Global Data Privacy

Novartis Binding Corporate Rules

Date: 03 September 2018

NOVARTIS

Novartis Binding Corporate Rules (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 Conduct contains the fundamental principles and rules concerning ethical business conduct including the commitment to the right to privacy and protection of Personal Information of our Associates and Other Data Subjects, including those participating in biomedical research as defined in Appendix 1.

The "Novartis Policy on the Protection of Personal Information", approved by the Board of Directors of Novartis AG and effective as of 1 January 2008, and its supporting guidelines, establish a common standard on the appropriate protection of personal information within Novartis AG 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 sensitive personal information and medical data with special care.

These Binding Corporate Rules ("BCR") complement the "Novartis Policy on the Protection of Personal Information" and its supporting guidelines and standard operating procedures ("SOP"). These BCR are intended to ensure an adequate level of protection for the Processing and Transfer of Personal Information of Novartis Associates, 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. These documents are in compliance with Regulation 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 or GDPR) and the Swiss Federal Act on Data Protection. In cases of contradictions between these BCR and Novartis guidelines regulating cross-border data transfers, these BCR will prevail for Companies that are bound by these BCR.

The terms in capital letter used in these BCR are defined in these BCR, in the Glossary (Appendix 2) and in Appendix 1 concerning Data Subjects covered 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.

These BCR apply to:

- The Transfer of Personal Information from Novartis Companies operating as Controllers in the EEA or Switzerland ("Data Exporters") to other Novartis Companies established outside the EEA and Switzerland ("Data Importers"), and
- The Onward Transfer of Personal Information from Data Importers to other Data Importers.

2. Guarantees of application

2.1 Binding upon Novartis Companies

These BCR are binding obligations upon each and every Novartis Company that signs the BCR Intercompany Agreement (Appendix 3).

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

2.2 Availability of the BCR

Each Novartis Company that signs the BCR Intercompany Agreement is responsible for making the rights of the Data Subjects as covered by the BCR readily available to the Data Subjects. Third party beneficiary rights and the procedures to exercise these rights will be published via the Novartis internet and intranet.

2.3 Binding upon Employees

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

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

3. Principles applicable to the collection and Processing of Personal Information

3.1 Obligations of Controllers

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

(i) Collect and Process Personal Information by fair and lawful means;

(ii) 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 data which are necessary for each specific purpose of the processing are processed (privacy by default);

(iii) Process and Transfer Personal Information only for specific and legitimate business or legal purposes and no further Processing of Personal Information in a manner incompatible with those purposes (purpose limitation);

(iv) Collect and Process only Personal Information that is relevant and not excessive to the purposes (proportionality and data minimisation);

(v) Ensure that Personal Information is accurate, complete and, where necessary, kept up to date;

(vi) Ensure that Personal Information is retained only for so long as necessary for the purpose for which it was collected, unless overriding legal or internal retention schedules require a longer or shorter retention period;

(vii) Where required by local law, ensure that Data Subjects are informed of the Transfer of their Personal Information and obtain the Data Subject's consent where appropriate. The notice must at a minimum include the identity of the Controller(s), how and for which purposes the information will be Transferred and Processed and the categories of data recipients as well as any further information insofar it is required by the GDPR or applicable laws;

(viii) Establish a process to provide for Data Subjects' right to request and obtain information regarding the collection and use of their Personal Information (referred to as "Access"). This includes the right to request limitation of processing or portability of their Personal Information under the conditions set forth in the GDPR, to ask for rectification or removal of their Personal Information if it is incomplete or inaccurate and to object, based on compelling legitimate grounds in their particular situation, to the Processing of their Personal Information. Where the request to limit, remove or object is justified, no Personal Information regarding this Data Subject may be further Processed;

(ix) Protect the confidentiality of Personal Information and take appropriate and reasonable physical, technical and administrative security measures against unauthorized access, accidental loss or damage, misuse and unauthorized alteration and deletion, taking into consideration the state of the art of technology and the cost of implementation;

(x) Establish a process in order to handle data breaches (including notification requirements) without undue delay and within the timeframes set out in GDPR or applicable laws;

(xi) 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 the European Commission and the Swiss Federal Data Protection Commission or meet any other legal means to Transfer Personal Information as provided by the GDPR or Swiss Federal Act on Data Protection;

(xii) Prior to disclosing Personal Information to a Novartis Company or a third party acting as Processor, provide instructions to the Processor regarding the Processing of the Personal Information;

(xiii) 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;

(xiv) Where making decisions solely based on automated processing that significantly affect the Data Subject, provide suitable measures to safeguard the Data Subject's legitimate interest, including implementing a process to review the decision manually and allowing the Data Subject to provide his point of view.

3.2 Obligations of Processors

A Novartis Company acting as a Processor must comply with applicable laws and with the following principles:

(i) Process Personal Information only on behalf and under instructions of the Controller, unless otherwise required by law, in which case the Processor shall promptly notify the Controller. The instructions to the Processors must include the general privacy principles that Processors must comply with and should be documented in a contract or other binding legal act that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the Controller;

(ii) Take appropriate steps to protect Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access through adequate technical, organizational and legal measures and allow the Controller, on request, to conduct an audit of its Processing activities to ensure that the Processor provides such sufficient security protections;

(iii) Disclose Personal Information to other Novartis Companies or third parties for sub-Processing, only if permitted by the Controller;

(iv) Ensure that procedures are in place so that Novartis Companies or third parties authorized to have access to the Personal Information are bound by equivalent obligations as those imposed on the Processor;

In addition, the Processor needs to cooperate with the Controller in order to enable the Controller to comply with its obligations as set out in section 3.1 of these BCR, including responding to Data Subject's requests and the handling of data breaches.

3.3 Transfers to third party Processors

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 and compliance with the obligations set out in section 3.2 (i) - (iv) of these BCR.

The third party Processor established in a country outside the EEA and Switzerland that does not provide an adequate level of data protection, must in addition satisfy the adequacy obligations required under applicable laws, including, but not limited to, entering into appropriate data transfer agreements ("Model Clauses Controller to Processor") prior to receiving any Personal Information.

3.4 Transfers to third party Controllers located in a country outside the EEA and Switzerland that does not provide an adequate level of protection

The Data Exporter in its role as Controller must ensure that a third party Controller located in a country established outside the EEA and Switzerland that does not provide an adequate level of data protection, has provided appropriate safeguards, including, but not limited to, entering into appropriate data transfer agreements ("Model Clauses Controller to Controller") prior to Transferring 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. 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 local data privacy laws and regulations and 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 Organization composed of Heads of Data Privacy who report directly or indirectly to the Global Head of Privacy and Group Data Protection Officer 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 privacy impact assessments in order to determine whether new technologies, information systems and Processing comply with data protection requirements and in order to minimize any impact upon a Data Subjects' privacy.

(ii) Each Novartis Company shall regularly conduct a privacy compliance assessment at the request and direction of the respective Data Privacy Head and report the results including a gap analysis and remediation plan to management, the respective Data Privacy Head and the Global Head Data Privacy. Findings of the compliance assessments shall be available to the relevant Data Protection Authority upon request.

(iii) Novartis Internal Audit shall include key data protection controls as part of internal audits, including audits of Novartis company level controls. Dedicated risk based privacy audits may be conducted by Internal Audit as decided by the Audit and Compliance Committee. The findings of these audits, including a remediation plan, shall be reported to management at group, divisional and business level, including the Chairman of the Board of Novartis AG as well as to the Global Head Data Privacy.

6. Complaint handling procedure

If a Data Subject reasonably and in good faith believes that there has been a violation of these BCR he or she should report the concern to the Group Data Protection Officer (GDPO), 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

Where the Data Subject, who claims to have suffered damage as a direct result of a violation of sections 2.2, 3, 6, 7, 8.2 and 10.2 of these BCR, is not satisfied with the resolution of his complaint, as described in Appendix 5, he can seek to enforce his third party beneficiary rights before the relevant Data Protection Authority or before the courts according to the principles and terms as set out below. The complaint handling procedure shall support Data Subjects to address any privacy complaint internally. Data Subjects are however free to lodge a complaint directly with the Data Protection Authority or the courts as provided by the GDPR and local laws.

As a rule, jurisdiction for any claim, irrespective of whether it is against the Data Exporter or the Data Importer, is in the country where the respective Data Exporter is established.

Where the Data Exporter is established outside of the EEA or Switzerland, but Processes Personal Information in the EEA or Switzerland, jurisdiction shall be in the country where such Processing takes place.

7.1. Controller to Controller Transfers

For Transfers between Data Exporters and Data Importers, both acting as Controllers, the following applies:

7.1.1. A Data Subject, who claims to have suffered damage as a direct result of a violation of sections 2.2, 3, 6, 7, 8.2 and 10.2 of these BCR, can, with regard to his Personal Information, seek to enforce his third party beneficiary rights against the Data Exporter or the Data Importer for their respective violation of their obligations according to these BCR. Liability is limited to actual damage suffered.

7.1.2. In cases involving allegations of breach by the Data Importer:

(i) The Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer.

(ii) If the Data Exporter does not take action described under (i) within a reasonable period (which under normal circumstances would be one month), the Data Subject may enforce his rights against the Data Importer directly.

(iii) The Data Subject is entitled to proceed directly against the Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these BCR. The Data Exporter shall have the burden to prove that it took reasonable efforts.

7.1.3. Each Data Exporter and Data Importer will be exempted from liability under the BCR if it proves that it has not violated the BCR or is not in any way responsible for the damages caused to the Data Subject. The burden of proof remains with the Data Exporter and Data Importer.

7.2 Controller to Processor Transfers

For Transfers between Data Exporters acting as Controllers and Data Importers acting as Processors or sub – Processors, the following applies:

7.2.1 The Data Subject, who can demonstrate that he has suffered damage as a direct result of the Data Exporter’s or Data Importer’s violation of their respective obligations under sections 2.2, 3, 6, 7, 8.2 and 10.2 of these BCR,

is entitled to receive compensation from the Data Exporter for the damage suffered. Liability is limited to actual damage suffered.

7.2.2 If the Data Subject is not able to bring a claim for compensation against the Data Exporter, arising out of a breach by the Data Importer of any of its respective obligations under these BCR, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Subject can enforce its rights against the Data Importer directly. If any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, the Data Subject can enforce its rights against such entity.

7.2.3 Each Data Exporter and Data Importer will be exempted from liability under the BCR if it proves that it has not violated the BCR or is not in any way responsible for the damages caused to the Data Subject. The burden of proof remains with the Data Exporter and Data Importer.

8. Mutual assistance and cooperation with relevant Data Protection Authorities

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 relevant Data Protection 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.

8.2 Cooperation with the relevant Data Protection Authorities

Novartis Companies bound by the BCR commit to cooperate with the competent Data Protection Authorities, particularly by diligently responding within a reasonable time frame to their requests concerning the interpretation and application of the BCR and to follow their advice and recommendations in this respect, provided they are reasonable and consistent with applicable law.

Novartis Companies bound by the BCR commit to accept audits from the Data Protection Authority responsible for the Data Exporter.

9. Amendments of the BCR

Novartis may amend the BCR if it is justified by a Legitimate Business Purpose, if the applicable laws have changed, or if Data Protection Authorities have requested

certain changes be made. Decisions will be taken by the Data Privacy Leadership Team. Changes will be communicated to Novartis companies bound by the BCR and to the Data Protection Authorities.

Novartis agrees that significant modifications may require a new authorization from the Data Protection Authorities. Updates to the BCR or to the list of the Novartis Companies bound by the BCR are possible without having to re-apply for an authorization, provided that:

(i) A person or department is appointed to take the responsibility for keeping an updated list of Novartis Companies bound by the BCR, keeping track of and recording any significant updates to the BCR and ensuring that the necessary information is provided to the Data Subjects if the changes affect the exercise of their rights and to the Data Protection Authorities upon request.

(ii) Novartis Companies commit that Personal Information is not Transferred to any new Novartis Company until the new Company is effectively bound by the BCR, unless this Company is established in a country that provides an adequate level of data protection as determined by the European Commission and the Swiss Federal Data Protection Commission or meet any other legal means to Transfer Personal Information that have been approved by the EU Commission or Swiss Federal Data Protection Commission.

(iii) Changes to the BCR or to the list of Novartis Companies are to be reported once a year to the CNIL, acting as Lead Data Protection Authority.

10. Application of laws

10.1 Application of laws

Novartis Companies shall Process and Transfer Personal Information in accordance with the BCR and applicable laws.

Where local laws require a higher level of protection for Personal Information, the more stringent rules have precedence over the BCR. Where applicable local laws require a lower level of data protection, the BCR shall apply and must be complied with.

10.2 Conflict with applicable laws

If the Data Importer believes that applicable local laws and regulations, or codes of practice prevent compliance with the BCR or have a substantial adverse effect on the obligations required in the BCR, it shall promptly inform the Data Exporter and the Global Head Data Privacy, except where prohibited for law enforcement purposes, for example, to preserve the confidentiality of a law enforcement investigation.

The Global Head Data Privacy, in alignment with the Data Privacy Leadership Team, the Data Exporter and the relevant Country Data Protection Head, shall decide on what action to take and will report to the relevant Data Protection Authority.

11. Entry into force

The BCR shall enter into force upon approval by the relevant Data Protection Authorities and be applicable to the Novartis Companies upon signing the BCR Intercompany Agreement (Appendix 3).

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: Privacy Organization at Novartis

13. Approvals

These BCR have been formally recognized on July 3, 2012 by the following Data Protection Authorities to provide a sufficient safeguard to transfer Personal Information outside of the EEA and Switzerland:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italia, Latvia, Lithuania, Luxembourg, Malta, Norway, Netherlands, Poland, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Author and Owner of the BCR: Global Head Data Privacy
Reviewed by: Privacy 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