APPENDIX A

Data Protection Appendix

Controller to Processor

This Data Protection Appendix ("DPA") shall be a part of and incorporated into the Agreement. In the event and to the extent of a conflict between this DPA and the Agreement, this DPA shall control with respect to that conflict. In the event and to the extent of a conflict between this DPA and the SCCs (as defined in Section 2(b) below), the SCCs shall control with respect to that conflict. Capitalized terms in this DPA that are not defined in this DPA shall have the meanings set forth elsewhere in the Agreement.

1. Definitions and Interpretation

a. **Definitions**. In this DPA and Section A, the terms "Controller", "data subject", "Personal Data", "Process/Processing", "Processor" and "Supervisory Authority" shall have the meanings ascribed to them in EU General Data Protection Regulation 2016/679 ("GDPR").

"BCP" means business continuity plan and disaster recovery capabilities.

"Incident" means any of the following: (i) Contractor's breach of the obligations of this DPA or of Contractor's security or related procedures that could impact the confidentiality, integrity, or availability of any Regeneron Confidential Information, or (ii) any other use of Regeneron Confidential Information not expressly permitted by this Agreement, or is otherwise notifiable under Applicable Laws (including, without limitation, any actual or attempted ransomware, malware or similar attack).

"Regeneron Confidential Information" means all confidential information of Regeneron, without limitation including Regeneron Personal Data.

"Regeneron Personal Data" means Personal Data provided by Regeneron or its agents to Contractor or collected by Contractor for Regeneron and Processed by Contractor on behalf of Regeneron in the performance of the Services.

"Risk Assessment" means the evaluation of documented assurances provided by Contractor that reasonable and appropriate data protection controls have been implemented and demonstrated through independent third-party security assessments (*e.g.* SOC2 Type II, ISO 27001, Shared Assessments SCA) of Contractor's computer systems and networks that processes Regeneron Confidential Information, or evaluation of completed supplier security risk assessment self-attestation evaluation provided by Regeneron.

"Sale" means (A) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data by the Contractor to a third party for valuable consideration; or (B) sharing orally, in writing, or by electronic or other means, Personal Data with a third party, whether for valuable consideration or for no consideration, for the Contractor's commercial purposes.

"Services" means the services provided by Contractor under the Agreement.

2. Data Processing:

a) The parties shall accurately complete concurrently Annexes I, II & III of the SCCs (hereinafter, "Schedule 1"), which is attached hereto and incorporated as an integral part of the SCCs and this DPA. Schedule 1 describes the list of parties, description of Personal Data transfers, the competent supervisory authority in Annex I, the technical and organizational measures in Annex II, and the Subprocessors in Annex III. In Processing Regeneron Personal Data, Contractor shall (i) comply with Applicable Laws, (ii) not use or aggregate Regeneron

Personal Data for purposes other than Regeneron's documented instructions, and (iii) not engage in activity that constitute the Sale of Personal Data. Contractor shall provide reasonable and timely assistance to Regeneron, at Contractor's cost and expense, to enable Regeneron to comply with its obligations under Applicable Laws. Schedule 1 applies to both the EU SCCs and the UK Addendum (as defined below) where applicable.

b. **Location and International Data Transfers**. Contractor shall only Process Regeneron Personal Data at locations where Regeneron has provided express prior written consent. Notwithstanding the foregoing, Contractor shall not transfer any Regeneron Personal Data from one jurisdiction to another unless such transfer is in accordance with Applicable Laws. Regeneron may require Contractor to enter into one or more additional agreements for transfer of Personal Data from one jurisdiction to another. For transfer of Personal Data subject to the General Data Protection Regulation, the parties agree to the Standard Contractual Clauses published by the European Commission, incorporated into this DPA in attached Section A and executed concurrently with the Agreement (the "SCCs"). The parties shall include a description of the Personal Data that will be transferred from one jurisdiction to another in Schedule 1. Where UK Restricted Transfers are involved, the parties agree to be bound by the terms and conditions set out in the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, in force March 2022 (the "UK Addendum"): https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf. The UK Addendum and its definitions are hereby incorporated into this DPA by reference where applicable to Restricted Transfers as defined under Chapter V of the UK GDPR.

3. Information Security

a. **Obligations**. Contractor acknowledges that Regeneron has relied on Contractor's responses to Regeneron's information security Risk Assessment in entering into this Agreement. In accordance with terms of the Agreement, including this DPA and the SCCs, Contractor shall implement and maintain administrative, technical, and physical practices regarding security, privacy, confidentiality, continuation, backup, and disaster-recovery protection that are consistent with leading industry standards and practices and to protect against known risks and vulnerabilities. Such protection shall include, but not be limited to:

(i) personnel training and controls, such as communication of all applicable information security policies, background checks (as permitted by Applicable Laws), user authentication, security awareness training, and disciplinary processes; (ii) controls designed to ensure the physical safety and security of Contractor's facilities, including, without limitation, records of access and limitation of access to the Contractor's employees on a need-to know basis; (iii) controls designed to ensure Contractor's security posture is maintained over time, such as patch management, backups, and incident management; (iv) controls designed to prevent intrusion or unauthorized access to Contractor's systems and Regeneron Confidential Information, including virus protection software, firewalls, intrusion prevention technologies and other measures designed to ensure appropriate levels of access are restricted to authorized Recipient Personnel and subcontractors; (v) encryption of Regeneron Confidential Information while in transport, and encryption of Regeneron Confidential Information while at rest, consistent with industry standards; (vi) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational controls for ensuring the security of the processing; (vii) maintenance of credential security, including keeping user logins and passwords confidential, not sharing passwords with other persons, utilizing complex passwords and changing those passwords periodically, and notifying Regeneron immediately of any unauthorized use of any password or account or any other known or suspected breach of security; and (viii) Contractor's performance of vulnerability scans on all systems at least monthly, such scan criteria to include currency on system patching and conformance with standard, secure baseline configurations, and scan criteria

for internet facing systems (e.g. web sites) to include known vulnerabilities and the Open Web Application Security Project (OWASP) top ten critical security risks.

Contractor shall remediate all urgent, critical and high vulnerabilities and provide to Regeneron, upon request, reports of these mitigation plans and timelines. Regeneron reserves the right to perform non-invasive, external security scans of these systems on a periodic basis. Contractor shall procure and provide to Regeneron every three years, upon written request, at its own cost, independent third-party security assessments (*e.g.* SOC2 Type II, ISO 27001, Shared Assessments SCA) of Contractor's computer systems and networks that processes Regeneron data. If Contractor is unable to provide an independent assessment report due to the nature and size of its firm, Regeneron shall request the completion of a Regeneron provided supplier security risk assessment, in the form of a self-attestation to a standard questionnaire based on the Share Assessments framework, which completed questionnaire shall be provided to Regeneron within forty-five (45) days.

b. **Business Continuity Plan (BCP).** To the extent any specific additional security measures are required under the Agreement, including this DPA, Contractor shall implement such measures as part of the Services. At the onset of the relationship, and at least annually, upon Regeneron's written request, Contractor shall show evidence of BCP and affirm that these activities are periodically tested for effectiveness. Contractor's BCP shall include, but not be limited to, business impact analysis, disaster recovery and an emergency response plan. Every three years, upon Regeneron's written request, Contractor shall accurately complete and provide to Regeneron, Regeneron's Risk Assessment describing Contractor's computer systems and networks that Process Regeneron Confidential Information.

c. **Notification of Security Incidents**. Contractor shall notify Regeneron without undue delay upon becoming aware of an Incident, but in no event more than twenty-four (24) hours after Contractor's confirmation of the Incident with full details at dataprotection@regeneron.com and such other contact point as Regeneron may specify from time to time.

d. **Remediation of Security Incidents.** In addition to notifying Regeneron under Section 3(c) of this DPA and requirements in the SCCs, Contractor shall, at Contractor's expense, in the most expedient time possible : (i) investigate and take all reasonable steps to mitigate any potential damages and remediate the cause of the Incident; (ii) provide Regeneron with full details about the cause and impact of the Incident, and provide updates on any material developments or findings; (iii) take all reasonable actions to prevent any similar recurrence; and (iv) fully cooperate with Regeneron in its efforts to remediate and mitigate the effects of the Incident, including without limitation by undertaking actions as directed by Regeneron related to any notifications to affected persons, affected entities, or government bodies on behalf of Regeneron. Without limiting any rights or remedies available to Regeneron, notwithstanding anything else in the Agreement, including this DPA to the contrary, Contractor shall bear full responsibility for any costs (including, but not limited to those related to notifying affected individuals, the costs of any credit monitoring services, call center services, or other similar assistance as required by Applicable Laws), any fines and penalties assessed by regulators, and attorneys' fees and costs of litigation as reasonably incurred by Regeneron in connection with an Incident.

Section A

Standard Contractual Clauses

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art,

the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-

processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

Module 2: Controller to Processor

SCHEDULE 1: THE STANDARD CONTRACTUAL CLAUSES ANNEXES

ANNEX I

A. LIST OF PARTIES

1. Name:
Unselect all Regeneron Data Exporters that do not apply:

☒ Regeneron Pharmaceuticals, Inc.
☒ Regeneron Healthcare Solutions, Inc. ☒ Regeneron Ireland DAC
☒ Regeneron Canada Company
☒ Regeneron NL BV [Netherlands]
☒ Regeneron UK Ltd
☒ Regeneron GmbH [Germany]
☒ Regeneron Belgium BV
☒ Regeneron India Private Limited
☐ Other

Address of Regeneron signing entity:	
Contact person's name, position and contact details: *-Insert Name, position, and Regeneron email of the Agreement Signatory* *with cc: dataprotection@Regeneron.com*	
Activities relevant to the data transferred under these Clauses: *-Briefly describe Services/Activities requiring European Personal Data*	
Signature and date: *-For Regeneron, the Agreement signatory also signs SCC Annex I.*	*[Sign in signature block below]*
Role (controller/processor):	☐ Controller ☐ Processor
Role (Data Exporter/ Data Importer)	☐ Data Exporter ☐ Data Importer

2.

Contractor Name:	
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	*[Sign in signature block below]*
Role (controller/processor):	☐ Controller ☐ Processor
Role (Data Exporter/ Data Importer)	☐ Data Exporter ☐ Data Importer

Regeneron Pharmaceuticals, Inc.	[Contractor Name]
By:	
Title:	
Date:	

B. DESCRIPTION OF TRANSFER[5]

Categories of data subjects whose personal data is transferred

☐ Regeneron's employees
☐ Contractors
☐ Staff augmentation individuals and job applicants
☐ Regeneron's vendors' employees and agents
☐ Study subjects participating in trials sponsored by Regeneron
☐ Patients
☐ Health care providers
☐ Visitors to Regeneron's facilities
☐ Patients/providers with adverse event and product complain
☐ Individuals with product inquiries
☐ Third Party Personal Data provided to Regeneron

☐ Other *(insert)*

Categories of personal data transferred

☐ Names
☐ Sex (biological/sex at birth)
☐ Date of birth
☐ Email addresses (business or personal)
☐ Government ID (Social security numbers, Passport, Driver's license)
☐ Financial information (account and other payment details)
☐ HR records
☐ Images (photo/ video)
☐ Study subject and patient information (blood samples, patient IDs and medical records)
☐ Biological samples (includes study/sample IDs)
☐ Instrument Identifiers (GPS data, device IDs, IP address, authentication information)

☐ Other *(insert)*

[5] Complete the Description of Transfer for the Personal Data related to all Services that will fall under this Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Types of Sensitive Data:

☐ None
☐ Medical /health records
☐ Genetic data
☐ Racial or ethnic origin
☐ Religious or philosophical beliefs
☐ Political opinions
☐ Trade union membership
☐ Biometric data (fingerprint/ hand ID, face recognition, iris/retina imagery)
☐ Sex life, sexual orientation
☐ Gender (self-identification)
☐ Other *(insert)*

See Annex II for restrictions and safeguards for Sensitive Data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

☐ One off
☐ Continuous basis

Nature of the processing:

☐ Remote access
☐ Collection
☐ Recording
☐ Organization
☐ Structuring
☐ Storage
☐ Adaptation or alteration
☐ Retrieval
☐ Consultation
☐ Use
☐ Disclosure by transmission
☐ Dissemination or otherwise making available
☐ Alignment or combination
☐ Restriction
☐ Erasure
☐ Destruction
☐ Other *(insert)*

Country location(s) where European Personal Data is transferred to:

☐ United States
☐ India
☐ Ireland
☐ UK
☐ Belgium
☐ Canada
☐ Germany
☐ Netherlands
☐ Italy
☐ France
☐ Spain
☐ Other *(insert)*

Purpose(s) of the data transfer and further processing

☒ To provide Services related to the Agreement
☐ Other *(insert)*

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

☒ For the duration necessary to provide for the purpose of the Agreement
☐ Other *(insert)*

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

☒ *This SCC Annex I(B) Description of Transfer also applies to sub-processors*
☐ Other *(insert)*

c. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

☐ Where Regeneron is Data Exporter:
Ireland
Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28

☐ Where Contractor is the Data Exporter: [6]

(insert)

[6] See SCCs Clause 13 for guidance. If the Contractor is the data exporter, they should insert their registered supervisory authority or the country location of the majority of the data subjects. If you have questions, contact contracting.privacy@Regeneron.com.

ANNEX II [7]- TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Approval Date: 5/19/2022

The following describes the information security protocols and controls of the data importer. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

Overview

Regeneron has aligned itself to technical security standards and frameworks appropriate for the business that it serves. These standards include:

- NIST Special Publication 800-37, Guide for Applying the Risk Management Framework.
- NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization.
- Center for Internet Security (CIS) Benchmarks.
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

Technical and organizational measures in place to ensure the security of Regeneron systems and data include, but are not limited to, the following:

Data

- **Classification**: Regeneron classifies data as either Restricted, Confidential, Internal, or Public according to its level of sensitivity, and requires it be labelled and protected appropriately.
- **Encryption**: Restricted and Confidential data is required to be encrypted while at rest and during transit.
- **Pseudonymization:** There are no enterprise-wide IT requirements related to pseudonymization, although there may be departmental procedures in place. The business must add language describing any pseudonymization used in the process being contracted.
- **Hard Copies**: Hard copy information classified as Restricted or Confidential may not be left unattended in an uncontrolled (non-office) environment, or when visitors are present. To prevent this, hardcopy information is stored in locked drawers/cabinets.
- **Data Retention**: Regeneron maintains an Enterprise Records Management Policy and associated Enterprise Records Retention Schedules specifying the appropriate retention and destruction time periods for business records.
- **Data Destruction**: Media containing Regeneron information assets and data are properly disposed of or sanitized when the media or the asset containing the media is end-of-life or is being repurposed. Appropriate disposal methods are used, based on device and media type. Regeneron utilizes the NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization.

Access

- **Access Management**: Access is managed on the principle of least access, that is, the user must have the minimum access required to perform job duties. Administrative accounts require additional review prior to being provisioned. Accounts of any kind must be disabled upon separation of the employee or when job duties no longer require the access. To ensure access

[7] This template describes Regeneron's enterprise-wide information security protocols and controls, which can be adopted by any data importer. Localized policies and procedures may differ, and some processes may utilize alternate controls. It is the business' responsibility to confirm the specific information security controls are in place for this agreement and modify Annex II accordingly. **If the Contractor is the data importer, they will either replace these terms with their Annex II template or update this template language to describe their controls.**

is maintained at the appropriate level, periodic reviews are performed. Regeneron applications are configured to log access and to trigger automatic lock-out after the account is idle for a specified period. Remote Access to the Regeneron Enterprise Network providing access to applications, systems, and data requires two-factor authentication (2FA).

- **Passwords and PINs**: Standard account passwords must be a minimum length of 8 characters and contain at least 3 of the 4 following constraints: upper case alpha, lower case alpha, and one number or special character. Passwords must expire in 90 days and cannot be reused for 5 iterations or 365 days. Administrator and service account passwords must be a minimum length of 16 characters and meet the other requirements above. Any default Password or PIN will be changed during or immediately upon the completion of the installation process. PIN's will be used where a numeric method for authentication is required because alphabetical characters cannot be entered (e.g., for entry on a telephone keypad); in all other instances, passwords will be used.
- **Physical Security**: Security desks are staffed 24x7. All visitors must be registered. Building access is controlled by employee and visitor badges. Buildings have video surveillance and access control systems which are actively monitored 24x7 in a Security Operations Center.

Information Security

- **Anti-Malware**: All systems must have approved and supported anti-malware software configured to automatically clean infected files.
- **Threat and Vulnerability Management**: Information Security conducts vulnerability assessments including scanning network-connected (internal and external) systems for vulnerabilities and reviewing the changes made since the last vulnerability assessment. Assessments are performed on all new system build types and existing systems, including systems in the internal, external, and critical infrastructure, to identify misconfigurations, vulnerabilities, and risk exposure to exploitable vulnerabilities. Vulnerability Assessments consist of, but are not be limited to, automated vulnerability scanning, web application scanning, port scanning, manual testing, and policy compliance scanning.
- **Patch Management**: Devices that are connected to the Regeneron network are patched using an approved schedule to maintain security. Deployment dates are set based on criticality of the patch when released. The timeframe for deploying patches is based on the Vendor rating and the Common Vulnerability Scoring System (CVSS) classification and vendor classification as a baseline.
- **Network Security**: Network segmentation is implemented where identified to limit access to data and resources. Segmentation is implemented based on the endpoint role, functionality, and business requirements. Regeneron networks implement security controls to limit lateral movement within the network. Regeneron network components are hardened where operationally feasible to mitigate security risks.
- **Logging**: All systems centralize logging to a Log Aggregator which forwards relevant events to the Security Information and Event Management software, if necessary and applicable. The log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.
- **Removable Media**: The use of portable/removable media is limited to Regeneron-supplied hardware (e.g., USB drives) or approved single/multi-write media (optical or magnetic), ensuring the media and/or data is appropriately protected.
- **Cybersecurity Incident Response**: Regeneron has developed an Information Security Incident Response Plan to provide organizational structure, operational guidance, response goals, general processes, and procedures to Regeneron personnel for properly responding to incidents that may affect the confidentiality, integrity, or availability of IT assets and

information or disrupt business operations. An information security Incident is any violation of Regeneron information security policies, breach of Regeneron physical, virtual, logical, or computer security which threatens the confidentiality, data, integrity, or availability of Regeneron's resources.

Recovery and Backup

- **Disaster Recovery**: Regeneron's critical systems and infrastructure have defined recovery requirements, documented recovery procedures, and are tested to ensure recovery capability. Systems are assigned to Recovery Tiers based on Recovery Time Objectives aligned with business recovery objectives.
- **Backups**: Information stored on computer systems are backed up on a routine basis to ensure its recoverability in the event of user or software error, system failure or other disaster. The frequency of backup is determined by the classification of the server or workstation. The retention period for backup copies is two years, as determined by policy.

Governance

- **Risk Management**: Regeneron has developed a Risk and Control Self-Assessment Program (RCS) – a structured process to effectively identify and assess IT risks impacting the company, as well as to validate the effectiveness of IT controls designed to protect our assets. Firmwide risks are evaluated to identify underlying inherent traits (risk factors) that require complementary controls to minimize risks from being realized. Regeneron keeps a Risk Register for documenting InfoSec risks and the associated mitigating actions to manage each risk. A technology risk management committee meets on a quarterly basis to review and monitor information technology risks and remediation efforts.
- **Information Security Policy Management**: Regeneron has developed information security policies that describe the technical and organizational measures in place to ensure the security of the company's systems and data. In addition, periodic reviews are performed to ensure the accuracy and completeness of policies. When compliance with a given policy is not possible or creates a significant hardship, an exception request is documented and submitted for review and approval by the business.
- **Third Party Assessments**: A Third-Party Assessment is required for new third-party suppliers or partners. InfoSec and other members of IT, as appropriate, evaluate the security, technical, and procedural controls that are implemented to identify and evaluate the associated risks. Regeneron considers the sensitivity of the information, the criticality of the services to Regeneron's revenue or reputation, and connectivity to the Regeneron Enterprise network, and applies an appropriate risk category. The assessment of the third-party includes, but is not limited to, its stability, security controls, and the impact of any external events on the services provided. The amount of review and documentation needed to support third-party contract management varies depending on the criticality and complexity of the system, process, or service outsourced and the risk category. At a minimum, third parties are re-assessed every 36 months.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processor(s):

1.

Name	
Address	
Contact person's name, position and contact details	
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	

2.

☐ Alternatively, Contractor's web link to sub-processor list with details above[8].

[8] Contractor's web link should contain all Annex III sub-processor descriptors above for Controller authorization subject to 9(a) of the SCCs.