JOINT CONTROLLER ADDENDUM

REVISION DATE: July 13, 2023

For the purposes of this Joint Controller Addendum ("JCA"), the Merck Sharp & Dohme LLC entity or affiliate executing the contract or other form of agreement referencing this JCA (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

A. 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 "Joint Purpose").

B. The Parties wish to supplement the terms of the Agreement to ensure all sharing of Personal Information in connection with the Agreement is performed in compliance with Data Protection Law, and to clarify their roles as joint controllers of such data.

The Parties agree:

1. *Joint Processing Activities*. In relation to Personal Information Processed in connection with the Agreement, the subject-matter, nature, purpose and duration of the sharing, the categories of Data Subjects concerned, and the categories of Personal Information are specified in exhibit to the Agreement titled "Data Processing Details".

2. *Applicability*. The terms of this JCA apply to every Statement of Work under the Agreement unless otherwise specified in that Statement of Work.

3. *Obligations*. With respect to Personal Information Processed in connection with the Agreement, both Parties shall:

a) comply with Data Protection Law and their respective obligations under this JCA, and in the event a Party cannot meet these obligations, notify the other Party immediately and take all reasonable and appropriate actions necessary to remedy the noncompliance.

b) only Process Personal Information on as specified in this JCA and the Agreement, except with the other Party's written consent and also where:

   i. that Party has obtained the data subject's prior valid consent as required under Applicable Data Protection Law;

   ii. it is necessary for the establishment, exercise, or defense of legal claims in the context of specific administrative, regulatory, or judicial proceedings;

   iii. it is necessary to protect the vital interests of the data subject or of another natural person; or

   iv. it is required otherwise by applicable law, in which case, the affected Party shall inform the other Party of that legal requirement, 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.

.

c) not disclose or transfer Personal Information to any third party without that third party entering into a written agreement with terms at least as protective of Personal Information as the obligations set out in this JCA and the Agreement.

d) not sell, share, retain, use, or disclose Personal Information other than as specified in the Agreement or as otherwise authorized under this JCA.

e) be fully liable for all acts or omissions of its employees, affiliates, agents, subcontractors, and other representatives.

f) 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 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 JCA, and as appropriate:

   i. the pseudonymisation and encryption of Personal Information;

   ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

   iii. the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident;

   iv. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing; and

   v. the ability to confirm within 72 hours of detection whether an event constitutes a Personal Data Breach.

g) in the event of an actual or reasonably suspected Personal Data Breach of Personal Information, the discovering Party shall notify the other Party without undue delay (and in any event within 24 hours of becoming aware of the Personal Data Breach) and cooperate with the other Party to determine an appropriate course of action.

h) promptly notify the other Party without undue delay and in any event within 24 hours of:

   i. any complaint, inquiry, request or concern by a competent data protection or other regulatory authority relating to Personal Information connected to the Agreement; and

   ii. any complaint, inquiry, request, or concern by a Data Subject relating to the Personal Information connected to the Agreement, including any request to exercise rights under Data Protection Law or either Party's privacy policy, such as to access, rectify, amend, correct, share, delete or cease Processing his or her Personal Information.

i) comply with all reasonable and appropriate measures requested by the other Party necessary for both Parties to comply with their respective obligations under Data Protection Law and this JCA.

j) retain Personal Information no longer than necessary to accomplish the Joint Purpose, unless required otherwise by applicable law.

k) maintain the accuracy and integrity of Personal Information subject to this JCA.

l) in accordance with the terms of the Agreement, provide notice to and obtain a consent from any Data Subject whose Personal Information is collected in connection with the Agreement.

m) 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 JCA and for each Party to comply with Data Protection Law.

n) to the extent either Party is to Process Personal Information regarding Data Subjects of any country or region with restrictions on the cross-border transfer of Personal Information, both Parties shall only do so in compliance with Data Protection Law, which may include without limitation entering into the Standard Contractual Clauses or similar mechanisms intended to protect transfers of Personal Information.

o) except for changes made consistent with meeting a higher industry standard or Data Protection Law, both Parties shall maintain in effect and consistently apply their respective privacy and data security practices disclosed to the other Party in connection with any due diligence the other Party most recently conducted on those practices in connection with the Agreement.

p) each Party acknowledges and agrees that its execution of this JCA constitutes its certification that it understands the restrictions set forth in this JCA and will comply with them.

4. Definitions

a) “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.

b) “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.

c) “Process” means to perform any operation or set of operations on Personal Information or sets of Personal Information, whether or not 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.

d) “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.

e) “Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to third countries that have not been assessed by the European Commission as providing an adequate level of protection for personal data, as published by the European Commission on June 4, 2021, as may be updated from time to time.

f) 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.

g) In the absence of a definition under this Section, a term shall be interpreted in a manner compliant with applicable Data Protection Law.

5. Interpretation.

a) The words "include" and “including” shall be construed to mean including without limitation.

b) In connection with the Joint Purpose under the Agreement, both Parties may Process Personal Information of one or more of the other Party’s affiliates. In such event, any of those affiliates shall be considered a “Controller” of Personal Information and a third-party beneficiary of this JCA and entitled to rely upon and enforce all rights and protections afforded under this JCA, whether or not that affiliate is named as a party to the Agreement or this JCA.

c) This JCA is hereby incorporated into and forms part of the Agreement.

d) In the event and to the extent of any conflict between the terms of the Agreement and this JCA, the terms of this JCA 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.

e) In the event and to the extent of any conflict between the terms of this JCA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

f) Except as expressly amended herein, the terms of the Agreement will remain in full force and effect.

g) If this JCA 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.

h) Section and other headings in this JCA are for convenience of reference only and shall not constitute a part of or otherwise affect the meaning or interpretation of this JCA.

i) Annexes and appendices to this JCA shall be deemed to be an integral part of this JCA to the same extent as if they had been set forth verbatim in this JCA.

j) The provisions of this JCA 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 JCA shall remain in full force and effect.

k) This JCA 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 JCA by executing such counterpart.

l) This JCA constitutes the entire agreement between the Parties with respect to the subject of this JCA 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 JCA and neither Party is attempting to exclude any liability for fraudulent statements.

m) The governing law and jurisdiction provisions of the Agreement will apply to this JCA.

6. *Limits on Updates*. 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 “Joint Controller Addendum” located at *https://msdprivacy.com/privacyterms* will supersede and replace the terms of this JCA and will not

change until the next Triggering Event, except for changes required for compliance with applicable Data Protection Laws, with all such changes residing in or indicated by Appendix 3, to which the Parties automatically agree unless an objection is issued within 30 days of change being posted. A mechanism to receive notice of changes is available at the above link. In the absence of any additional written agreement regarding changes required for compliance with applicable Data Protection Laws between Triggering Events, such changes shall be interpreted in the manner having the most minimal material impact on the Agreement and this JCA that still meets those legal requirements.

7. *Applicability of Appendices*. The Standard Contractual Clauses attached hereto as Appendix 2 and the addenda attached as 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.

8. *Notice*. Notices given under this JCA (each a "Notice") shall be in writing. Notices given under this JCA 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 "JCA Notice from Supplier" or in the case of a Personal Data Breach "Urgent: Personal Data Breach Notice".

APPENDIX 1 – Information Technology Security Measures

1. **Network Security** - Supplier shall maintain network security policies, procedures, and systems and shall perform network security and activities consistent with best practices in Supplier's industry but that, at a minimum, include but are not limited to network firewall provisioning, intrusion detection, and regular (but in no event less frequently than annually) vulnerability assessments. In no event shall the foregoing as applied to the Personal Information of the Company be any less stringent and protective than those applied by Supplier to the protection of its own data and systems of a like or similar nature.

2. **Application Security** - Supplier shall provide, maintain, and support any of its software and systems provided or used in connection with the services or products under the Agreement and subsequent updates, upgrades, and bug fixes such that they are and remain secure from vulnerabilities, utilizing recognized and comparable industry practices or standards as set forth in paragraph 9 below.

3. **Data Security** - Without limiting Supplier's confidentiality obligations or other obligations to protect data and other information of Company or its Affiliates, including any Personal Information, under the Agreement or this JCA, Supplier shall store all Personal Information in accordance with industry best practices and in compliance with all applicable laws, and use security measures, including, but not limited to, encryption and firewalls, to protect such Personal Information from unauthorized disclosure or use. Such measures shall be no less rigorous than those measures maintained by Supplier for its own data of a similar nature. When Supplier stores Personal Information in a third-party's offsite facility, Supplier must have complied with the terms of this JCA related to disclosing Personal Information to third parties or otherwise subcontracting services or products to third parties and shall only use a third party's offsite storage facility that is otherwise reasonably acceptable to Company, without limiting the foregoing, the facility of a third party that is in full compliance with all of the provisions of this Appendix.

4. **Data storage** - Any and all Personal Information will be stored, processed, and maintained solely on designated Supplier computing and storage resources, and that no Personal Information will at any time be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of the Supplier's designated backup and recovery processes and encrypted in accordance with paragraph 6 below. Supplier shall store all backup Personal Information as part of its designated backup and recovery processes.

5. **Data Transmission** - Any and all electronic transmission or exchange of Personal Information with Company and/or any third parties shall take place via secure means (using HTTPS or SFTP or equivalent) and solely in accordance with paragraph 6 below.

6. **Data Encryption** - Supplier agrees that any and all Personal Information stored on any portable or laptop computing device or any portable storage medium, including all company backup data, shall be kept in encrypted form, using a commercially supported encryption solution. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption.

7. **Data Re-Use** –Except as required to provide the services or products under the Agreement or as otherwise permitted under this JCA, Supplier shall not distribute, repurpose or share across other applications, environments, or business units of Supplier any Personal Information.

8. **Security Breach Notification -** In the event of a personal data breach or breach of any of Supplier's security obligations, then in addition to its obligations under the Agreement or the JCA, Supplier shall notify Company of such an event within 24 hours of discovery by telephone and e-mail at the following phone number and email address:

Security Breach Notice Telephone No.: 704-345-6700

Merck Global Operations Center (“GOC”) (Select the option for “IT service disruption” (This option is currently #1. The GOC can page the Merck Cyber Personal Data Breach Response Team.)

Security Breach Notice Email: GOC@Merck.com

9. **Industry Standards** – As applicable to the services or products under the Agreement, generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by the following:

   a. Center for Internet Security - see http://www.cisecurity.org

   b. Payment Card Industry/Data Security Standards (PCI/DSS) – see http://www.pcisecuritystandards.org/

   c. National Institute for Standards and Technology - see http://csrc.nist.gov

   d. Federal Information Security Management Act (FISMA) - see http://csrc.nist.gov

   e. ISO/IEC 27000-series - see http://www.iso27001security.com/

   f. Organization for the Advancement of Structured Information Standards (OASIS) – see http://www.oasis-open.org/

   g. The Open Web Application Security Project’s (OWASP) “Top Ten Project” – see http://www.owasp.org

   h. The CWE (Common Weakness Enumeration) – see http://cwe.mitre.org or CWE/SANS Top 25 Programming Errors - http://cwe.mitre.org/top25/

   i. The SANS Institute- see http://www.sans.org

   j. Most Dangerous Software Errors http://www.sans.org/top25-programming-errors/

APPENDIX 2

In the event Company or Supplier is exporting Personal Information in a manner that requires Module 1 of the Standard Contractual Clauses, the following terms apply:

The body text of Module 1 (Controller 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:

1. *Clause 7 (docking clause) is omitted.*

2. *For Clause 11, the optional text is omitted.*

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

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

ANNEX I 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
8 rue Vivienne, CS 30223
F-75002 Paris, Cedex 02
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: **http://www.cnil.fr/**

ANNEX 2 TO APPENDIX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

See Appendix 1 of the JCA to which these Clauses are attached. In addition, Data Importer shall ensure all Personal Data is pseudonymized and encrypted when appropriate. Also, when receiving a request from a governmental authority relating the Personal Data 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 data described in Annex 1B will be contested by the Data Importer and its Affiliates in accordance with applicable laws and regulations before extraction.

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 JCA, 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
    a. Where the data transfer is governed by the FADP: the Federal Data Protection and Information Commissioner (“FDPIC”) is the competent supervisory body;
    b. 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 notification required under of this JCA 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 JCA by Suppler.
2. If required to collect consent in connection with the terms of this JCA, Supplier must also retain the evidence of all consents for three (3) years after the end of the Agreement.