DATA PRIVACY ANNEX FOR PURCHASE ORDERS

NOVARTIS DATA PROTECTION REQUIREMENTS

Section A

1. Conflict; Survival.

This Data Protection Requirements Exhibit ("Data Protection Exhibit") is made a part of the Statement of Work/Purchase Order (hereinafter also: "Agreement" or "Contract") and incorporated therein by reference. This Data Protection Exhibit and any associated Data Transfer Agreement will survive the expiration or termination of the Agreement for as long as Personal Data is being processed by Data Processor. In the event of a conflict or inconsistency between this Data Protection Exhibit and any other portion of the Agreement, the following order of precedence will govern:

a. Data Transfer Agreement (e.g. EU Model clauses);
b. This Data Protection Exhibit;
c. The Agreement

2. Data protection.

2.1. The representatives of the parties, or if they hire a natural person in their own name and representation, acknowledge being informed that the personal data reflected in the Contract are processed by the other parties for the purposes of maintenance, compliance, development, control and management of the contractual relationship.

2.2. In relation to the data of the contracting supplier, we inform you that Novartis Hellas, ("Novartis Hellas" or "Novartis"), is processing information about you, which constitutes "**personal data**" and the Novartis group considers the protection of your personal data and privacy a very important matter. Novartis reference includes Sandoz. Novartis is located at National Rd. No 1, 12th km, GR-144 51 Metamorphosis and Sandoz is located at 7B Fragkokklisias Street, GR-151 25 Maroussi, Athens.

Novartis is responsible for the processing of your personal data as it decides why and how it is processed, thereby acting as the "**controller**". In this Privacy Notice, "**we**" or "**us**" refers to Novartis.

We invite you to carefully read this Privacy Notice, which sets out in which context we are processing your personal data and explains your rights and our obligations when doing so.

Should you have any further question in relation to the processing of your personal data, regarding Novartis we invite you to contact the Data Protection Officer (DPO) at

privacy.novartisgr@novartis.com regarding Novartis and at privacy.sandozgr@novartis.com regarding Sandoz.

2.2.1. What information do we have about you?

This information may either be directly provided by you or provided by our supplier or service provider (i.e. the legal entity for whom you work).

We may collect various types of personal data about you, including:

(i) your general and identification information (e.g. name, first name, last name, gender, date and place of birth, nationality, ID card or passport numbers, email and/or postal address, fixed and/or mobile phone number and car registration number);
(ii) your function (e.g. title, position and name of company);
(iii) for natural persons acting as suppliers or service providers, financial information (e.g. bank account details); and
(iv) your electronic identification data where required for the purpose of the delivery of products or services to our company (e.g. login, access right, passwords, badge number, IP address, online identifiers/cookies, logs, access and connexion times, image recording or sound such as badge pictures, CCTV or voice recordings).

If you intend to provide us with personal data about other individuals (e.g. your colleagues or employees), you must provide a copy of this Privacy Notice to the relevant individuals, directly or through your employer.

2.2.2. For which purposes do we use your personal data and why is this justified?

2.2.2.1. Legal basis for the processing

We will not process your personal data if we do not have a proper justification foreseen in the law for that purpose. Therefore, we will only process your personal data if:

- we have obtained your prior consent;
- the processing is necessary to perform our contractual obligations towards you or to take pre-contractual steps at your request;
- the processing is necessary to comply with our legal or regulatory obligations; or
- the processing is necessary for our legitimate interests and does not unduly affect your interests or fundamental rights and freedoms.

Please note that, when processing your personal data on this last basis, we always seek to maintain a balance between our legitimate interests and your privacy. Examples of such ‘legitimate interests’ are data processing activities performed:

- to benefit from cost-effective services (e.g. we may opt to use certain platforms offered by suppliers to process data);
- to offer our products and services to our customers;
- to prevent fraud or criminal activity, misuses of our products or services as well as the security of our IT systems, architecture and networks;
- to sell any part of our business or its assets or to enable the acquisition of all or part of our business or assets by a third party; and
- to meet our corporate and social responsibility objectives.

2.2.2.2. Purposes of the processing

We always process your personal data for a specific purpose and only process the personal data which is relevant to achieve that purpose. In particular, we process your personal data for the following purposes always in accordance with the nature of our collaboration as well as applicable legislation and regulations:

- manage our suppliers and service providers throughout the supply chain;
- organise tender-offers, implement tasks in preparation of or to perform existing contracts;
- monitor activities at our facilities, including compliance with applicable policies as well as health and safety rules in place;
- grant you access to our training modules allowing you to provide us with certain services;
- manage our IT resources, including infrastructure management and business continuity;
- preserve the company's economic interests and ensure compliance and reporting (such as complying with our policies and local legal requirements, tax and deductions, managing alleged cases of misconduct or fraud, conducting audits and defending litigation);
- manage mergers and acquisitions involving our company;
- archiving and record-keeping;
- billing and invoicing; and
- any other purposes imposed by law and authorities.

2.2.3. Who has access to your personal data and to whom are they transferred?

We will not sell, share, or otherwise transfer your personal data to third parties other than those indicated in this Privacy Notice.

In the course of our activities and for the same purposes as those listed in this Privacy Notice, your personal data can be accessed by or transferred to the following categories of recipients on a need to know basis to achieve such purposes:

- our personnel (including personnel, departments or other companies of the Novartis group);

- our independent agents or brokers (if any);
- our other suppliers and services providers that provide services and products to us;
- our IT systems providers, cloud service providers, database providers and consultants;
- any third party to whom we assign or novate any of our rights or obligations; and
- our advisors and external lawyers in the context of the sale or transfer of any part of our business or its assets.

The above third parties are contractually obliged to protect the confidentiality and security of your personal data, in compliance with applicable law.

Your personal data can also be accessed by or transferred to any national and/or international regulatory, enforcement, public body or court, where we are required to do so by applicable law or regulation or at their request.

The personal data we collect from you may also be processed, accessed or stored in a country outside the country where Novartis is located, which may not offer the same level of protection of personal data.

If we transfer your personal data to external companies in other jurisdictions , we will make sure to protect your personal data by (i) applying the level of protection required under the local data protection/privacy laws applicable to Novartis, (ii) acting in accordance with our policies and standards and, (iii) for Novartis located in the European Economic Area (i.e. the EU Member States plus Iceland, Liechtenstein and Norway, the "**EEA**"), unless otherwise specified, only transferring your personal data on the basis of standard contractual clauses approved by the European Commission. You may request additional information in relation to international transfers of personal data and obtain a copy of the adequate safeguard put in place by exercising your rights as set out in Section "What are your rights and how can you exercise them?".

For intra-group transfers of personal data, the Novartis Group has adopted Binding Corporate Rules, a system of principles, rules and tools, provided by European law, in an effort to ensure effective levels of data protection relating to transfers of personal data outside the EEA and Switzerland. Read more about the Novartis Binding Corporate Rules by clicking or following the link https://www.novartis.com/sites/www.novartis.com/files/bcr-individual-rights-2012.pdf

2.2.4. How do we protect your personal data?

We have implemented appropriate technical and organisational measures to provide a level of security and confidentiality to your personal data.

These measures take into account:

(i) the state of the art of the technology;
(ii) the costs of its implementation;
(iii) the nature of the data; and
(iv) the risk of the processing.

The purpose thereof is to protect it against accidental or unlawful destruction or alteration, accidental loss, unauthorized disclosure or access and against other unlawful forms of processing.

Moreover, when handling your personal data, we:

- only collect and process personal data which is adequate, relevant and not excessive, as required to meet the above purposes; and
- ensure that your personal data remains up to date and accurate.

For the latter, we may request you to confirm the personal data we hold about you. You are also invited to spontaneously inform us whenever there is a change in your personal circumstances so we can ensure your personal data is kept up-to-date.

2.2.5. How long do we store your personal data?

We will only retain your personal data for as long as necessary to fulfil the purpose for which it was collected or to comply with legal or regulatory requirements.

The retention period is the term of your (or your company's) supply or service contract, plus the period of time until the legal claims under this contract become time-barred, unless overriding legal or regulatory schedules require a longer or shorter retention period. When this period expires, your personal data is removed from our active systems. Personal data we hold in our database about you which is not related to a specific contract, will be stored for as long as necessary for the purpose of processing, also taking into account the need to ensure that the Company is able to comply with its regulatory and other obligations and can establish, exercise or support legal claims. When this period expires, your personal data is removed from our active systems

Personal data collected and processed in the context of a dispute are deleted or archived (i) as soon as an amicable settlement has been reached, (ii) once a decision in last resort has been rendered or (iii) when the claim becomes time barred.

2.2.6. What are your rights and how can you exercise them?

You may exercise the following rights under the conditions and within the limits set forth in the law:

- the right to access your personal data as processed by us and, if you believe that any information relating to you is incorrect, obsolete or incomplete, to request its correction or updating;

- the right to request the erasure of your personal data or the restriction thereof to specific categories of processing;
- the right to withdraw your consent at any time, without affecting the lawfulness of the processing before such withdrawal;
- the right to object, in whole or in part, to the processing of your personal data; and
- the right to request its portability, i.e. that the personal data you have provided to us be returned to you or transferred to the person of your choice, in a structured, commonly used and machine-readable format without hindrance from us and subject to your confidentiality obligations.

If you have a question or want to exercise the above rights, you may send an email to the DPO of Novartis at privacy.novartisgr@novartis.com and regarding Sandoz to the DPO at privacy.sandozgr@novartis.com or a letter at the proper address indicated in the beginning of this notice with a scan of your identity card for identification purpose or any other lawful identification proof, it being understood that we shall only use such data to verify your identity and shall not retain the scan after completion of the verification. When sending us such a scan, please make sure to redact your picture and national registry number or equivalent on the scan.

If you are not satisfied with how we process your personal data, please address your request to our data protection officer global.privacy_office@novartis.com who will investigate your concern.

In any case, you also have the right to file a complaint with the competent data protection authorities, in addition to your rights above.

2.2.7. How will you be informed of the changes to our Privacy Notice?

Any future changes or additions to the processing of your personal data as described in this Privacy Notice will be notified to you in advance through an individual notice through our usual communication channels (e.g. by email or via our internet websites).

SECTION B)

PROCESSING OF PERSONAL DATA

1. Subject-matter and duration of the Processing Activities

1.1. The subject-matter of the Processing Activities are the services described in the Agreement and/or in a Statement of Work/Purchase Order executed under the Agreement in as far as these require the processing of Personal Data.

1.2. The duration of the Processing Activity is subject to the term and termination of the Agreement or – as the case may be – more specific provisions on term and termination in the relevant Statement of Work/Purchase Order.

2. Specification of the Personal Data and Processing Activities

2.1 Nature and Purpose of the intended processing of Personal Data are contained in the Statement of Work/Purchase Order.

2.2 Type of Personal Data to be Processed are contained in the Statement of Work/Purchase Order.

2.3 Categories of Data Subjects are contained in the Statement of Work/Purchase Order.

3. Documented Instructions

3.1 Vendor shall carry out Processing Activities on Personal Data solely for the purposes specified in the Agreement and as may be further instructed and documented by Novartis, including with regard to transfers of Personal Data to a country outside the EEA/CH, unless required to do so by European Union or EU Member State law to which Vendor is subject. In such a case, Vendor shall inform Novartis of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2 Vendor shall immediately inform Novartis, if, in its opinion, an instruction infringes Data Protection Laws.

4. Technical and Organizational Measures

4.1 Vendor has to ensure that all persons who have access to Personal Data have committed themselves to confidentiality. Vendor has to limit the use to the specified purposes, and permit access to authorized persons only on a need-to-know basis to the extent required for the performance of Vendor's obligations. Vendor shall ensure that all persons who have access to Personal Data have received appropriate privacy and security training, which shall be updated periodically in accordance with applicable laws, regulations, and industry standards, or as otherwise requested by Novartis. Vendor shall not use or disclose any Personal Data that Vendor creates, receives, maintains, or transmits as a result of

performance of Vendor's obligations, other than as expressly permitted or required by the Agreement.

4.2 The Vendor shall take all measures required to ensure a level of security appropriate to the risk of protecting the rights and freedoms of natural persons, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed. At a minimum, Vendor shall establish the technical security and organizational measures referenced in the Novartis Third Party Code together with the additional requirements set forth under this Contract named (Additional Information Security Requirements). The technical and organizational measures are subject to technical advancements and development. In this regard, it is permissible for Vendor to implement alternative adequate measures so long as the minimum defined level of security is not reduced. Substantial changes must be documented.

4.3 Throughout the term of the Agreement, Vendor will maintain and monitor a comprehensive, written privacy and information security program, including data protection policies and procedures, and consistent with any privacy compliance plan established between the parties and attached hereto, that contains administrative, technical and physical safeguards designed to protect against reasonably anticipated threats to the security, confidentiality or integrity of, and the unauthorised Processing of, Personal Data. Vendor will periodically assess reasonably foreseeable risks to the security, confidentiality, integrity, and resilience of electronic, paper and other records containing Personal Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks.

5. Rectification, restriction and erasure of Personal Data

5.1 The Vendor may not on its own authority rectify, erase or restrict the Processing of Personal Data that is being Processed on behalf of Novartis, except by written instructions from Novartis. Vendor will notify Novartis promptly (and in any event within three (3) business days from receipt) of any communication received from a Data Subject relating to the Data Subject's rights to access, modify or correct Personal Data, as well as any claim for compensation from a Data Subject, and to comply with all instructions of Novartis in responding to such communications.

5.2 Insofar as the data at stake are in scope of the Personal Data Processed pursuant to this Agreement, any applicable Data Subject's right to transparent information, erasure ('right to be forgotten'), rectification, restriction, data portability, to object, to not be subject to an automated decision without human intervention, and access

shall be ensured by the Vendor in accordance with documented instructions from Novartis without undue delay.

6. Duty of cooperation and other duties of Vendor

6.1 Vendor shall provide Novartis with the contact details of Vendor's data protection officer or, if not applicable, the Vendor's direct point of contact for any matter related with the Agreement. Novartis shall be informed in writing within twenty-four (24) hours of any change of the data protection officer or direct point of contact.

6.2 Vendor will notify Novartis in writing and as soon as practical of any request made by any government, law enforcement or regulatory agency (but no later than one (1) business day from the date of receipt of any such request) for information concerning, or access to, Personal Data, unless notification to Novartis is prohibited by Data Protection Laws or other applicable laws, rules, regulations or orders. Vendor will cooperate with Novartis in responding to such requests.

6.3 Novartis shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to the Processing of Personal Data. This also applies insofar as the Vendor is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the processing of Personal Data in connection with the Agreement.

6.4 Vendor shall assist Novartis in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (e.g. ensuring the appropriate level of security, notifying the supervisory authority and the Data Subject in case of data breach, conducting any required data protection impact assessment and consulting the supervisory authority in relation therewith), taking into account the nature of Processing and the information available to the Vendor.

7. Vendor Subcontracting

7.1 Subcontracting for the purpose of this Data Protection Exhibit are to be understood as meaning services which relate directly to the provision of the principal obligation related to the Processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

7.2 Vendor shall not engage another Vendor Subcontractor without prior specific or general written authorisation of Novartis. In the case of general written authorisation, Vendor shall inform Novartis of any intended changes concerning the addition or

replacement of other Subcontractors, thereby giving Novartis the opportunity to object to such changes.

7.3 Vendor understands and agrees that, without limitation, the confidentiality, privacy and security requirements contained in this Agreement apply to any permitted Vendor Subcontractors, temporary employees or other third-parties who receive any Personal Data as a result of this Agreement. Vendor shall only enter into sub-contract agreements that include data protection provisions no less restrictive than the provisions set forth in this Data Protection Exhibit. Upon written request by Novartis, copies of such sub-contracts shall be provided to Novartis within seven (7) business days. Novartis must be granted: (a) the right to monitor and inspect Vendor Subcontractors upon reasonable notice; and (b) the right to obtain information from Vendor about the substance of the sub-contract and the implementation of the data protection obligations within the sub-contract relationship, upon written request.

7.4 If Vendor Subcontractor processes Personal Data outside the EU/EEA or Switzerland, Vendor shall obtain Novartis' prior written consent in accordance with the Agreement not only for the use of a Subcontractor but also for the transfer of Personal Data to any third country, and shall ensure compliance with EU Data Protection Regulations by appropriate measures, including without limitation the execution of a Data Transfer Agreement. In case Vendor is itself party to a Data Transfer Agreement with Novartis (or if required, with the relevant Novartis Affiliate) covering the relevant Processing operations, it shall ensure that it has obtained Novartis' (or the relevant Novartis Affiliate's) consent regarding the Vendor Subcontractor and third country Processing and prior to any Processing, Clause 11 of the Data Transfer Agreement is complied with.

7.5 Where that Vendor Subcontractor fails to fulfil its data protection obligations, Vendor shall remain fully liable to Novartis (and any relevant Novartis Affiliates) for the performance of that Vendor Subcontractor's obligations.

8. Data Security Breach

8.1 At any time during the processing of Personal Data, Vendor shall notify Novartis immediately after becoming aware of any Data Security Breach involving Personal Data, including any breach at facilities, systems or equipment of Vendor's Subcontractors. Vendor shall notify Novartis with details about Data Security Breach without limitation the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned. Vendor shall notify Novartis of the likely consequences of the Data Security Breach and the measures taken or proposed to be taken to address the Data Security Breach in a quick, adequate and effective way, including, where appropriate, measures to mitigate its possible adverse effects. Vendor shall document any Data Security Breach, comprising the facts relating to the Personal Data breach, its effects and

the remedial action taken and Vendor makes available that documentation to Novartis. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

8.2 Vendor agrees to assist and cooperate with Novartis concerning any disclosures to affected parties, government or regulatory agencies and with any other remedial measures requested by Novartis or required under any law. Vendor will take such mutually agreeable steps to prevent the continuation or repetition of such Data Security Breach.

8.3 Unless otherwise required by applicable Data Protection Laws or any other law, rule, regulation or order, Vendor will make no disclosures to affected parties or any government, law enforcement or regulatory agencies concerning a Data Security Breach relating to the Personal Data except as directed by Novartis. Notwithstanding the foregoing, Vendor may contact local police in the event of a physical breach of Vendor facilities or theft of equipment or documents.

8.4 Vendor will assist and cooperate with Novartis concerning any disclosures to such parties or agencies, and with any other remedial measures requested by Novartis or required under any law, rule, regulation or order applicable to Vendor or Novartis, at Vendor's expense, including providing notice to Data Subjects of a Data Security Breach and providing credit monitoring services to such individuals.

9. Compliance, Audits and Inspections

9.1 Vendor shall make available to Novartis all information necessary to demonstrate compliance with this Data Protection Exhibit and shall allow for and contribute to audits, including inspections, conducted by Novartis or another auditor mandated by Novartis.

10. Deletion and return of Personal Data

10.1 Copies or duplicates of Personal Data shall never be created without the knowledge of Novartis, with the exception of back-up copies as far as they are necessary to ensure orderly data processing and provided that such back-up copies are placed on media where they can be deleted, as well as Personal Data required to meet regulatory requirements to retain data.

10.2 Upon termination or expiration of the Agreement, or as requested in writing by Novartis at any time, Vendor will, at its own expense and at Novartis's option: (a) promptly return all Personal Data, copies or duplicates in a structured and commonly used format; or (b) destroy all documents, materials, and any other media that may contain Personal Data, without retaining any portion or copy thereof. Vendor will provide Novartis with a Certificate of Destruction of Personal Data in a form acceptable to Novartis, signed by an authorised employee of Vendor who has supervised such destruction.

11. Definitions

"**Personal Data**" – any information that relates to an identified or identifiable person including without limitation electronic data and paper based files that is Processed directly or indirectly, by Vendor or Vendor Subcontractors on behalf of and as instructed by Novartis. This may include: name or initials, home or other physical address, cell/mobile or telephone number; photograph and/or any data or information subject to Data Protection Laws. Personal Data includes Special/Sensitive Personal Data as defined below.

"**Data Protection Laws**" – all laws, rules, regulations, and orders of any jurisdiction or subdivision thereof relating to the privacy, security, confidentiality and/or integrity of Personal Data that are applicable to the operations, services or products of Vendor and Novartis, including but not limited to the EU General Data Protection Regulation (2016/679).

"**Data Security Breach**" – (a) the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to or acquisition of or misuse of Personal Data or any media containing Personal Data; (b) the disclosure or use of Personal Data in a manner inconsistent with Data Protection Laws, the Agreement or this Data Protection Exhibit; or (c) any other act or omission that negatively impacts the security, confidentiality, and/or integrity of Personal Data.

"**Data Subject**" – an identified or identifiable person whose Personal Data are Processed, accessed, received, transmitted, deleted, or maintained by the Vendor on behalf of and under the instruction of Novartis. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

"**Data Transfer Agreement**" – means the agreement that formally sets forth standards and requirements for the legal transfer of Personal Data to persons or entities subject to country laws that do not provide adequate data protection consistent with the standards of the European Economic Area ("**EEA**") or Switzerland ("**CH**"). This is also known as the EU Model Clauses or EU Standard Contractual Clauses.

"**Process, Processed, Processing**" – any handling of Personal Data by any means, including, without limitation, collecting, accessing, receiving, using, transferring, retrieving, manipulating, recording, organizing, storing, maintaining, hosting, adapting, altering, possessing, sharing, disclosing (by transmission, dissemination or otherwise making available), blocking, erasing, destroying, selling, or licensing. Reference to "Processing Activity" or "Processing Activities" shall be a reference to the Processing activities carried out pursuant to this Data Protection Exhibit.

"**Special/Sensitive Personal Data**" – an individual's physical, physiological or mental characteristics, racial or ethnic origin, political, ideological, religious opinions or philosophical beliefs, trade union membership, health or medical information including information related to payment for health services, sex life or sexual preference, genetic material or information, human biological samples or cells, unique biometric data, personality profiles. Special/Sensitive Personal Data is a subset of Personal Data.

"**Vendor**" – the performer and provider of the Services under the Agreement as described on the first page of the Agreement.

"**Vendor Subcontractor**" – any third party that assists Vendor in performing its obligations under the Agreement, including an affiliate or direct or indirect subcontractor of Vendor.

C) ADDITIONAL INFORMATION SECURITY REQUIREMENTS

These Additional Information Security Requirements ("**AISRs**") are intended to supplement any other information security requirements that may be contained in the terms and conditions of the Agreement or in any standalone data processing agreement, including without limitation the Minimum Information Security Requirements referenced in the Novartis Supplier Code (such other information security requirements being referred to as "**Baseline Requirements**"). In the case of a conflict between the Baseline Requirements and the AISRs, the stricter requirement (from an information security perspective) shall prevail. The Supplier agrees and acknowledges that the AISRs form part of the Agreement.

In these AISRs the following capitalized expressions shall have the following meanings unless stated otherwise or the context requires otherwise:

"Good Industry Practice" means, the exercise of reasonable skill and care, implementation of industry standards, efficiency, security, promptness, timeliness, diligence, in a professional manner, as expected from a skilled, trained and experienced professional provider of similar services, including but not limited to Security Industry Practice;

"Information Security Controls" means Novartis Minimum Information Security Controls for Suppliers as published on Novartis public internet: https://www.novartis.com/our-company/corporate-responsibility/codes-policies-guidelines and which form part of the Novartis Supplier Code;

"**Novartis Data**" means all data, documents or records of whatever nature (including Personal Data and Novartis Confidential Information) and in whatever form relating to the business of Novartis including details of customers, employees or otherwise, whether subsisting before or after the date of the Agreement and whether created or processed as part of, or in connection with, the Services or provided by Novartis (or third parties acting on their behalf) to Supplier in connection with the Agreement;

"Novartis Environment" means any Novartis system, Novartis data center, 3rd party system owned by or licensed to Novartis, infrastructure managed by Novartis, Novartis Affiliate or Novartis sub-contractor or any other system, interface or infrastructure as notified by Novartis from time to time;

"Novartis Supplier Code" means the Novartis Supplier Code as referenced in the **Agreement;**

"Third Party Code" means the Third Party Code as referenced in the Agreement;

"**Parties**" means collectively Novartis and Third Party;

“Recovery point objective (RPO)” means the point to which Novartis data must be restored after a disruptive incident occurs. It is an information or data recovery objective that must be achieved in order to allow an activity to resume after a disruptive incident has occurred. RPO refers to a data recovery objective;

“Recovery time objective (RTO)” means the maximum amount of time allowed to resume an activity, recover resources, or provide products and services after a disruptive incident occurs. This target time period must be short enough to ensure that adverse impacts do not become unacceptable. RTO refers to a time period;

“Security Incident” means an actual or imminent event which may impact Novartis Data confidentiality, integrity, availability or resilience;

“Security Industry Practice” means, then-current and applicable practices as defined in the International Organization for Standardization (ISO/IEC) ISO/IEC ISO27001, ISO/IEC 27002:2013, SSAE-16, ISAE3402, National Institute of Standards and Technology (NIST) NIST 800-44, the Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications, and the Center for Internet Security (CIS) Standards (or any successor to these security standards) or any other industry security standards mutually agreed by Parties;

“**Supplier**” includes, unless the context requires otherwise, a reference to the Supplier, its Affiliates and their respective subcontractors and agents;

1. Supplier Assessments: Section 9.5 of Novartis Supplier Code is supplemented as follows:

   1.1 Novartis or nominated third party has the right to monitor, inspect and assess organizational, technical and administrative safeguards maintained by Supplier and any respective measures employed to ensure security, availability, integrity and resilience of Novartis Data including without limitation processes, policies, systems, business continuity test report and infrastructure. Supplier shall provide records and evidence about such measures in form and timescale reasonably requested by Novartis. Supplier shall cooperate and support Novartis or nominated third party in such assessment. Without prejudice to the aforementioned rights of Novartis, Novartis may at any time require the Supplier to prove that it has certificates or audit reports from third parties.

   1.2 Novartis shall have the right to perform detailed technical on-site or off-site assessments evaluating effectiveness of implemented measures to ensure confidentiality, availability, integrity and resilience of the platform. Report(s) from such assessment will be provided to Supplier and Supplier shall remediate gaps as defined in Clause 1.5 of this Exhibit C.

   1.3 Supplier shall ensure penetration and security tests are periodically performed in alignment with Good Industry Practice covering then-current known vulnerabilities

on the environment where Novartis Data is being processed to identify gaps that help increase security.

1.4 No more than once per calendar year (if not triggered by gaps identified during previous penetration testing, independent assessments or another previous Novartis assessment) Novartis may perform or contract to perform, at its own expense, an application and infrastructure penetration test. Report(s) from penetration tests will be provided to Supplier and Supplier shall remediate gaps as defined in Clause 1.5.

1.5 Supplier shall remediate any identified gaps without undue delay but not later than as defined in the remediation plan. The Parties agree that a second occurrence of assessment result in material non-compliance or Supplier's failure to remediate deficiencies according to the remediation plan shall be deemed as an irremediable material breach of the Agreement.

1.6 Third Party shall comply with the Information Security Controls as supplemented and/or amended by these AISRs. Any references to "Supplier" in the Information Security Controls will be treated as referencing Third Party.

2. Services to be provided according recognized standards: Section 1 of Information Security Controls is supplemented as follows:

2.1 Supplier shall process, treat and handle Novartis Data in accordance with Good Industry Practice.

3. Minimum encryption and continuity standards: Sections 2 and 6 of Information Security Controls is supplemented as follows:

3.1 Supplier shall utilize at least 256-bit AES (symmetric) or 4096-bit (asymmetric) RSA encryption or equivalent state of the art cryptographic techniques approved by Novartis and TLS 1.2 at minimum.

3.2 If the Services may adversely impact any Novartis operations, the Parties shall agree and specify in writing, Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) to be ensured by Supplier.

4. Production data processing: Sections 3 and 5 of Information Security Controls is supplemented as follows:

4.1 In case Supplier may process or store Novartis Data, the Parties shall agree and specify in the Agreement location of data and location for which Supplier may be accessing Novartis Data. If the aforementioned locations are not specified in the Agreement, it will be understood that these must be consistent with the type of stored data and with reasonable security measures and, in any case, in strict compliance with the applicable regulations.

4.2 Supplier shall process production Novartis Data only in: (a) a secure production environment; or (b) any other mutually agreed environment where security measures are equivalent as in the applicable production environment.

5. Novartis Environment: Sections 4, 7 and 15 of Information Security Controls is supplemented as follows:

5.1 Supplier acknowledges and accepts that any interface, connection or interaction with Novartis Environment shall be done only after documented approval from Novartis (which may already be included as part of this Agreement). Such connection to Novartis Environment shall be maintained, protected and tested in line with Security Industry Practice as mutually agreed between the Parties and connection may be terminated or requested to be terminated by Novartis at any time at its sole discretion.

5.2 Supplier shall ensure that no: (a) viruses or other harmful code intended to disable, damage or provide unauthorized access; or (b) code used to keylogging or any software used to enforce licensing restrictions; or (c) any other code providing functionality not intentionally accepted by Novartis in writing is infiltrated into the Novartis Environment by Supplier or it personnel (including without limitation, in all of the three aforementioned cases as a result of failure to observe the requirements as defined in Clause 5.1 of this Exhibit.

5.3 Supplier shall extract and access only data as defined by Novartis and shall inform immediately Novartis if Supplier is able to access or extract other data than specified by Novartis. Such notification should follow the provisions on Security Incident notification as defined in Clause 8 of this Exhibit.

6. Supplier personnel with access to Novartis Environment: Section 8 of Information Security Controls is supplemented as follows:

6.1 In the event that any Supplier personnel: (i) receives a Novartis issued badge (or other access mechanism) providing them with access to Novartis premises; (ii) a personalized Novartis network access account (e.g. a Novartis 5-2-1 account) Novartis laptop, or (iii) a Novartis e-mail account, or (iv) other type of access to Novartis Environment, Supplier shall ensure that such Supplier personnel shall follow any applicable information security policies of Novartis and participate in Novartis trainings at no costs to Novartis. Supplier shall notify Novartis without

undue delay of any changes to the status of Supplier's or Supplier subcontractor's personnel that may affect the right to access to Novartis Environment. Such status changes may include without limitation termination of personnel's employment relationship, change in area of work/responsibilities or termination of subcontractor's engagement.

7. Return of Novartis Data: Section 10 of Information Security Controls is supplemented as follows

   7.1 As an alternative option to the disposal of Novartis Data as per section 10 of Information Security Controls, Novartis shall have the right to receive such Novartis Data in the form and timescale specified by Novartis.

8. Security Incidents: Section 12 of Information Security Controls is supplemented as follows:

   8.1 Supplier shall monitor, analyze and respond to Security Incidents as defined in this Clause 8. Supplier will engage and report to Novartis if there is any actual or suspected Security Incident which could impact Novartis or Novartis Data. Confirmed Security Incident is always considered as priority 1 incident.

   8.2 Novartis contact for reporting Security Incident identified by Supplier: Phone: +420 225 775 050 (backup number: +420 225 850 012), Email: soc@novartis.com.

   8.3 Supplier contact for reporting Security Incident identified by Novartis: contact person identified in the contract or, failing that, the signatory of the contract.

   8.4 Supplier shall follow as a minimum the following Security Incident management process:

   8.4.1 Supplier shall notify Novartis without undue delay, but not later than twenty four (24) hours after Security Incident was evidenced

   8.4.2 If Security Incident is confirmed, Supplier shall take appropriate actions to minimize further exposure of Novartis Data in consultation with Novartis without undue delay, but not later than in forty eight (48) hours after Security Incident was confirmed, where such actions shall include without limitation:

   8.4.2.1 stopping inappropriate access or any other inappropriate activities with Novartis Data;
   8.4.2.2 defining remediation actions to prevent repetition of such Security Incident;
   8.4.2.3 restoring normal operations of the Services; and
   8.4.2.4 informing Novartis periodically on progress of remediation actions.

After above actions preventing repetition of Security Incident are implemented, Supplier shall provide a written report to Novartis detailing actions performed and safeguards implemented.

9. Patch management: Section 14 of Information Security Controls is supplemented as follows

9.1 Supplier shall monitor available patches, evaluate, test and implement them in a timely manner for any systems involved in support of the Services or in the processing of Novartis Data.

9.2 If a patch has been evaluated to not be applied, Supplier shall ensure: a) alternative controls or safeguards are implemented to ensure the confidentiality, integrity and availability for any systems involved in support of the Services or in the processing of Novartis Data; or b) evidence indicating the evaluation, the risk it potentially imposes and the reason for the decision.

Breach of these AISRs shall be considered as a material breach of the Agreement and shall be subject to the termination provisions of the Agreement in respect of material breach.