Effective: April 1, 2022

DATA PROTECTION ADDENDUM

In the event an agreement ("Underlying Agreement") entered into by and between (i) Sumitomo Pharma America Holdings, Inc. or its Affiliate (including Sunovion Pharmaceuticals Inc.) identified the Underlying Agreement ("Company") and (ii) the service provider, vendor, or consultant identified in the Underlying Agreement (for the purpose of this Addendum, "Service Provider") requires Service Provider to collect, store, use, disclose, or otherwise process any Personal Information (defined below) under Data Protection Laws (defined below), the terms and conditions stated in this addendum ("Addendum") shall apply and are incorporated by reference into the Underlying Agreement. To the extent the terms in this Addendum conflict with those in the Underlying Agreement, these terms will control.

This Addendum applies to Personal Data processed by or accessible to Service Provider (including its Affiliates) and its Subprocessors in connection with the provision of services under the Agreement. At all times during the term of the Agreement and during any period of time during which Service Provider processes or has access to Personal Data, Service Provider shall, and shall cause each authorized Subprocessor to, comply with the terms of the Agreement, including the terms set forth in this Addendum.

1. DEFINITIONS

Terms used in this Addendum but not defined in Section 1 below (or elsewhere in this Addendum) shall have the meaning ascribed to them in the Underlying Agreement.

1.1. "**Administrative, Technical, and Physical Security Measures**" means those administrative, technical, and physical safeguards, including pseudonymization, Encryption, and all applicable requirements described in the most recent version of the Center for Internet Security Controls, designed to protect the confidentiality, security, integrity and confidentiality of Personal Data, including measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

1.2. "**Affiliate**" means an entity related to Service Provider or Company, respectively, through common ownership or control.

1.3. "**Applicable Law**" means any applicable national, federal, state, provincial, local, and other laws, regulations, industry-recognized codes of conduct or other legal requirements governing the relationship between Company and Service Provider and the services provided under the Underlying Agreement,

including but not limited to the California Consumer Protection Act (Cal. Civ. Code 1798.100 – 1798.199) and the European Union's General Data Protection Regulation (Regulation (EU) 2016/679).

1.4. "**Data Controller**" shall mean the entity which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

1.5. "**Data Processor**" shall mean an entity which Processes Personal Data on behalf of the Data Controller.

1.6. "**Data Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure and acquisition of, or access to, Personal Data transmitted, stored, or otherwise processed.

1.7. "**Data Subject**" means any person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The term includes persons who have already been identified as well as those who might be identified by reference to the identifiers set forth above.

1.8. "**Encryption**" means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key. For the purposes of this agreement, any encryption mechanism used must accord with industry best practices for data encryption.

1.9. "**Government Authority**" means a legislative, executive, administrative, or regulatory entity, judicial body, or other public agency or authority of any country, state, territory, or political subdivision of a country, state, or territory, or a person or entity acting under a grant of authority from or under contract with such public agency or authority, that is authorized by law to enforce individual rights with respect to Personal Data, or to oversee or monitor compliance with privacy, data protection, or data security laws, rules, regulations, or other Applicable Law.

1.10. "**Personal Data**" shall mean (a) all individually identifiable information created, collected, accessed, received, or otherwise processed pursuant to the services performed under this Underlying Agreement; and (b) any other information that Applicable Law treats as "personal information" (or equivalent term, including without limitation, "personal data," "personally identifiable information," and "nonpublic personal information").

1.11. "**Privacy Program**" means Service Provider's comprehensive written privacy and information security program.

1.12. "**Process**" (and its conjugates, including without limitation, "**processed**" and "**processing**," regardless of whether such terms are capitalized or not, unless contrary to the context or meaning thereof) shall mean any operation or set of operations which is performed upon Personal Data, including (without limitation) collection, recording, organization, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.13. "**Sell**" (and its conjugates, including without limitation, "**selling**," "**sale**," and "**sold**," regardless of whether such terms are capitalized or not, unless contrary to the context or meaning thereof) means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to another business or a third party for monetary or other valuable consideration.

1.14. "**Security Incident**" shall mean:

A. any of the following:

(1) a Data Security Breach;

(2) a security vulnerability that carries a material risk of compromising the confidentiality, integrity, or security of Personal Data; or

(3) a violation of Applicable Law relating to the Processing of Personal Data under this Agreement;

B. but shall exclude:

(1) any unintentional acquisition, access, or use of Personal Data by an employee or agent of Service Provider if such acquisition, access, or use was made in good faith and does not result in further unauthorized or inappropriate Processing of Personal Data;

(2) any inadvertent disclosure by a person who is authorized to access Personal Data on behalf of Service Provider to another person authorized to access Personal Data on behalf of Service Provider, provided the information received as a result of such disclosure is not further used or disclosed in an unauthorized or inappropriate manner; or

(3) any loss or unauthorized acquisition of or access to Encrypted Personal Data, provided the confidential process or key that is capable of compromising the security, confidentiality, or integrity of the Encrypted Personal Data is not also subject to compromise, loss or unauthorized acquisition or access.

C. Notwithstanding paragraph B above, a "Security Incident" shall include any loss or unauthorized acquisition, access, or use of Personal Data that triggers a breach notification requirement under Applicable Law.

1.15. "**Subprocessor**" means any third party engaged by Service Provider to process Personal Data on behalf of Company but excludes any Affiliate of Service Provider.

2. USE AND DISCLOSURE OF PERSONAL DATA

Service Provider's Processing of Personal Data shall be governed by the Underlying Agreement or any Statement of Work or Exhibit thereto, which sets out the subject matter, duration, nature, and purpose

of the Processing, type of Personal Data and categories of Data Subjects, and obligations and rights of Company as Data Controller.

2.1. Service Provider shall only Process Personal Data in accordance with Company's instructions and as necessary to carry out an obligation under the Underlying Agreement, including any Statement of Work thereunder, or as otherwise required by Applicable Law. Service Provider will only Process the minimum amount of Personal Data required to meet its obligations under the Underlying Agreement or Applicable Law.

2.2. Except as provided in the Underlying Agreement or Applicable Law, neither Service Provider nor any of its employees, agents, consultants or assigns shall have any right to Process Personal Data for their own commercial benefit in any form (including, without limitation, to create de-identified or anonymized data) or to Sell, retain, use or disclose Personal Data for any commercial purpose or outside of the direct business relationship between the Parties.

2.3. Service Provider certifies that it understands the restrictions contained in this Addendum and will comply with them.

3. IDENTIFICATION OF PARTIES AND OWNERSHIP OF DATA.

3.1. The Parties agree that Company shall act as a Data Controller and Service Provider shall act as a Data Processor under the Underlying Agreement.

3.2. The Parties agree that Company is the sole owner of all Personal Data provided by Company to Service Provider or created or received by Service Provider on behalf of Company in pursuit of the services provided under the Underlying Agreement.

4. COMPLIANCE WITH APPLICABLE LAW

Both Parties agree to comply with all Applicable Law throughout the term of the Underlying Agreement and mutually covenant not to place the other in violation of Applicable Law. Service Provider will immediately inform Company if it believes any of Company's instructions are inconsistent with Applicable Law.

4.1. Both Parties understand that they have a duty to stay informed of possible changes to such laws throughout the course of this Underlying Agreement.

4.2. Where Applicable Law may require Service Provider to Process Personal Data for a purpose unrelated to the delivery of the services (including to respond to a government investigation, subpoena, request for information, or similar process), Service Provider shall:

A. promptly notify Company of any required Processing;

B. accommodate reasonable efforts and requests by Company to limit any such required Processing; and

C. Process only the Personal Data necessary to meet its legal obligations.

5. COMPLIANCE WITH COMPANY POLICIES AND PROCEDURES

Service Provider shall act only in accordance with applicable Company policies and procedures provided to Service Provider in advance of performing the services hereunder, including, but not limited to, policies concerning required Administrative, Technical, and Physical Security Measures. Service Provider agrees to implement such reasonable additional data protection policies and procedures as required by Company from time to time upon written request.

6. DATA PROTECTION ASSISTANCE

6.1. Service Provider shall provide full and prompt cooperation with and assistance to Company with respect to any data protection impact assessments and/or prior consultations that may be required in respect of Processing carried out under the Underlying Agreement.

6.2. Service Provider shall promptly make available to Company all information necessary to demonstrate compliance with this Addendum and Applicable Law and shall cooperate with relevant Government Authorities upon request by Company.

7. SERVICE PROVIDER PRIVACY AND SECURITY PROGRAM

During the term of this Underlying Agreement, Service Provider will maintain and materially comply with a Privacy Program designed to ensure that Personal Data will only be Processed in accordance with this Addendum, including the appointment of a data protection officer as required by Applicable Law.

7.1. Security Measures. Service Provider will implement Administrative, Technical, and Physical Security Measures to protect Personal Data, ensure a level of security and confidentiality appropriate to the risk represented by the processing and the nature of the data to be protected, and restore availability

and access to data in the event of an incident. Service Provider agrees to regularly test, assess and evaluate the effectiveness of the measures for ensuring the security of Processing.

7.2. Encryption. Service Provider agrees that all Personal Data transferred to or stored on any mobile device, including but not limited to smart phones, laptop computers, compact discs, PDAs, thumb drives, backup tapes, and/or zip drives, shall utilize Encryption.

8. OVERSIGHT OF PERSONNEL

8.1. Confidentiality. Service Provider shall ensure that any persons authorized to Process Personal Data on Service Provider's behalf have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Service Provider shall ensure such persons are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Service Provider shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

8.2. Limitation of Access and Processing. Service Provider shall ensure that access to Personal Data is limited to those employees, contractors, and Subprocessors performing services in accordance with this Underlying Agreement on a "need-to-know" basis only. Service Provider shall ensure that any Processing by its employees, contractors, and Subprocessors is done only pursuant to this Underlying Agreement or as required by Applicable Law.

9. SECURITY INCIDENTS

9.1. Service Provider agrees to notify Company without undue delay but in all cases within twenty-four (24) hours of discovery of any actual or suspected Security Incident of which it becomes aware, including those occurring at its Subprocessors. Service Provider agrees to take such reasonable, remedial actions warranted to investigate and halt the root cause of such incident to the extent it is ongoing.

9.2. In the course of notification to Company, Service Provider will provide to Company, as feasible, sufficient information for Company to assess the Security Incident and make any required notification to any Government Authority within the timeline required by Applicable Law. Such information must include, but is not necessarily limited to:

A. The nature of the Security Incident, and the categories and approximate number of data subjects and Personal Data records involved;

B. The likely consequences of the Security Incident, in so far as consequences are able to be determined; and

C. Any measures taken or proposed to be taken to address or mitigate the incident.

9.3. Company will decide on the basis of all available information and Applicable Law if notification to Data Subjects and/or Government Authorities is required by law or deemed prudent by Company. Where Company determines that notice should be provided, Service Provider shall reimburse Company for all reasonable costs associated with providing notice to affected individuals and Government

Authorities, unless Service Provider demonstrates that the breach was caused by Company's negligence or willful misconduct.

9.4. In the event of a Security Incident relating to the Personal Data collected or received under this Underlying Agreement, Service Provider agrees to assist and fully cooperate as instructed by Company with any internal investigation or external investigation by third parties, such as law enforcement, through the provision of information, employees, interviews, materials, databases, or any and all other items required to fully investigate and resolve any such incidents and provide information necessary to provide required notifications. Service Provider agrees to take such remedial actions as the Parties mutually agree is warranted, such agreement not to be unreasonably withheld by Service Provider.

9.5. Service Provider shall not disclose, without Company's prior written approval, any information related to the suspected Security Incident to any third party other than a vendor hired to investigate/mitigate such Security Incident and bound by confidentiality and non-disclosure obligations, except as required by Applicable Law.

9.6. Notwithstanding any other limitation of liability or other indemnification obligation contained in the Underlying Agreement, Service Provider agrees to indemnify Company for all losses resulting from any Security Incident due to negligence or willful misconduct by Service Provider, its agents, its affiliates, or any Subprocessor retained by Service Provider, including but not limited to costs associated with investigating the Security Incident, expenses associated with making notices or providing support to impacted Data Subjects, legal damages, government penalties, and/or mitigation expenses.

10. RIGHTS OF DATA SUBJECTS

In the event Service Provider receives a request from a Data Subject to exercise the Data Subject's rights under Applicable Law, Service Provider agrees to promptly advise Company of such request and follow reasonable instructions by Company. Service Provider shall assist Company as needed in responding to or fulfilling requests, whether received by Service Provider or Company, from Data Subjects to exercise rights under Applicable Law.

11. NOTIFICATION OF INSPECTION

Service Provider agrees to promptly notify Company of any inspection or audit by a Government Authority concerning compliance with Applicable Law related to the services provided under this Underlying Agreement.

12. CROSS-BORDER DATA TRANSFERS

12.1. Service Provider shall not transfer any Personal Data from the country in which it was collected from Data Subjects or received from Company without express written approval from Company. In the event Company requests Service Provider to transfer Personal Data across national borders, and without prejudice to the Data Subject's rights, Service Provider agrees to consult with Company to ensure the lawful export of Personal Data through an appropriate mechanism, the terms of which may be outlined

in a separate agreement. Where permitted by Applicable Law of the country from which Personal Data is exported, possible arrangements for the export of Personal Data may include, without limitation:

A. Applicable Law in the importing country ensures an adequate level of protection for Personal Data , as recognized by the laws of the exporting country;

B. Service Provider has in place binding corporate rules approved under Applicable Law;

C. Service Provider is subject to a code of conduct with binding and enforceable commitments in accordance with Applicable Law; or

D. Contractual data protection clauses have been put in place between Company and Service Provider that provide adequate protection.

12.2. Service Provider agrees to comply with any alternative lawful method of transfer as may be required by Company. This may include, without limitation:

A. Where the safeguards set forth in items (i) through (iv) of paragraph (a) above are not available, that Company may request Service Provider to transfer Personal Data pursuant to the explicit consent of the data subject, once the data subject has been notified and informed of potential risks pursuant to Applicable Law.

B. Where the safeguards set out in items (i) through (iv) of paragraph (a) above are not available, that Company may request Service Provider to transfer Personal Data pursuant to other arrangements permitted under Applicable Law.

13. RETENTION

Service Provider agrees to retain Personal Data received from Company or created on behalf of Company for only so long as necessary to conduct the services under the Underlying Agreement or as may otherwise be required under Applicable Law.

14. RETURN/DESTRUCTION

Upon termination or expiration of the Underlying Agreement, or earlier upon written request by Company, Service Provider agrees to return or destroy all Personal Data received or created pursuant to the Underlying Agreement, to the extent permitted by law.

14.1. Service Provider agrees to promptly notify Company of any inability to return or destroy Personal Data.

14.2. Service Provider agrees that any Personal Data retained as required by law shall remain subject to the requirements of this Addendum, which shall survive termination of the Underlying Agreement with respect to such data.

15. RECORDS

15.1. Service Provider shall maintain a written record of all Processing activities carried out on behalf of Company. Such record shall contain, at a minimum:

A. The name and contact details of any Subprocessors;

B. The name and contact details of the Subprocessors' data protection officers;

C. The categories of Processing carried out;

D. Transfers to third countries or international organizations and documentation of the suitable safeguards employed;

E. A general description of the Administrative, Technical, and Physical security measures taken to safeguard the Personal Data.

15.2. Service Provider shall provide such written record to Company promptly upon request and agrees that such written record, together with the relevant privacy provisions of this Addendum, may be submitted by Company to any third-party data controller (where applicable) and to relevant Government Authorities.

16. SUBPROCESSORS

16.1. Service Provider agrees that all subprocessing agreements shall be in writing and Service Provider has provided Company with a list of Subprocessors, and will inform Company of any intended changes concerning the addition or replacement of such Subprocessors and provide Company with an opportunity to object to such changes. Service Provider agrees that it will not disclose Personal Data to any Subprocessor without Company's prior written approval.

16.2. Service Provider agrees that all approved Subprocessors must agree to (i) comply with the terms of this Addendum and Applicable Laws; (ii) be properly trained on how to handle Personal Data; and (iii) comply with applicable Company policies and procedures, as referenced in Section 5.

16.3. Service Provider shall be responsible for any noncompliance with the terms of this Addendum by any Subprocessor, which noncompliance will constitute a breach as if committed directly by Service Provider. Service Provider will indemnify Company for all losses caused by any Subprocessor's non-

compliance with this Addendum, including but not limited to costs of investigation, legal damages, government penalties, and/or mitigation expenses.

17. AFFILIATES

17.1. Service Provider agrees that before delegating any rights or obligations under this Addendum to Affiliates of Service Provider, such Affiliates of Service Provider shall be bound by written agreement to comply with the terms of this Addendum to the same extent as Service Provider.

A. Service Provider shall be responsible for any noncompliance with the terms of this Addendum by any Affiliate of Service Provider.

B. Service Provider shall make available to Company at Company's request a list of Affiliates to which it has delegated any rights or obligations under this Addendum.

17.2. Company may delegate its rights and obligations under this Addendum to an Affiliate of Company.

18. RIGHT TO AUDIT

Company or any agent, representative, or third party working on Company's behalf, shall have the right to audit Service Provider during Service Provider's normal business hours and on reasonable notice in order to monitor compliance with the terms of this Addendum. Each Party shall bear their own expenses in relation to such audit.

19. EFFECT OF VIOLATION

If Service Provider breaches the terms of this Addendum, including by engaging in unauthorized data processing, and such breach is capable of cure, Service Provider will have five (5) days to the cure the breach. If the breach is not cured within five (5) days or is incapable of cure, Company has the right to immediately terminate the Underlying Agreement, including any applicable Statements of Work hereunder, without penalty. Failure to comply with any provision of this Addendum shall constitute a material breach of the Underlying Agreement.

20. INDEMNIFICATION

Service Provider will indemnify Company against all fines, losses or damages incurred by Company and Company's Affiliates, as a result of Service Provider's breach of this Addendum. For the avoidance of doubt, Service Provider's liability to Company under this Addendum shall not be subject to the limitations or exclusions set forth in Section 9 of the Underlying Agreement.

21. MISCELLANEOUS

21.1. Survival. The obligations of confidentiality and data privacy under this Addendum will survive the termination and/or expiration of the Underlying Agreement, including any Statement of Work hereunder. In addition, all remedies available to the Parties under this Addendum or Applicable Law shall survive the termination or expiration of the Underlying Agreement.

21.2. Equitable Relief. Each Party acknowledges that a breach of this Addendum may cause the non-breaching Party irreparable damages, for which an award of damages would not be adequate

compensation and agrees that, in the event of such breach or threatened breach, the non-breaching Party will be entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the non-breaching Party may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in the Underlying Agreement to the contrary.

21.3. Interpretation. For purposes of this Addendum: (A) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation"; (B) the word "or" is not exclusive; (C) the words "herein," "hereof," "hereby," "hereto," and "hereunder" refer to this Addendum as a whole; and (D) words denoting the singular have a comparable meaning when used in the plural, and vice-versa. The Parties intend this Addendum to be construed without regard to any presumption or rule requiring construction or interpretation against the Party drafting an instrument or causing any instrument to be drafted.

21.4. Headings. The headings contained in this Addendum are intended solely for ease of reference and shall be given no effect in the construction or interpretation of this Addendum.

21.5. Notices. All notices required pursuant to this Addendum should be sent to Company's Data Privacy Officer by email and physical mail at the following addresses:

a. privacy@sunovion.com
b. Gregory Bokar
   Attn: Legal Affairs
   84 Waterford Drive
   Marlborough, MA 01752
   USA