE: October 23, 2024**

For the purposes of this Data Processing Addendum (“DPA”), the Merck Sharp & Dohme LLC (Rahway, NJ, USA) entity or affiliate executing the contract or other form of agreement referencing this DPA (the “Agreement”) shall be referred to as “Company” and all other parties to such Agreement shall be collectively referred to as “Supplier”. Company and Supplier are each a “Party” and together the “Parties.”

Background

1. The Parties entered into the Agreement, and along with the Agreement may enter into one or more purchase or task orders, project agreements, project plan addenda, statements of work, work orders or other service terms (each a “Statement of Work”), governing the services contemplated therein (the “Services”).
2. The Parties wish to supplement the terms of the Agreement to ensure all Processing of Personal Information in connection with the Agreement is performed in compliance with Data Protection Law.

The Parties agree:

1. *Data Processing Activities*. In relation to Personal Information Processed in connection with the Agreement, the subject-matter, nature, purpose and duration of the Processing, the categories of Data Subjects concerned, and the categories of Personal Information are specified in the exhibit to the Agreement titled “Data Processing Details”.
2. *Applicability*. The terms of this DPA apply to every Statement of Work under the Agreement unless otherwise specified in that Statement of Work.
3. *Supplier Obligations*. When Processing Personal Information on behalf of Company in connection with the Agreement, Supplier shall:
	1. comply with all applicable Data Protection Law and Supplier’s obligations under this DPA, and in the event Supplier cannot meet these obligations, Supplier shall notify Company immediately and take all reasonable and appropriate actions Company deems necessary to remedy the noncompliance.
	2. only Process Personal Information on Company’s documented instructions, including Supplier performing its obligations under, and in accordance with, the Agreement and this DPA, unless required otherwise by applicable law. In that case, Supplier shall inform Company of the corresponding legal requirement before commencing the Processing, unless prohibited by applicable law and shall use its best efforts to limit the nature and scope of any required disclosure and shall only disclose the minimum amount of Personal Information necessary to comply with applicable law.
	3. only Process Personal Information to the minimum extent necessary to perform the Services, which includes a prohibition on combining Personal Information with any other data unless expressly permitted in writing by Company.
	4. immediately inform Company if Supplier is of the opinion that an instruction of Company regarding Processing Personal Information infringes Data Protection Law.
	5. ensure that Supplier’s personnel who have access to Personal Information (i) require access to the Personal Information to perform the Services, (ii) only Process the Personal Information as permitted under this DPA, and (iii) are subject to obligations at least as protective of Personal Information as Supplier’s obligations under this DPA and the Agreement.
	6. not disclose or transfer Personal Information to any third party or otherwise engage any agent or subcontractor in any Processing in connection with the Agreement (each such agent or subcontractor a “Subprocessor”) unless Company has provided its prior written consent. A current list of Subprocessors for which Company has given its prior written consent as of the date of this DPA is specified in the exhibit to the Agreement titled “Data Processing Details”. In addition, when engaging a Subprocessor:
		1. the disclosure or transfer must be reasonably necessary to perform the Services under the Agreement,
		2. Supplier must carry out reasonable due diligence to ensure the Subprocessor is capable of providing the level of protection of Personal Information required under this DPA and the Agreement, and
		3. the Subprocessor must enter into a written agreement with terms at least as protective of Personal Information as the obligations set out in this DPA and the Agreement.
	7. not sell, share, retain, use, or disclose Personal Information other than to provide the Services as specified in the Agreement or as otherwise authorized under this DPA.
	8. be fully liable for all acts or omissions of its employees, affiliates, agents, subcontractors, and other representatives.
	9. implement and maintain reasonable and appropriate written information security and privacy programs, which programs shall incorporate physical, technical and organizational measures that are commensurate with the nature of Personal Information Processed in connection with the Agreement, that meet or exceed good industry practices (or such higher standard as may be required in Appendix 1) and that reasonably protect against a Personal Data Breach, including training of all personnel responsible for Processing Personal Information in a manner sufficient to meet the requirements of this DPA, such measures described in Appendix 1 and to the extent not otherwise addressed in Appendix 1 and as appropriate:
		1. the pseudonymisation and encryption of Personal Information;
		2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
		3. the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident;
		4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and
		5. the ability to confirm within 72 hours of detection whether an event constitutes a Personal Data Breach.
	10. in the event of an actual or reasonably suspected Personal Data Breach of Personal Information within the custody or control of Supplier or resulting from the acts or omissions of Supplier (a “Supplier Personal Data Breach”), Supplier shall:
		1. notify Company without undue delay (and in any event within 72 hours of becoming aware of a Supplier Personal Data Breach);
		2. undertake an appropriate investigation and all remediation efforts necessary to rectify and prevent a recurrence of such Supplier Personal Data Breach in a manner satisfactory to Company;
		3. promptly provide Company with all information Company reasonably deems necessary to enable Company to comply with Data Protection Law, including with respect to record keeping and reporting, and all other information Company may reasonably request regarding a Supplier Personal Data Breach;
		4. provide notification to all Data Subjects whose Personal Information may have been affected, with content required under Data Protection Law and satisfactory to Company, or provide Company with all assistance and information necessary to enable Company to provide notification to all Data Subjects whose Personal information may have been affected, as Company deems appropriate;
		5. bear sole responsibility for the costs and expenses of either Party for any such notification to Data Subjects, whether the notice was given by Supplier or Company, unless Company acted unreasonably in providing notice or requesting Supplier provide notice; and
		6. except for Supplier’s attorneys, consultants, insurers, and other affected third parties for which Supplier provides services, Supplier may not provide any third parties with any information regarding a Supplier Personal Data Breach prior to informing Company, unless otherwise required by applicable law.
		7. For the avoidance of doubt and to the extent permitted by law, the obligations under this Section 3(j) also apply to Personal Information Processed by any of Supplier’s affiliates or Supplier’s or any of its affiliates’ Subprocessors or other agents, subcontractors, or representatives.
	11. promptly notify Company without undue delay and in any event within 72 hours of:
		1. any complaint, inquiry, request or concern by a competent data protection or other regulatory authority relating to Personal Information that Supplier Processes in connection with the Agreement, and assist Company for answering those demands; and
		2. any complaint, inquiry, request, or concern by a Data Subject relating to the Personal Information that Supplier Processes in connection with the Agreement, including any request to exercise rights under Data Protection Law or Company’s or Supplier’s privacy policy, such as to access (including requesting information on any processing of their Personal Information), rectify, amend, correct, share, delete or cease Processing his or her Personal Information.
	12. comply with all reasonable and appropriate measures requested by Company necessary for Supplier and Company to comply with their respective obligations under Data Protection Law and this DPA, including without limitation, if necessary, aiding in the completion of any data protection impact assessment or privacy impact assessment required by Data Protection Law.
	13. on Company’s request or at the expiration or earlier termination of the Agreement or a Statement of Work in connection with which the Personal Information is Processed, promptly delete or return, at Company’s option, all Personal Information Processed, unless required otherwise by applicable law. In that case, Supplier may retain one copy of the Personal Information required to be retained under applicable law, until thirty (30) days after that period for retaining Personal Information required under applicable law ends, and Supplier will continue to comply with this DPA with respect to any Personal Information Supplier retains and will only Process that Personal Information as required by that applicable law. Supplier shall delete or return the Personal Information by such means and, in the case of returning Personal Information, in such format, as Company reasonably requests.
	14. maintain the accuracy and integrity of Personal Information that it Processes on behalf of Company, consistent with the form in which Supplier received or collected such Personal Information.
	15. maintain all records necessary to be able to demonstrate that Personal Information was only Processed in accordance with applicable notices, consents, authorizations, and rights and as permitted under this DPA and otherwise as necessary for the Parties to comply with Data Protection Law.
	16. upon Company’s request, allow for and contribute to audits by Company or another auditor mandated by Company of Supplier’s compliance with this DPA and of Supplier’s privacy and information security programs, and have a third-party auditor conduct an audit of Supplier’s privacy and information security programs. Such audits shall be subject to any reasonably applicable audit restrictions and requirements detailed in the Agreement, except to the extent such restrictions would prevent any audits, assessments, or reviews required by Data Protection Law.
	17. to the extent Supplier is to Process Personal Information regarding Data Subjects of any country or region with restrictions on the cross-border transfer of Personal Information, Supplier shall only do so in compliance with all applicable Data Protection Law, which may include without limitation entering into the Standard Contractual Clauses or similar mechanisms intended to protect transfers of Personal Information.
	18. upon Company’s request and in accordance with the terms of the Agreement, provide notice to, and obtain a consent from, any Data Subject whose Personal Information is collected by or on behalf of Supplier in connection with the Agreement. Supplier will use forms of notice and consent and provide and obtain any such notice and consent in a manner and at the times, that are satisfactory to Company and meet the requirements of Data Protection Law.
	19. except for changes made consistent with meeting a higher industry standard or Data Protection Law, Supplier shall maintain in effect and consistently apply Supplier’s privacy and data security practices disclosed to Company in connection with any due diligence Company most recently conducted on those practices in connection with the Agreement; provided that Supplier may not reduce the standards in those practices by subsequently disclosing privacy and data security practices that would be a degradation of the previously disclosed practices. Supplier represents and warrants that all responses provided by Supplier in any such due diligence are true, accurate, and complete when made, and that an authorized representative of Supplier completed such due diligence. Supplier shall promptly notify Company of all material changes to Supplier’s privacy and data security practices.
	20. if required by Data Protection Law, appoint a Data Protection Officer or similar role charged with the protection of Personal Information and inform Company of that person’s name and contact information.
	21. Supplier acknowledges and agrees that its execution of this DPA constitutes its certification that it understands the restrictions set forth in this DPA and will comply with them.
4. *Indemnification*. Without limiting any of Company’s rights or entitlements, or Supplier’s obligations under the Agreement or otherwise, the Parties agree that Supplier will indemnify Company and its affiliates and their respective officers, directors, employees, contractors, temporary workers, subcontractors, agents and other representatives (each an “Indemnified Party”) for any losses, damages, fines, costs, or expenses (including legal expenses and disbursements) incurred by that Indemnified Party resulting from a Supplier Personal Data Breach in relation to Personal Information Processed by Supplier in connection with the Agreement. Any liability under this section shall be subject to applicable limitations or exclusions of liability in the Agreement, unless such liability is the result of Supplier’s negligence or intentional wrong act, in which case no limitations or exclusions shall apply.
5. *Definitions*
	1. “Data Protection Law” means any applicable data protection, data security or privacy law, including the EU General Data Protection Regulation and any national implementing legislation relating thereto, the Health Insurance Portability and Accountability Act, the California Privacy Rights Act, and any other national, state, federal, provincial, or regional data protection, data security or privacy laws.
	2. “Personal Information” means any data connected to the Agreement relating to an identified or identifiable individual, including data that identifies an individual or that could be used to identify, locate, track, or contact an individual. Personal Information includes both directly identifiable information, such as a name, identification number or unique job title, and indirectly identifiable information such as date of birth, unique mobile or wearable device identifier, information that could be used to identify a household, telephone number, key-coded data, online identifiers, such as IP addresses, or personal activities, behavior or preferences, and includes any data that constitutes “personal data” under Data Protection Law.
	3. “Process” means to perform any operation or set of operations on Personal Information or sets of Personal Information, whether by automated means, such as collection, recording, organization, structuring, storage, access, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, evaluation, analysis, reporting, sharing, alignment or combination, restriction, erasure, or destruction.
	4. “Personal Data Breach” means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, use, or access to Personal Information, transmitted, stored, or otherwise Processed.
	5. “Standard Contractual Clauses” means the standard contractual clauses for the transfer of Personal Information to third countries that have not been assessed by the European Commission as providing an adequate level of protection for Personal Information, as published by the European Commission on June 4, 2021, as may be updated from time to time, or any similar transfer instrument issued required for the export of Personal Information beyond national boundaries issued by other national or federal governments.
	6. In the event these definitions restrict or reduce the scope of related definitions under Data Protection Law, then the definition shall be expanded to match the definition under that Data Protection Law.
	7. In the absence of a definition under this Section, a term shall be interpreted in a manner compliant with all applicable Data Protection Laws.
6. *Interpretation*.
	1. Defined terms used in this DPA but not defined herein shall have the meaning specified elsewhere in this Agreement.
	2. In performing their obligations under the Service Agreement and this DPA, the Parties acknowledge that the corporate policy of MSD and its Affiliates requires that MSD’s business be conducted within the letter and spirit of any applicable Data Protection Law, which includes the EU General Data Protection Regulation. In the event both Parties are not subject to the same Data Protection Laws, it is the expectation that both Parties abide by all reasonably relevant data protection standards contained in any such laws.
	3. The words "include" and “including” shall be construed to mean including without limitation.
	4. In connection with the Services under the Agreement, Supplier may Process Personal Information of one or more of Company’s affiliates. In such event, any of those Company affiliates shall be considered a “Controller” of Personal Information and a third-party beneficiary of this DPA and entitled to rely upon and enforce all rights and protections afforded Company under this DPA, regardless of whether that affiliate is named as a party to the Agreement or this DPA.
	5. This DPA is hereby incorporated into and forms part of the Agreement.
	6. In the event and to the extent of any conflict between the terms of the Agreement and this DPA, the terms of this DPA will prevail, except if the terms of the Agreement are more protective of Personal Information Processed in connection with the Agreement, in which case the more protective terms of that Agreement will prevail.
	7. In the event and to the extent of any conflict between the terms of this DPA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.
	8. Except as expressly amended herein, the terms of the Agreement will remain in full force and effect.
	9. If this DPA is drafted in English and a foreign language, in the case of differences between the text in English and the text in the foreign language, the text in English shall prevail.
	10. Section and other headings in this DPA are for convenience of reference only and shall not constitute a part of or otherwise affect the meaning or interpretation of this DPA.
	11. Annexes and appendices to this DPA shall be deemed to be an integral part of this DPA to the same extent as if they had been set forth verbatim in this DPA.
	12. The provisions of this DPA are severable. If any phrase, clause, or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.
	13. This DPA governs any Processing of Personal Information in connection with the Services and supplements the terms of the Agreement applicable to the Services, except where Company and Supplier have entered into another DPA applicable to certain of the Services.
	14. This DPA may be entered into in any number of counterparts, all of which together will constitute one and the same agreement. Any Party may enter into this DPA by executing such counterpart.
	15. This DPA constitutes the entire agreement between the Parties with respect to the subject of this DPA and (to the extent permissible by law) supersedes all prior representations or oral or written agreements between the Parties with respect to that subject matter, provided nothing in this DPA and neither Party is attempting to exclude any liability for fraudulent statements.
	16. The governing law and jurisdiction provisions of the Agreement will apply to this DPA.
7. *Limits on Updates*
	1. When the Parties renew, amend, issue a new Statement of Work under, or in any way modify the Agreement or any Statement of Work under the Agreement (a “Triggering Event”), the most recent document under “Data Processing Addendum” located at <https://www.msdprivacy.com/privacyterms/> will supersede and replace the terms of this DPA until the next Triggering Event unless an objection is lodged within 30 days of the triggering event's occurrence. Notwithstanding the foregoing, there may be situations requiring immediate amendment to the terms of this DPA, which shall only occur for reasons articulated in 7(b), and shall only be made in good faith and after ensuring any new or modified terms are limited to those necessary to comply with new applicable Data Protection Law, case law, or guidance issued by relevant data protection authorities.
	2. In the event any of the following scenarios occur, the Parties immediately agree to the newest terms posted at the above address, unless an objection is lodged within 30 days upon Company’s notice of new terms provided to all entities that have requested to receive notice at privacy\_updates@msd.com:
		1. applicable Data Protection Law has been updated in a manner where the existing contractual terms of this DPA are inadequate to satisfy the requirements of the updated law,
		2. there is a change in applicable Data Protection Law and the Parties have a reasonable and legitimate interest in amending these terms due to the change in law, for instance and without limitation, in removing requirements that are no longer necessary, or
		3. there is new case law or guidance issued by relevant data protection authorities that has a comparable effect to a change in law described in (i) or (ii) above.
8. *Applicability of Appendices.* The Standard Contractual Clauses attached hereto as Appendix 2 and the addenda in Appendix 3 shall apply only to the extent that they are required by applicable Data Protection Law. The Parties agree to comply with such clauses and addenda solely insofar as they align with and are necessitated by the requirements of the applicable Data Protection Law in each respective jurisdiction.
9. *Notice*. Notices given under this DPA (each a “Notice”) shall be in writing. Notices given under this DPA shall be given in accordance with the notice provisions of the applicable Agreement, together with copy(ies) sent to the Company by email, to msd\_privacy\_office@msd.com, marked with a subject line of “DPA Notice from Supplier” or in the case of a Personal Data Breach “Urgent: Personal Data Breach Notice”.

**APPENDIX 1 – Information Technology Security Measures**

1. **Definitions –** When used in this Exhibit, each of the following defined terms will have the definition given below for that term. Defined terms used in this Exhibit but not defined herein shall have the meaning specified elsewhere in the Agreement.
	1. “Company Information” means any information of Company or any of Company’s Affiliates or their respective suppliers, customers or other business partners provided to, obtained by, created or generated by or otherwise processed by Supplier or any of Supplier’s third-party service providers in connection with any of the Services and any other information to be treated as confidential under the Agreement.
	2. “Data Breach” means an accidental or unauthorized destruction, loss, alteration, use, transmission or disclosure of or access to any Company Information.
	3. “Endpoint” means any computer, including any laptop or desktop, mobile device, lab equipment, server or other device on Supplier Systems, including any hosted at an external third-party site (e.g., cloud provider).
	4. “Notification Event” means any event, including a Data Breach, that requires the notification of individuals or entities under any Laws.
	5. “Security Event” means any A) Data Breach, (B) Notification Event, (C) unauthorized access to or interference with the operations of Supplier Systems or (D) breach of Supplier’s security obligations under this Exhibit, the Agreement or any Laws.
	6. “Subject Software” means any software provided or used in connection with any of the Services, including any software delivered to, or installed on any computer, including any laptop or desktop, mobile device, lab equipment, server, other device or other component of, or connected to, the information systems of, Company or any of Company’s Affiliates.
	7. “Supplier Systems” means Supplier’s networks and all systems, including Subject Software, (A) provided or used in connection with any of the Services, (B) on which any Company Information or deliverables or work in progress for Company or its Affiliates, is stored or otherwise processed or from which they are accessed, (C) connected to Company’s or its Affiliates’ information, network or other systems or from which Company’s or its Affiliates’ information, network or other systems may be accessed, or (D) to which any of the foregoing may be connected or from which any of the foregoing may be accessed.
2. **Network Security -** Supplier shall maintain network security policies, procedures and controls and shall perform network security activities, consistent with best practices in Supplier’s industry, but that at a minimum include network firewall provisioning, intrusion detection and prevention controls, distributed denial-of-service attack (DDoS) protection controls and vulnerability assessments and penetration tests conducted regularly, in accordance with best practices in Supplier’s industry (but no less frequently than annually). In no event shall any of Supplier’s network security policies, procedures or controls applied to the protection of Company Information and Supplier Systems be any less stringent and protective than those applied by Supplier to the protection of its own information and its other systems of a similar nature.
3. **Application Security** - Based on the nature of services provided, if applicable, Supplier shall have software development lifecycle processes and controls (“SDLC Process”) governing the development of and changes to any Supplier Software, including updates, upgrades, patches, enhancements, bug fixes, modifications, improvements, corrections, revisions, releases and other changes. The SDLC Process shall, at a minimum, include recognized and comparable industry standards secure software development practices. Supplier shall follow a patch management process that ensures Supplier Information Systems are up to date with appropriate security and functionality. Supplier shall timely, commensurate with the risk, and within the timeframes provided in Supplier Policies and Procedures, remediate and retest any identified vulnerability.
4. **Data Security** -Based on the nature of services provided, if applicable, Supplier shall handle, store, and otherwise process Company Information, in accordance with recognized and comparable industry practices and standards, such as those set forth in paragraph 11 (including PCI DSS, as applicable) and in accordance with all Laws. Supplier shall establish and maintain reasonable safeguards against a Data Breach. In addition to and without limiting any other of Supplier’s obligations, Supplier shall store all Company Information in accordance with best practices in Supplier’s industry and in compliance with all Laws, and shall use security measures that meet best practices in Supplier’s industry, including encryption and firewalls, to protect Company Information from a Data Breach. When Supplier stores Company Information in an offsite facility, Supplier must have complied with all terms in the Agreement or in any agreement executed in connection with the Agreement, related to disclosing Company Information to third parties or otherwise engaging third parties to provide or assist in providing products or services, and Supplier shall use an offsite storage facility reasonably acceptable to Company that shall, without limiting the foregoing, be in full compliance with all of the provisions of this Exhibit. In addition, the provider of such offsite storage facility must be bound by a written confidentiality agreement between Supplier and such provider, which contains terms no less strict than those in the Agreement or any agreement executed in connection with the Agreement and which protects all Company Information stored therein.
5. **Data Storage** - Based on the nature of services provided, if applicable, any and all Company Information will be handled, stored and otherwise processed solely on designated Supplier computing and storage resources. Company Information will only be handled, stored or otherwise processed on or transferred to a laptop or mobile device, if(A) it is a laptop or mobile device of Supplier, (B) Supplier encrypts all Company Information on that laptop or mobile device in accordance with the encryption standards in paragraph 7 below and (C) that laptop or mobile device is subject to Endpoint controls consistent with recognized and comparable industry practices and standards, such as those set forth in paragraph 11. Company Information will not be handled, stored or otherwise processed on a portable device, except as provided in the sentence immediately above. Supplier shall store all backups of Company Information as part of its designated backup and recovery processes, and such backups of Company Information must be encrypted in accordance with this Exhibit, including the requirements of this paragraph 5 and paragraph 7 below.
6. **Data Transmission** - Based on the nature of services provided, if applicable, any electronic transmission or exchange of Company Information shall take place via secure means (using HTTPS or SFTP or equivalent) that are consistent with recognized and comparable industry practices and standards, such as those set forth in paragraph 11, and solely in accordance with paragraph 7 below.
7. **Data Encryption** - Based on the nature of services provided, if applicable, in addition to and without limiting any other of Supplier’s obligations, Supplier agrees that any Company Information comprised of Personal Information subject to protection under any Law or comprised of information subject to protection under the then-current Payment Card Industry Data Protection Standard, including all Company backup data, shall be kept in encrypted form, using a commercially supported encryption solution. Supplier agrees encryption solutions shall be deployed that encrypt Company Information in accordance with recognized and comparable industry practices and standards, such as those set forth in paragraph 11, but with no less than a 128-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption.
8. **Data Re-Use** - Based on the nature of services provided, if applicable, Supplier shall use any and all Company Information solely for purposes of performing the Services. Supplier shall not distribute, repurpose or share across other applications, environments or business units of Supplier any Company Information.
9. **End of Agreement Data Handling** - Based on the nature of services provided, if applicable, In addition to and without limiting any other of Supplier’s obligations, upon Company’s request and except as otherwise provided in the Agreement, upon the expiration or earlier termination of the Agreement, all Company Information in the possession or control of Supplier or any of Supplier’s affiliates, subcontractors, service providers, agents or other consultants shall be destroyed or returned, as Company elects.
10. **Security Breach Notification** - In addition to and without limiting any other of Supplier’s obligations, Supplier shall notify Company of an actual or reasonably suspected Security Event within 24 hours of becoming aware of such actual or reasonably suspected Security Event. Supplier shall notify Company of such actual or reasonably suspected Security Event by contacting Company’s Security team by telephone (+1-704-345-6700 – Choose Option 1) and e-mail Global Operations Center globalopscnt@merck.com. Supplier will provide information and assistance Company may reasonably request regarding a Security Event, including root cause information.
11. **Industry Standards** - Generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by the following:
	1. Center for Internet Security - see <http://www.cisecurity.org>
	2. Payment Card Industry / Data Security Standards (PCI/DSS) – see <http://www.pcisecuritystandards.org/>
	3. National Institute for Standards and Technology - see <http://csrc.nist.gov>
	4. Federal Information Security Management Act (FISMA) - see <http://csrc.nist.gov>
	5. ISO/IEC 27000-series - see <http://www.iso27001security.com/>
	6. Organization for the Advancement of Structured Information Standards (OASIS) – see <http://www.oasis-open.org/>
	7. The Open Web Application Security Project’s (OWASP) – see <http://www.owasp.org>
	8. The CWE (Common Weakness Enumeration) – see <http://cwe.mitre.org> or CWE/SANS Top 25 Programming Errors - <http://cwe.mitre.org/top25/>
	9. The SANS Institute- see <http://www.sans.org>
	10. Most Dangerous Software Errors <http://www.sans.org/top25-programming-errors/>

Upon Company’s reasonable request, Supplier shall permit Company to audit Supplier’s compliance with the requirements listed above. Supplier shall correct any failures to comply with the requirements, as soon as reasonably possible.

**APPENDIX 2**

In the event Company is exporting Personal Information in a manner that requires Module 2 of the EU Standard Contractual Clauses, the following terms apply:

*The body text of Module 2 (Controller to Processor) of the Standard Contractual Clauses attached to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are hereby incorporated by reference. Optional aspects are described below:*

1. *Clause 7 (docking clause) is omitted.*
2. *For Clause 9, Option 1: Specific Prior Authorization is chosen.*
3. *For Clause 11, the optional text is omitted.*
4. *For Clause 17, Option 1 is chosen, with the member state being the Netherlands.*
5. *For Clause 18, the choice of forum is the Netherlands.*

In the event Supplier is exporting Personal Information in a manner that requires Module 4 of the EU Standard Contractual Clauses, the following terms apply:

*The body text of Module 4 (Processor to Controller) of the Standard Contractual Clauses attached to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are hereby incorporated by reference. Optional aspects are described below:*

*Clause 7 (docking clause) is omitted.*

*For Clause 17, Option 1 is chosen, with the member state being the Netherlands.*

*For Clause 18, the choice of forum is the Netherlands.*

Click or tap here to enter text.

**ANNEX 1 TO APPENDIX 2**

**A. LIST OF PARTIES**

*See Agreement*

**B. DESCRIPTION OF TRANSFER**

*See Exhibit to the Agreement titled “Data Processing Details”.*

**C. COMPETENT SUPERVISORY AUTHORITY**

**Commission Nationale de l'Informatique et des Libertés – CNIL**

3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**ANNEX 2 TO APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES**

See Appendix 1 of the DPA to which these Clauses are attached. In addition, Data Importer shall ensure all Personal Information is pseudonymized and encrypted when appropriate. Also, when receiving a request from a governmental authority relating the Personal Information that is the subject of these Clauses, Data Importer and its Affiliates warrant that (i) access demands by intelligence services or similar authorities in the USA or elsewhere to, and (ii) any “duty of disclosure” of, the Personal Information described in Annex 1B will be contested by the Data Importer and its Affiliates in accordance with applicable laws and regulations before extraction.

**ANNEX 3 TO APPENDIX 2 – LIST OF SUB-PROCESSORS**

*See Exhibit to the Agreement titled “Data Processing Details”*.

**APPENDIX 3**

**Additional State, Country, Regional, and Provincial Legal Requirements**

**UK ADDENDUM: Data Protection Act 2018**

This Appendix 3 hereby incorporates by reference the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, and shall be considered executed in full by all parties to the Agreement, covering all applicable transfers under the DPA, and including all Part 2 Mandatory Clauses.

**SWITZERLAND ADDENDUM: FADP**

1. In so far as the data transfers described in Appendix 2 are subject to the FADP, references to the GDPR should be understood as references to the Swiss Federal Act on Data Protection (“FADP”).
2. For so long as required under the FADP, the personal data of legal entities shall be protected pursuant to these Clauses in the same manner as individuals who are data subjects.
3. Clause 13: Parallel Supervision
	1. Where the data transfer is governed by the FADP: the Federal Data Protection and Information Commissioner (“FDPIC”) is the competent supervisory body;
	2. Where the data transfer is governed by GDPR: the criteria of Clause 13(a) shall apply.
4. Clause 18(c): Choice of forum and jurisdiction: A data subject, who has his/her habitual residence in Switzerland, may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland.

**CANADA ADDENDUM: Quebec Law 25**

* + - 1. Any section of this DPA that ensures Supplier only Processes Personal Information in accordance with Company's documented instructions shall be interpreted to also forbid any attempt to anonymize, aggregate, or otherwise modify Personal Information in a manner so that it no longer constitutes or includes information relating to or about an identified or identifiable Data Subject, except to the extent required to provide the Services to Company or as expressly authorized in writing by Company.
			2. Any notification required under this DPA in relation to a Personal Data Breach, and any similar notification required under the Agreement, shall also be required for any event constituting a breach or attempted breach of this DPA by Supplier.
			3. If required to collect consent in connection with the terms of this DPA, Supplier must also retain the evidence of all consents for three (3) years after the end of the Agreement.

**United Arab Emirates ADDENDUM: Federal Law No. 45 of 2021 on the Protection of Personal Data**

1. In so far as the data transfers described in Appendix 2 are subject to the United Arab Emirates’ Federal Law No. 45 of 2021 on the Protection of Personal Data (“**PDPL**”), unless and until the UAE’s Data Office issues its own standard contractual clauses to legitimize the transfer of Personal Information outside the United Arab Emirates and the Parties have entered into such standard contractual clauses, the Parties agree that the Standard Contractual Clauses attached hereto as Appendix 2 shall apply, *mutatis mutandis*, in relation to such transfers to provide for appropriate safeguards for the Personal Information and Data Subjects. For these purposes:
	1. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “PDPL”.
	2. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of the PDPL.
	3. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “United Arab Emirates”.
	4. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Data Office”.
	5. Any dispute arising from the Standard Contractual Clauses shall be governed by the laws of the United Arab Emirates and resolved by the courts of the United Arab Emirates. The Parties agree to submit themselves to the jurisdiction of such courts.
	6. If there is any inconsistency or conflict between the PDPL and the Standard Contractual Clauses attached hereto as Appendix 2, the PDPL applies.
	7. If the meaning of the Standard Contractual Clauses attached hereto as Appendix 2 is unclear in so far as it applies to transfers of Personal Information outside the UAE, or there is more than one meaning, the meaning which most closely aligns with the PDPL applies.
2. If the UAE’s Data Office issues its own standard contractual clauses to legitimise the transfer of Personal Information outside the United Arab Emirates, the Parties shall negotiate in good faith with a view to agreeing and implementing the standard contractual clauses as soon as is reasonably practicable. Where the Parties enter into standard contractual clauses in accordance with the foregoing sentence, such standard contractual clauses shall, in relation to transfers of Personal Information subject to the PDPL outside the United Arab Emirates, replace the Standard Contractual Clauses attached hereto as Appendix 2 as the appropriate safeguards implemented to provide appropriate safeguards for the Personal Information and Data Subjects in relation to the transfers.
3. Company may revoke its agreement to be bound by the Standard Contractual Clauses attached hereto as Appendix 2 on written notice to Supplier where the Data Office adopts an adequacy decision that covers the transfer of Personal Information to which the Standard Contractual Clauses apply, or Company otherwise determines that other appropriate safeguards apply in relation to the transfer. From the date of any notice served by Company in accordance with the foregoing sentence, the Standard Contractual Clauses attached hereto as Appendix 2 shall cease to apply to transfers of Personal Information subject to the PDPL outside the United Arab Emirates.

**BRAZIL ADDENDUM: LGPD - Standard Contractual Clauses**

The following terms apply to any processing of personal data involving Brazilian residents, or where Brazilian law otherwise requires adherence to the Brazilian Standard Contractual Clauses.

The Brazilian Standard Contractual Clauses (“SCCs”) under the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD) must be adhered to where data of Brazilian residents is processed, or where any data transfer falls within the jurisdiction of Brazil’s LGPD. The parties agree to adopt the controller-to-processor SCCs in their entirety, as issued by the Brazilian National Data Protection Authority (ANPD), unless otherwise modified according to the terms expressly permitted by the clauses. Such SCCs are hereby incorporated by reference into the Agreement, with the following selections made where more than one option for text is presented:

OPTION B is selected for Section 3.1. *The Importer may carry out an Onward Transfer of Personal Data subject to the International Data Transfer governed by these Clauses, in the cases and according to the conditions described below and the provisions of CLAUSE 18.*

OPTION A. is selected for Section 4.1. *Without prejudice to the duty of mutual assistance and the general obligations of the Parties, the Designated Party below shall be primarily responsible for complying with the following obligations set forth in these Clauses:*

*a) Responsible for publishing the document provided in CLAUSE 14;*

*[x] Exporter [ ] Importer*

*b) Responsible for responding to requests from Data Subjects dealt with in CLAUSE 15:*

*[x] Exporter [ ] Importer*

*c) Responsible for notifying the security incident provided in CLAUSE 16:*

*[x] Exporter [ ] Importer*

**SAUDI ARABIA ADDENDUM: PDPL - Standard Contractual Clauses**

The following terms apply to any processing of personal data involving Saudi Arabian residents, or where Saudi Arabian law otherwise requires adherence to the Saudi Standard Contractual Clauses.

The Saudi Arabian Standard Contractual Clauses (“SCCs”) under the Personal Data Protection Law (PDPL) must be incorporated where data of Saudi Arabian residents is processed, or where a data transfer is subject to Saudi jurisdiction. The version of the SCCs aligned with the template type described in Annex 2 are applicable in full, and such SCCs are hereby incorporated by reference into the Agreement.