Novartis Binding Corporate Rules (BCR)

(*Binding Corporate Rules* for the transfer of personal information outside the EEA+ under Article 47 GDPR and Article 16 (2) (e) FADP)

Terms capitalized in these Binding Corporate Rules ("BCR") are defined in these BCR, in the Glossary (Appendix 2) and in Appendix 1 concerning Data Subjects covered by these BCR.

Introduction

At Novartis, our mission is to discover new ways to improve and extend people's lives. We use science-based innovation to address some of society's most challenging healthcare issues. We discover and develop breakthrough treatments and find new ways to deliver them to as many people as possible.

Our Code of Ethics contains the fundamental principles and commitments concerning ethical business conduct including the commitment to the right to privacy and protection of Personal Information of our Employees and Other Data Subjects, including those participating in biomedical research as defined in Appendix 1.

The Novartis Ethical Use of Data and Technology Policy, effective as of 1 November 2024, and its supporting documentation, establish a common standard on the appropriate protection of Personal Information within Novartis and its affiliates ("Novartis," "Novartis Group" or where appropriate "Novartis Companies"). It provides general principles regarding the right of individuals to privacy and to reasonable safeguards of their personal information. We treat Special Categories of Personal Information, including medical data with special care.

These BCR complement the current Novartis Ethical Use of Data and Technology Policy and its supporting documentation and standard operating procedures. These documents are put in place in accordance with EEA+ Data Protection Law. In cases of contradictions between these BCR and Novartis guidelines regulating cross-border data transfers, these BCR will prevail for Novartis Companies that are bound by these BCR.

1. Purpose and scope of application

The purpose of these BCR is to ensure an adequate level of protection for Transfers of Personal Information within the Novartis Group, from a Novartis Company acting as a Controller to a Novartis Company acting as a Controller or as a Processor.

These BCR apply to the Transfer of Personal Information that is subject to EEA+ Data Protection Law (or that was subject to EEA+ Data Protection Law prior to the Transfer of such Personal Information to a Novartis Company outside of the EEA+) to a Novartis Company in a country for which there is no Adequacy Decision.

These BCR apply to Personal Information of Novartis Employees, Consumers**,** Business Customers and Other Stakeholders, Vendors and Business Partners, and Data Subjects participating in or contributing to research and Pharmacovigilance, as defined in the Glossary in Appendix 2 and specified in Appendix 1.

2. Guarantees of application

2.1 Binding upon Novartis Companies

These BCR constitute Binding Corporate Rules for the Transfer of Personal Information outside the EEA+ under Article 47 GDPR and Article 16 (2) (e) FADP and are legally binding and shall apply to and be enforced by all Novartis Companies that have signed the BCR Intercompany Agreement (Appendix 3), including their Employees.

Each Novartis Company that signs the BCR Intercompany Agreement is responsible for administering and overseeing the implementation of these BCR within their respective organizations, including making these BCR binding upon their Employees.

No Transfer of Personal Information must be made to a Novartis Company, unless such Novartis Company is bound by these BCR and can ensure compliance with the same.

Any Novartis Company acting as Data Importer which for any reason is not able to comply with these BCR, or is in breach of this BCR, should promptly notify the Novartis Company acting as Data Exporter. In this case, the Novartis Company acting as Data Exporter should suspend the Transfer. Furthermore, the Novartis Company acting as Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Information that has been Transferred under the BCR in its entirety, where:

i. the Novartis Company acting as Data Exporter has suspended the Transfer, and compliance with this BCR is not restored within a reasonable time, and in any event within one month of suspension; or
ii. the Novartis Company acting as Data Importer is in substantial or persistent breach of these BCR; or
iii. the Novartis Company acting as Data Importer fails to comply with a binding decision of a competent court or competent Supervisory Authority regarding its obligations under these BCR.

The Novartis Company acting as Data Importer should certify the deletion of the data and of any copies thereof to the Novartis Company acting as Data Exporter.
Until the data is deleted or returned, the Novartis Company acting Data Importer should continue to ensure compliance with these BCR.
In case of local laws applicable to the Novartis Company acting as Data Importer that prohibit the return or deletion of the Transferred Personal Information, the Novartis Company acting as Data Importer should continue to ensure compliance with these BCR, and will only process the Personal Information to the extent and for as long as required under that local law.

2.2 Availability of the BCR

Data Subjects have the right to easily access the BCR. Each Novartis Company that signs the BCR Intercompany Agreement is responsible for making information on the rights of the Data Subjects as covered by the BCR, including the means to exercise those rights, readily available to the Data Subjects. The BCR will be published on the Novartis website and intranet.

2.3 Binding upon Employees

Employees are bound by these BCR and have a duty to comply with the obligations set out herein.

Employees who violate these BCR may be subject to disciplinary procedures, as defined by the respective Novartis Company.

2.4 Role of Novartis Pharma S.A.S.

Novartis has appointed Novartis Pharma S.A.S. ("Novartis France") as the Novartis Company within the EEA+ with delegated data protection responsibilities for the purposes of these BCR. These responsibilities include the oversight, coordination and implementation of the BCR, and accepting liability for breaches of the BCR by Novartis Companies outside the EEA+ as described in more detail in section 7 of these BCR.

3. Principles applicable to the Processing of Personal Information

3.1 Obligations of Controllers

A Novartis Company acting as a Controller must comply with the following principles when Processing Personal Information:

(i) **Transparency**:

a. Collect and Process Personal Information in a fair, lawful and transparent manner (lawfulness, fairness and transparency);

b. Notice: Ensure that Data Subjects are informed of the Processing and Transfer of their Personal Information (transparency) in accordance with EEA+ Data Protection Law and, obtain the Data Subject's consent, where appropriate. The notice must include the information required by Articles 13 and 14 of the GDPR and Article 19 FADP, including as appropriate:

i. the identity and contact details of the Controller(s);
ii. the contact details of the Group Data Protection Officer (or other competent data protection officer);
iii. for which purposes and on what legal basis the Personal Information will be Processed and Transferred;
iv. where the Processing is based on the Controller's legitimate interest, the description of the interest pursued;
v. the recipients or categories of recipients of the Personal Information;
vi. where applicable, the fact that the Controller intends to Transfer Personal Information outside of the EEA+, and whether the Transfer destination is covered by an Adequacy Decision, or the reference to the appropriate safeguards, such as Model Clauses, and how to obtain a copy of them or where they have been made available;
vii. the period for which Personal Information will be stored, or if it is not possible, the criteria used to determine this period;
viii. information about Data Subjects' rights under the BCR, including third-party beneficiary rights, and the means to exercise those rights;
ix. where the Processing is based on Data Subjects' consent, the right to withdraw consent at any time, without affecting the lawfulness of the Processing or the lawfulness of Processing not based on consent;
x. the right to lodge a complaint before the competent Supervisory Authority under Section 7.2;

xi. whether the provision of Personal Information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Information and the possible consequences of failure to provide such Personal Information;
xii. the existence of automated decision-making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;
xiii. where the Personal Information have not been obtained directly from the Data Subject, the description of the categories of Personal Information and the source of the Personal Information.

(ii) **Legitimate and meaningful Processing**:

a. Process only Personal Information that is relevant and not excessive to the purposes (data minimisation);
b. Ensure that Personal Information is Processed lawfully by ensuring an appropriate legal basis exists under EEA+ Data Protection Law, in accordance with Novartis Ethical Use of Data and Technology Policy and any relevant specifications documents and local Standard Operating Procedure(s) if applicable; and
c. Ensure that the Processing of Special Categories of Personal Information meets one of the exceptions provided by EEA+ Data Protection Law, and Personal Information relating to criminal convictions and offences shall be only processed in accordance with the applicable EEA+ Data Protection Law, and following relevant rules and guidance in Novartis Ethical Use of Data and Technology Policy, in any other relevant documents and in local Standard Operating Procedure(s).

(iii) **Responsible and sustainable Processing**:

a. Process and Transfer Personal Information only for specific, explicit and legitimate business or legal purposes and no further Processing of Personal Information in a manner incompatible with those purposes (purpose limitation);
b. Privacy by design and by default: Take into account the right to data protection when developing and designing products, services and application (privacy by design) and ensure that, by default, only Personal Information that is necessary for each specific purpose of the Processing is processed (privacy by default);
c. Accuracy: Ensure that Personal Information is accurate, complete and, where necessary, kept up to date;
d. Data Subject Rights: Establish a process to provide for Data Subjects' rights under EEA+ Data Protection Law. This includes the right of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, data portability, objection to the Processing, the right to request an independent authority for judicial protection and the right not to be subject to decisions solely based on automated Processing, including profiling;
e. Transfers: Disclose Personal Information only to other Novartis Companies and third parties that are either bound by these BCR (only applicable to Novartis Companies) or are established in countries providing an equivalent level of data protection as determined by an Adequacy Decision or meet any other legal means to Transfer Personal Information as provided by EEA+ Data Protection Law;
f. Processors: Prior to disclosing Personal Information to a Novartis Company acting as a Processor or a third party acting as Processor, provide instructions to the Processor regarding the Processing of the Personal Information and

enter into written contracts that include the requirements established by the applicable EEA+ Data Protection Law and in paragraph 3.2 of these BCR;

g. Third parties: Ensure that procedures are in place so that Novartis Companies or third parties authorized to have access to the Personal Information, including Processors, will respect and maintain the confidentiality and security of the Personal Information appropriately and comply with the principles as set out in these BCR;
h. Automated decision-making: Where making decisions solely based on automated Processing that significantly affect the Data Subject, including profiling, provide suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, and providing to the Data Subject the right to have the decision manually reviewed and to provide his/her point of view.

(iv) **Security, Integrity and Quality**:

a. Novartis shall give its Employees and other staff access to Personal Information only to the extent necessary to serve the Processing and to perform their jobs. Novartis shall impose confidentiality obligations on Employees and other staff with access to Personal Information.
b. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subject, take appropriate technical and organisational measures to protect Personal Information from accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure, access or other Processing ("**Security Breach**"), including, where appropriate, reinforced measures to ensure the security of Special Categories of Personal Information (integrity and confidentiality);
c. Security Breach management: Establish a process in order to document Security Breaches, make such documentation available to the Competent Supervisory Authority upon request (including facts, effects and remedial action), and escalate Security Breaches without undue delay internally to the liable Novartis Company, the Group Data Protection Officer as well as to the Novartis Company acting as Controller when a Novartis Company acting as a Processor become aware of the Security Breach, and, if required by applicable EEA+ law, notify the competent Supervisory Authorities without undue delay, and where feasible no later than 72 hours after having become aware of the Security Breach, and without undue delay Data Subjects, where the Security Breach is likely to result in a high risk to their rights and freedoms in line with the requirements of Article 34 GDPR.

(v) **Minimal retention**: Ensure that Personal Information is retained only for so long as necessary for the purpose for which it is Processed, unless overriding legal or internal retention schedules require a longer or shorter retention period (storage limitation).

3.2 Processors

Transfers to third party Processors, as well as internal Processors, by a Novartis Controller must be on the basis of a validly entered into written contract that complies with the requirements of EEA+ Data Protection Law ("**Processor Contract**"). The Processor Contract must include the following provisions:

(i) the Processor shall Process Personal Information only for the purposes authorized by the Controller and in accordance with the Controller's documented instructions, including on Transfers of Personal Information to any subcontractors not covered by an Adequacy Decision, unless the Processor is required to do so under mandatory requirements applicable to the Processor and notified to Novartis;
(ii) the Processor shall keep the Personal Information confidential and shall impose confidentiality obligations on staff with access to Personal Information;
(iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Information;
(iv) the Processor shall only permit subcontractors to Process Personal Information in connection with its obligations to the Controller (a) with the prior specific or generic consent of the Controller and (b) based on a validly entered into written or electronic contract with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Processor under the Processor Contract and provided that the Processor remains liable to the Controller for the performance of the subcontractors in accordance with the terms of the Processor Contract. In case the Controller provides generic consent for involvement of subcontractors, the Processor shall provide notice to the Controller of any changes in its subcontractors and will provide the Controller the opportunity to object to such changes based on reasonable grounds;
(v) the Controller should be able to verify the above-mentioned security measures taken by the Processor (a) by an obligation of Processor to subject its relevant facilities used to Process Personal Information to audits and inspections by the Controller, a third party on behalf of the Controller or any relevant public authority; or (b) by means of a statement issued by a qualified independent third party assessor on behalf of Processor certifying that the facilities of the Processor used for the Processing of Personal Information comply with the requirements of the Processor contract;
(vi) the Processor shall promptly inform the Controller of any security incident involving Personal Information;
(vii) the Processor shall promptly and appropriately deal with:
    a) requests for information necessary to demonstrate compliance of the Processor with its obligations under the Processor Contract and will inform the Controller if any instructions of the Controller in this respect violate applicable law;
    b) requests and complaints of Data Subjects as instructed by Controller;
    c) requests for assistance of the Controller as reasonably required to ensure compliance of the Processing of the Personal Information with EEA+ Data Protection Law, and Processor shall assists the Controller in ensuring compliance with the obligations relating to security of Personal Information, notification of Security Breaches, Data Protection Impact Assessment, taking into account the nature of Processing and the information available to the Processor; and
    d) upon termination of the Processor contract, the Processor shall, at the option of the Controller, return the Personal Information and copies thereof to the Controller or shall securely delete such Personal Information, except to the extent the Processor contract or EEA+ Data Protection Law provides otherwise.

A Novartis Company that wishes to Transfer Personal Information to a third-party Processor must select a third-party offering sufficient guarantees of their ability to ensure the security of Personal Information.

3.3 Transfers to third parties located in a country outside the EEA+ for which there is no Adequacy Decision

The Novartis Company that wishes to Transfer Personal Information to a third party located in a country established outside the EEA+ for which there is no Adequacy Decision, must implement appropriate safeguards for Transfers under EEA+ Data Protection Law, such as by (i) entering into appropriate Model Clauses, or (ii) if entering into Model Clauses is not possible, relying on a derogation under EEA+ Data Protection Law, prior to the Transfer of any Personal Information.

4. Awareness and training program

Novartis commits to providing basic training on privacy and data protection, including the requirements under the BCR, to its Employees, and specific trainings to Employees who have regular access to and Process Personal Information, as well as those who develop tools and systems for the Processing of Personal Information. Where relevant, the training will also be provided to other persons who Process Personal Information as part of their respective duties or responsibilities using Novartis information technology systems or working primarily from Novartis' premises. The specialized training covers data protection standards and requirements specific to their areas of work. The training shall be organized in accordance with the Data Privacy Training Program as set out in Appendix 4.

5. Compliance, monitoring and audit program

5. 1 Privacy Organization

Novartis' approach to managing data privacy is based on the accountability principle. Novartis Companies are responsible and accountable for compliance with these BCR, local data privacy laws and regulations, and are responsible to drive the implementation of the Novartis Group privacy program ("Group Privacy Program") at country level. The Group Privacy Program aims to support local activities and to ensure compliance of cross-border projects, including international data flows in connection with outsourcing activities and global databases.

In order to ensure compliance with privacy laws, regulations and our standards, we strive to integrate privacy principles and requirements into our processes and systems and to promote accountability throughout the Novartis Group through awareness and training programs.

Novartis has established a Global Privacy, Digital and AI (DPDAI) Compliance Organization under the Ethics, Risk & Compliance function, composed of DPDAI Heads at country level, who report indirectly to the Global DPDAI Head, as described in Appendix 6.

5.2 Monitoring and Audit Program

Novartis commits to conducting regular privacy compliance assessments to ensure that the privacy standards including the BCR are effectively applied. These assessments may be conducted in multiple ways:

(i) As required as part of internal procedures, Novartis Companies will perform data protection impact assessments where a Processing is likely to result in a high risk to the rights and freedoms of a Data Subject. Where the assessment shows that, despite mitigating measures taken by Novartis, the Processing still presents a residual high risk for the rights and freedoms of Data Subjects, the competent Supervisory Authority will be consulted prior to such Processing taking place.

(ii) Each Novartis Company that processes Personal Information will regularly be subject to pre-defined privacy-related controls under the direction of the Corporate DPDAI Team. The results, including a remediation plan, will be documented and reported to the Global Head DPDAI. Findings of the privacy controls and remediation plan shall be available to the Competent SA on request.

(iii) Novartis Internal Audit will audit business processes at regular intervals based on risk assessment, and in any case no less frequently than once every three years, procedures and systems that involve the processing of Personal Information for compliance with the BCR. Novartis Internal Audit will be guaranteed independence as to the performance of these audits. These audits cover all aspects of the BCR, including methods of ensuring that corrective actions will take place. The audits shall be carried out in the course of the regular activities of Novartis Internal Audit as approved by the Audit and Compliance Committee (ACC) or at the request of the Global Head DPDAI. The Global Head DPDAI may request to have an audit as specified in this Section conducted by an external accredited auditor, who will be guaranteed independence as to the performance of their duties. The findings of these audits, including a remediation plan, shall be reported to the management at group, divisional and business level, including the Executive Committee of Novartis, the ACC, as well as to the Global Head DPDAI. A copy of the full audit results relating to compliance with the BCR shall be provided to the Competent SA upon request.

(iv) Novartis has established a DPDAI Review & Remediation function under Corporate Ethics, Risk & Compliance Assurance, which conducts periodic monitoring reviews of the different Novartis organizational units in order to identify and oversee the remediation of potential non-compliance in the implementation of the Novartis Data Privacy program and of the BCR.

(v) Novartis maintains readily available records of Processing activities in line with the requirements of EEA+ Data Protection Law, and in particular art. 30.1 GDPR. These records will include (i) name and contact details of the Novartis Company that is the Controller of Personal Information, (ii) the purposes for Processing, (iii) a description of the categories of Personal Information and categories of Data Subjects (iv) information about Transfers of Personal Information, and where possible, (v) retention periods, and (vi) a general description of security measures. A copy of this information will be provided to the Competent SA on request. Novartis also maintains readily available records of Processing activities for Novartis Companies acting as Data Processors, in line with the requirements of EEA+ Data Protection Law, and in particular art. 30.2 GDPR. These records will include (i) the name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting; (ii) the categories of Processing carried out on behalf of each Controller; (iii) where applicable, Transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable

safeguards; (iv) where possible, a general description of the technical and organizational security measures referred to in the GDPR.

6. Complaint handling procedure

If a Data Subject believes that there has been a violation of these BCR, he or she should report the concern to the DPDAI Team (global.privacy_office@novartis.com), designated by Novartis in accordance with article 37 of the GDPR, in accordance with the procedure described in Appendix 5.

7. Liability and Third Party Beneficiary Rights

7.1. Third Party Beneficiary Rights

The rights contained in this section are in addition to, and shall not prejudice, any other rights or remedies that Data Subjects may otherwise have under EEA+ Data Protection Law or applicable laws.

If Novartis violates these BCR with respect to its Processing of a Data Subject's Personal Information as a Controller, the affected Data Subject can, as a third-party beneficiary, enforce sections 2.2, 3, 6, 7, 8.2, 9, 10.2, 10.3 and Appendix 5 of these BCR, with appropriate reference as needed to the information included in Appendixes 1, 2 and 7.

Data Subjects are encouraged to first follow the complaint handling procedure which shall support Data Subjects to address any privacy complaint internally. Data Subjects are however free to lodge a complaint directly with the competent SAs or to bring a legal claim before the competent courts under section 7.2 at any time.

7.2. Jurisdiction and Liability

In case a Data Subject has a claim under section 7.1, the Data Subject may, at his or her choice, submit a complaint under this section with the SA in the Member State of the Data Subject's habitual residence, place of work or place of the alleged infringement, or to bring a legal claim before the competent courts (as applicable):

(i) in the EEA+ country where the Novartis Company being the Controller of the relevant Personal Information is established, against such Company;

(ii) in the EEA+ country where the Data Subject has his/her habitual residence or place of work;

(iii) in France, against Novartis France. Novartis France shall ensure that adequate steps are taken to address violations of these BCR by a Novartis Company. Novartis France shall abide by the advice of the Competent SAs issued on the interpretation and application of these BCR.

Data Subjects have the right to be represented by a non-for-profit body, organization or association if, and to the extent, applicable law permits such representation.

Novartis France accepts liability for a breach by a Novartis Company located outside the EEA+, although Novartis France may assert any defense that such Novartis Company or the third party Processor could have asserted.

7.3. Right to Claim Damages and Burden of Proof

In case a Data Subject has a claim under section 7.1, such Data Subject shall be entitled to compensation of material and non-material damages suffered by the Data Subject resulting from a violation of these BCR to the extent provided for by applicable EEA+ law, in accordance with section 7.2.

In order to bring a claim for damages, the Data Subject must demonstrate that he or she has suffered the relevant damages and to establish facts which show it is plausible that the damage has occurred because of a violation of these BCR. Novartis must then prove that the damages suffered by such Data Subject are not attributable to Novartis or a Processor or assert other applicable defenses.

8. Mutual assistance and cooperation

8.1 Mutual assistance

Novartis Companies bound by the BCR commit to cooperate and assist each other to appropriately deal with:

(i) Requests from the competent Supervisory Authorities concerning the application of the BCR;

(ii) Requests and investigations from other public authorities where this may impact the application of the BCR;

(iii) Requests and complaints from the Data Subjects.

The Novartis Company that is responsible for the Processing to which a request, complaint or claim relates, shall bear all costs involved and reimburse Novartis France.

8.2 Cooperation with the competent Supervisory Authorities

Novartis Companies bound by the BCR commit to cooperate with the Competent Supervisory Authorities, particularly by diligently responding within a reasonable time frame to their requests concerning the interpretation and application of the BCR and to take into account their advice and recommendations in this respect.

Novartis Companies bound by the BCR commit to accept to be inspected and/or audited, including where necessary, on-site, by Competent Supervisory Authorities for compliance with these BCR. They also commit to provide the Competent Supervisory Authority, upon request, with any information about the processing operations covered by the BCR.

Novartis will abide by the decisions of the Competent SA on issues related to the BCR. Any disputes relating to the competent SA's exercise of supervision of compliance with the BCR will be resolved by the courts of the Members State of that SA.

9. Amendments of the BCR

Novartis may amend the BCR if it is justified by a Legitimate Business Purpose, if the applicable EEA+ Data Protection laws, regulations and regulatory guidance, and case law have changed, or if Supervisory Authorities have requested certain changes to be made. Decisions will be taken by the Data Privacy, Digital & AI Leadership Team.

Significant changes that have a material impact on the protection offered by these BCR or on the BCR itself will be communicated promptly by the Head DPDAI Region Europe to Novartis Companies bound by the BCR and to the Lead SA. The Head DPDAI Region Europe will also be responsible for coordinating Novartis' responses to questions of the Lead SA in respect thereof. When reporting any changes to the Lead SA, Novartis will include a brief explanation of the reasons justifying the changes. Other non-material changes to the BCR or changes to the list of the Novartis Companies bound by the BCR will be reported without undue delay to Novartis Companies, and once a year to the Lead SA, with a brief explanation for such changes. Novartis will publish on its website without undue delay any update version of the BCR and of the list of BCR members under Appendix 7.

In addition, Novartis has taken steps so that a country DPDAI Head is appointed to take the responsibility for keeping an updated list of Novartis Companies bound by the BCR, keeping track of and recording updates to the BCR and ensuring that the necessary information is provided to the Data Subjects and to the Competent SA upon request.

10. Application of laws

10.1 Application of laws

Data Subjects shall be entitled to enforce any rights and remedies they may have under applicable local laws. Where the applicable local law provides more protection than these BCR, the local law shall apply. Where these BCR provide more protection than applicable local law or provide additional safeguards, rights or remedies for Data Subjects, these BCR shall prevail.

10.2 Conflict with local applicable laws

Novartis Companies will use the BCR as a tool for Transfers only where they have assessed that the law and practices in the destination country outside of EEA+ applicable to the processing of the Personal Information by the Novartis Company acting as Data Importer, including any requirements to disclose Personal Information or measures authorizing access by public authorities, do not prevent the importing Novartis Company from fulfilling its obligations under these BCR. These requirements also apply to onward Transfers, which are Transfer from a Data Importer to another Data Importer or a third party established in an non-EEA+ country.
In assessing the laws and practices of the non-EEA+ country which may affect the respect of the commitments contained in these BCR, the Novartis Companies should take into due account, in particular, the following elements:

(i) The specific circumstances of the Transfers, including:

a. purposes for which the Personal Information are Transferred and Processed;
b. types of entities involved in the Processing;
c. economic sector in which the Transfer occurs;
d. categories and format of the Personal Information Transferred;
e. location of the Processing, including storage; and
f. transmission channels used.

(ii) The laws and practices of the non-EEA+ country of destination relevant in light of the circumstances of the Transfer, including those requiring to disclose data to public authorities, and those providing for access to these data during the transit between the country of the Novartis Company acting as Data Exporter and the country of the Novartis Company acting as Data Importer, as well as the applicable limitations and safeguards, or authorizing access by such authorities and those providing for access to this Personal Information.

(iii) Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these BCR, including measures applied during the transmission and to the Processing of the Personal Information in the country of destination.

Where any safeguards in addition to those envisaged under the BCR should be put in place, Novartis France, and the relevant DPDAI Head will be informed and involved in such assessment.

Novartis shall document appropriately such assessment, as well as the supplementary measures selected and implemented. They should make such documentation available to the competent SAs upon request.

Any Novartis Company acting as Data Importer shall promptly notify the Data Exporter if it has reasons to believe that the Data Importer is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR, including following a change in the laws in the third country or a measure (such as a disclosure request). This information should also be provided to Novartis France. In this case, the Novartis Company acting as Data Exporter, along with Novartis France and the relevant DPDAI Head or Function, should commit to promptly identify supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Novartis Company acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the BCR. The same applies if a Novartis Company acting as Data Exporter has reasons to believe that a Novartis Company acting as its Data Importer can no longer fulfil its obligations under this BCR-C.

Where the Novartis Company acting as Data Exporter, along with Novartis France and the relevant DPDAI Head, assesses that the BCR cannot be complied with for a Transfer or set of Transfers, or if instructed by the Competent SAs, it commits to suspend the Transfer or set of Transfers at stake, as well as all Transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the Transfer is ended.

Following such a suspension, the Novartis Company acting as Data Exporter has to end the Transfer or set of Transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Information that have been Transferred prior to the suspension, and any copies thereof, should, at the choice of the Novartis Company acting as Data Exporter, be returned to it or destroyed in their entirety.

The relevant DPDAI Head will inform all other Novartis Companies of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of Transfers is carried out by any Novartis Company or, where effective supplementary measures could not be put in place, the Transfers at stake are suspended or ended.

Novartis Companies acting as Data Exporters shall monitor, on an ongoing basis, and where appropriate in collaboration with Novartis Companies acting as Data Importers, developments in the third countries to which the Data Exporters have Transferred Personal Information that

could affect the initial assessment of the level of protection and the decisions taken accordingly on such Transfers.
Where there is a conflict between applicable local law and these BCR, including where a legal requirement to Transfer Personal Information conflicts with EEA+ Data Protection Law, the Global Head DPDAI must be consulted to determine how to comply with these BCR and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Novartis Company. The Global Head DPDAI may seek the advice of the Lead SA or another competent public authority.

10.3 Government Access to Personal Information

Subject to the following paragraph, a Novartis Company acting as Data Importer will promptly inform the Novartis company acting as Data Exporter, and where possible, the data subjects, if Novartis: (i) receives a legally binding request under the laws of the country of destination, or of another non-EEA+ country, for disclosure of Personal Information from a law enforcement authority or state security body ("**Disclosure Request**"); or (ii) becomes aware of any direct access by public authorities to Personal Information Transferred pursuant to these BCR ("**Access**"). The Novartis company acting as Data Importer will provide to the Novartis company acting as Data Exporter as much relevant information as possible on the Access or the Disclosure Request at regular intervals. Notifications of a Disclosure Request shall include information about the data requested, the requesting body, the legal basis for the disclosure, and the response provided. If the Novartis company acting as Data Importer is or becomes partially or completely prohibited from providing the aforementioned information, it will, without undue delay, use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Novartis Company acting as Data Exporter.

The Data Importer will preserve the abovementioned information for as long as the Personal Information is subject to the safeguards provided by the BCR, and shall make it available to the Competent SAs upon request.

The Novartis Company acting as Data Importer will provide the Novartis Company acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Novartis Company acting as Data Importer is or becomes partially or completely prohibited from providing the Novartis Company acting as Data Exporter with the aforementioned information, it will, without undue delay, inform the Novartis Company acting as Data Exporter accordingly.

Novartis will review the legality of the Disclosure Request and will challenge it if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful, and will pursue possibilities of appeal. When challenging the request, Novartis will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. Novartis will not disclose the Personal Information requested until required to do so under the applicable procedural rules. Novartis will document its legal assessment and any challenge to the Disclosure Request and, to the extent permissible under the laws of the country of destination, make the documentation available to the Novartis Company acting as Data Exporter. Upon request, the Novartis Company acting as Data Importer will also make the documentation available to the Competent SA.

Novartis will provide the minimum amount of information permissible when responding to a Disclosure Request, based on a reasonable interpretation of the request. In any event, any sharing by Novartis of Personal Information in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

This section does not apply to requests received by Novartis from other government agencies in the normal course of its activities, which Novartis can continue to provide in accordance with applicable law.

11. Entry into force and Termination

The BCR has entered into force on July 3, 2012 and has subsequently been updated in 2018, 2019 and 2024. The BCR are applicable to the Novartis Companies upon signing the BCR Intercompany Agreement (Appendix 3).

Any changes or updates to the BCR shall enter into force after they are approved by the DPDAI Leadership Team, communicated to the relevant Novartis Companies and published on the Novartis website and intranet.

Any request, complaint or claim of a Data Subject involving the BCR shall be judged against the version of the BCR as it was in force at the time that the event giving rise to the request, complaint or claim took place.

A Novartis Company acting as Data Importer which ceases to be bound by these BCR because they are no longer part of the Novartis Group of Companies should seek Novartis instructions on whether to return or delete the Personal Information in its possession.

If the Novartis Company acting as Data exporter and Novartis Company acting as Data Importer agree that the data may be kept by the Novartis Company acting as Data Importer, protection must be maintained in accordance with Chapter V GDPR.

12. Appendices

The attached Appendices form an integral part of the BCR.

Appendix 1: Categories of Data Subjects and Transfer Purposes covered by the BCR
Appendix 2: Glossary of Data Privacy Terms for the purpose of the BCR and the Application
Appendix 3: Template BCR Intercompany Agreement
Appendix 4: Data Privacy Training Program related to the BCR
Appendix 5: Complaint Handling Procedure related to the BCR
Appendix 6: Global Data Privacy, Digital & AI Compliance Organization at Novartis
Appendix 7: List of BCR members

Author and Owner of the BCR: Head Data Privacy, Digital & AI Compliance, Region Europe
Reviewed by: Data Privacy, Digital & AI Compliance Leadership Team

Version History

Effective Date	Owner	Version	CNIL
3 July 2012	Group Data Privacy	1.0	3 July 2012
3 September 2018	Group Data Privacy	2.0	3 September 2018
20 December 2024	Head Data Privacy, Digital & AI Compliance Region Europe	3.0	20 December 2024