Amgen Binding Corporate Rules (BCRs) Public Document

Introduction:

Amgen is a biotechnology leader committed to serving patients with grievous illness.

Binding Corporate Rules (BCRs) express Amgen's commitment to privacy and data protection as it strives to provide adequate protection for the transfers and processing of Personal Information between Amgen entities.

All legal entities within Amgen and all staff members are committed to respecting BCRs. Non-compliance can lead to disciplinary actions, as permitted by local law.

The Chief Compliance Officer in liaison with the Chief Privacy Officer ensure that the described rules will be enforced.

BCRs have been adopted in reference to the current applicable European texts on data protection which are EU Directives 95/46/EC and 2002/58/EC.

1 – Scope

Amgen BCRs apply to transfers and processing, automated or manual, of all Personal Information of employees, customers, suppliers, shareholders, patients and all other Data Subjects performed by an Amgen Participating Companies operating as Controller in any of the following cases:

a) the Amgen Participating Company which processes the Personal Information is established in a Regulated country; or

b) the Amgen Participating Company which processes the Personal Information is not established in a Regulated Country ("Data Importer") and has received the Personal Information from an Amgen Participating Company established in a Regulated Country as defined in article 2 ("Data Exporter").

These BCRs apply as well to onward transfers of Personal Information from Data Importers to Data Importers.

2 – Definitions

Terms	Definitions
Personal Information	Information relating to an individual whose identity is apparent, or can be ascertained, from the information, by direct or indirect means. Alternatively, Personal Information may be thought of as information that can, either alone or in combination with other information, identify, or be used to contact or locate a single individual. Examples of Personal Information may include the following, depending on the local privacy and data protection laws: • An individual's name, address, social security number, driver's license number, financial account information, family information, or medical data, • The name, professional education, and prescribing practices of a physician, • The email address and other identifying information provided by someone visiting an Amgen website. The above list is exemplary only and not exhaustive.
Sensitive Personal Information	Information about a Data Subject's: • Medical or health conditions (physical or mental) • Financial information • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade-union membership • Sexual preference • Criminal convictions or arrest history Amgen considers sensitive information, information that could be used to perpetrate identity theft, e.g., Social Security Number, driver's license number, credit card or other bank account information.
Data Subject	The individual to whom Personal Information pertains. A Data Subject can be (among others) a: • Patient / Consumer / Clinical Trial Subject • Healthcare Professional (e.g., physician or nurse practitioner) • Employee (current, former or retired) • Contractor / Sole proprietor / Vendor/ Consultant
Controller (Data Controller)	Any entity which makes decisions with regard to the collection and Processing of Personal Information, including decisions about with the purposes for, and manner in which, Personal Information is Processed.
Data Processor	A person or entity that processes Personal Information on behalf of a Controller.
Processing	Any operation or set of operations that is performed on Personal Information, whether or not by automatic means, such as collecting, viewing, accessing, storing, recording, organizing, adapting or altering, retrieval, consultation, use, disclosure by

	transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Third Party	Natural or legal person, public authority, agency or any other body other than the data subject, the controller and the persons who, under the direct authority of the controller are authorized to process. At Amgen, a Vendor is considered a third Party.
Vendor	Any person, business or organization that provides goods and/or services to Amgen, is under a contractual relationship, and/or is a recipient of Personal Information from Amgen which are required to render these good and/or services.
Data Protection Authorities (DPA)	One or more public authorities responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive 95/46. These authorities act with complete independence in exercising the functions entrusted to them.
Regulated Country	A country in the European Economic Area (EEA) or a country with an adequate level of data protection as acknowledged by a decision of the EU Commission or any other countries recognizing BCRs as legitimate ways of transferring Personal Information outside of their jurisdiction such countries are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay.
Data Exporter	An Amgen entity operating as a Data Controller established in a Regulated Country that transfers Personal Information to another Amgen entity that is not established in a Regulated Country (Data Importer)
Data Importer	An Amgen entity which is not established in a Regulated Country that receives Personal Information from a Data Exporter
Technical and Organizational Security Measures	Measures aimed at protecting Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Participating Company	A legal entity from the Amgen group that is bound by the BCRs.
Consent	Any freely-given specific and informed indication of a Data Subject's wishes, by which the Data Subject signifies agreement to the collection and Processing of Personal Information relating to him/her.
Data Protection Officer	Company staff member who has been identified and nominated by an affiliate or business unit management as being responsible for

	the oversight of Privacy and Data Protection at local level as well as implementation of appropriate and required controls.

Amgen interprets the terms in BCRs according to the EU Directives 95/46/EC and 2002/58/EC, mentioned below as the EU Directive.

3 – Purpose Limitation

Personal Information shall be processed for explicit, specific and legitimate purposes pursuant to Article 6.1(b) of Directive 95/46.

Personal Information will not be processed in ways that are incompatible with the legitimate purposes for which the Personal Information was collected. Data Importers are obligated to adhere to original purposes when storing and/or further processing or using data transferred to them by another participating company. The purpose of data processing may only be changed with the consent of the data subject or to the extent permitted by local law to which the Data Exporter transferring the data is subject.

Sensitive Data will be provided with additional safeguards such as provided by the EU Directive 95/46/EC.

4 - Data Quality and Proportionality

Personal Information must be factually correct and where necessary, kept up to date. Appropriate measures must be taken to ensure that inaccurate or incomplete data is corrected or erased.

Personal Information shall be adequate and relevant, pursuant to Article 6.1(c) of Directive 95/46.

Data processing will be guided by the objective of limiting the collection, processing and/or usage of Personal Information to only what is necessary, i.e. as little Personal Information as possible. The possibility of anonymous or pseudonymous data must be used, provided that the cost and effort involved is commensurate with the desired purpose.

Personal Information which is no longer required for the business purpose for which it was originally collected and stored, must be deleted according to Amgen Record Retention Schedule. In the event that statutory retention periods or legal holds apply, the data will be blocked rather than deleted. At the end of the retention period or the legal hold, the data will be deleted.

5 – Legal Basis for Processing Personal Information

Processing of Personal Information is only permissible if at least <u>one</u> of the following prerequisites is fulfilled:

- The Data Subject has freely and unambiguously given his or her informed consent
- The Processing is necessary for the performance of a contract to which the Data Subject is party or a similar relationship of trust or in order to take steps at the request of the data subject prior to entering into a contract

- The Processing is necessary for compliance with a legal obligation to which the Controller is subject or is stipulated or permitted by applicable laws or regulations
- The Processing is necessary in order to protect the vital interests, such as life, health or safety, of the Data Subject
- The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller or in a third party to whom the data are disclosed
- The Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by the Third Party or parties to whom the data are disclosed, except where such interests are overridden by the legitimate interests for fundamental rights and freedoms of the Data Subject

6 – Processing of Sensitive Data

If according to a specific and legitimate purpose, Amgen needs to process Sensitive Data, Amgen will only do so if:

- The Data Subject has given his or her explicit consent to the Processing of such Sensitive Data, except where the applicable laws prohibits Processing
- The Processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards
- The Processing is necessary to protect the vital interests of the Data Subject or of another person where the data subject is physically or legally incapable of giving his or her consent
- The Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a Third Party without the consent of the Data Subjects
- The Processing relates to Sensitive Data which are manifestly made public by the Data Subject
- The Processing of Sensitive Data is necessary for the establishment, exercise or defense of legal claims
- The Processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Sensitive Data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy

7 – Transparency and Information Right

All Participating Companies shall process Personal Information in a transparent manner. Amgen is committed to making the BCRs, including contact information, readily available to every Data Subject and to informing Data Subjects of the transferring and Processing of their Personal Information.

In order to do so, Amgen will use various communication means such as corporate websites, including internal websites and newsletters, contracts, and specific privacy notices added to appropriate supports.

Data Subjects whom Personal Information is processed by a Participating Company shall be provided with the following information:

- The identity of the Controller(s) and of its representative, if any;
- The purposes of the Processing for which the data are intended;
- Origin of the data (unless this is Personal Information collected directly from the Data Subject)
- Any further information such as:
  i) the recipients or categories of recipients of the data,
  ii) the existence of the right of access to and the right to rectify the data concerning him or her so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

When the data is not received from a Data Subject, the obligation to inform the Data Subject does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

8 – Rights of Access, Rectification, Erasure and Blocking of Data

Every Data Subject has the right to obtain without constraint at reasonable intervals a communication to him or her in an intelligible form of the data undergoing Processing and of any available information as to their source. The follow up on this request, including the possibility to charge a fee or the time frame to answer such a request, will be subject to applicable laws and communicated appropriately to the Data Subject when he/she submits his/her request.

Every Data Subject has the right to obtain the rectification, erasure or blocking of data in particular because the data are incomplete or inaccurate.

Every Data Subject has the right to object, at any time on compelling legitimate grounds relating to their particular situation, to the processing of their Personal Information, unless that Processing is required by legal or regulatory requirements. Where the objection is justified, the Processing must cease.

Every Data Subject has the right to object (free of charge) to the Processing of Personal Information relating to him or her for the purposes of direct marketing.

Every Data Subject has the right to obtain the notification to third parties to whom the data have been disclosed of any rectification, erasure, or blocking, pursuant to Article 12(c) of Directive 95/46.

Every Data Subject has the right to know the logic involved in any automatic processing of data, pursuant to Article 12(a) of Directive 95/46.

9 – Automated Individual Decisions

Automated procedures are only being used as a tool for the decision-making process. No evaluation of or decision about a Data Subject which significantly affects him or her is based solely on automated processing of his or her data unless that decision:

- is taken in the course of entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to add his/her point of view; or
- is authorized by a law which also provides measures to safeguard the Data Subject's legitimate interests.

10 – Security and Confidentiality

Amgen implements appropriate technical and organizational security measures, to protect against and detect accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Information, in particular where the Processing involves the transmission of data over a public network, and against all other potential forms of unlawful Processing. International framework such as ISO/IEC 27002 are used by Amgen to determine these security measures.

Amgen has processes in place to ensure that potential privacy incidents are subject to reporting, tracking and appropriate corrective actions, as necessary.

Information Security Risk Assessments are used to identify potential threats to Sensitive Personal Information and implementation of additional security controls as appropriate.

The implementation of the measures will be done having regard to the state of the art, pursuant to Article 17.1 of Directive 95/46.

The Chief Information Security Officer works jointly with the Chief Privacy Officer in order to ensure the security and confidentiality of Personal Information.

11 – Relationships with Data Processors (Amgen Data Importer or Vendor)

The Controller will carefully choose a Data Processor that can be either an Amgen participating company or a Vendor. The Processor must provide sufficient guarantees regarding their technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

When outsourcing is deemed necessary after assessing the business needs and risks of such an outsourcing, the process of choosing the Vendor will include an evaluation of privacy risk factors and balance business needs against potential risks.

The Controller, utilizing written contractual means will, in accordance of applicable law, instruct the Vendor that, among other things:

i) the Processor shall act only on instructions from the Controller and that the Processing of data for the Processor's own purposes or for the purposes of a Third Party is prohibited; and

ii) the rules relating to the security and confidentiality to be incumbent on the Processor.

The Controller shall ensure that the Processor remains fully compliant with the agreed technical and organizational security measures.

The Controller retains responsibility for the legitimacy of processing and is still liable for the Data Subject's rights.

In order to provide such contractual obligations, a contractual template titled the Data Privacy Schedule is provided. Regarding the specific contractual situation, the Data Controller may negotiate a different provision, but it will still cover the obligations provided above.

12 – Restrictions on Transfers and Onward Transfers

Vendors acting as Data Processors are bound by written agreements stipulating that the Vendor shall act only on instructions from the Controller and shall be responsible for the implementation of the adequate security and confidentiality measures.

All transfers of data to Vendors located outside of the EU respect the European rules on transborder data flows either by making use of the EU Standard Contractual Clauses approved by the EU Commission or by other adequate contractual means according to Articles 25 and 26 of the EU Directive.

All transfers of data to Vendors acting as Data Processors located outside of the EU respect the EU Directive rules relating to the Processors in addition to the rules on transborder data flows.

13 – Training Program

Amgen provides appropriate training on privacy principles and the BCRs to all staff members. This training also includes information regarding the consequences under both criminal and employment law for employees who violate the BCRs.

The training is mandatory and repeated annually. Successful participation in training is documented.

Specific trainings will be provided on a case by case basis to staff members who have permanent or regular access to Personal Information, or who are involved in the collection of Personal Information or in the development of tools used to process Personal Information.

In addition, Amgen's Privacy Office provides appropriate information and resources related to privacy on the Amgen intranet portal as well as other avenues.

14 – Audit and Monitoring Program

As Amgen initiates Binding Corporate Rules (BCRs), the privacy Audits will remain and Amgen's compliance program will be updated to incorporate the BCRs. In addition, Amgen will continue its regular privacy monitoring performed locally by the Data Protection Officers in their capacity as a Compliance Lead.

The Audit program covers all aspects of the BCRs, including methods of ensuring that corrective actions will take place.

Such Audits are carried out on a regular basis by the internal accredited audit team.

The Audit program is developed and agreed to in cooperation by the Chief Audit Executive and the Chief Compliance Officer.

The Chief Privacy Officer, the Chief Compliance Officer, and the Chief Information Officer can initiate ad hoc BCR--related Audits, at any time.

All BCR Audit reports are communicated to the Chief Compliance Officer and to the Chief Privacy Officer in a timely manner. The BCRs Audit summaries and findings, as well as other relevant information is regularly reported to the Board of Directors via appropriate committees (e.g., Corporate Responsibility and Compliance Committee and/or Audit Committee of the Board).

The Data Protection Authorities can receive a copy of BCR-related audit reports upon request.

Each Participating Company understands that they can be audited by the Data Protection Authorities and they will abide by the advice of the Data Protection Authorities on any issue related to the BCRs. Each audited entity must inform the Chief Privacy Officer immediately upon notice of an Audit.

15 – Compliance and Supervision of Compliance

Amgen appoints appropriate staff members, including a network of Data Protection Officers, with top management support to oversee and ensure compliance with the rules.

At Amgen, the Chief Privacy Officer's responsibilities, among others, include:

- advising the board of management,
- ensuring data protection compliance at a global level
- reporting regularly on data protection compliance, and
- working with Data Protection Authorities' investigations

The Chief Privacy Officer is in charge of the Global Privacy Office which is a team providing expert support worldwide for Amgen entities.

At the local level, Data Protection Officers are responsible for handling local privacy requests from Data Subjects, for ensuring compliance at a local level with support from the Privacy Office and for reporting major privacy issues to the Chief Privacy Officer. Amgen maintains a Data Protection Officer network and ensures that a DPO is appointed or assigned for each country where Amgen (the Participating Company) has a corporate entity. This designation is

made in agreement with the local manager of the DPO and the local human resources department.

Usually, Data Protection Officers are the local healthcare compliance managers who report into Worldwide Compliance and Business Ethics department. The Privacy Office also reports into the Worldwide Compliance and Business Ethics department. Rarely, due to the specificity of an Amgen entity or special circumstances, the Data Protection Officer may come from another function, for example Regulatory. In any event, the Privacy Office ensures that the Data Protection Officers are trained appropriately and have a sufficient level of management and expertise to fulfill his or her Data Protection Officer role. In addition, the Data Protection Officers have a direct line to the Chief Privacy Officer as well as Privacy Office staff, in the event they need any additional guidance.

16 – Actions in Case of National Legislation Preventing Respect of BCRs

Where a member of the group has reason to believe that the legislation applicable to him or her prevents the company from fulfilling its obligations under the BCRs and has a substantial effect on the guarantees provided by the rules, he/she will promptly inform the Chief Privacy Officer (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

Where there is conflict between national law and the commitments in the BCRs, the Chief Privacy Officer in liaison with local legal counsel and the local Data Protection Officer will determine what legally appropriate action is required. If necessary, the Chief Privacy Officer will also consult with the relevant Data Protection Authorities.

17 – Internal Complaint Mechanisms

Amgen will expand and utilize its existing complaint handling process to incorporate handling of any BCR-related complaints or concerns.

Any data subject may complain, at any time, that any Participating Company is not complying with the BCRs. Such complaints will be handled by the Privacy Office under the direction of the Chief Privacy Officer and in cooperation with the relevant local Data Protection Officer.

Amgen recommends that such complaints are provided in writing either by postal mail or email directly to the Privacy Office or to the affiliate. Date Subjects may as well, when acceptable according to applicable laws, use the Business Conduct Hotline to report a BCRs complaint.

If the complaint is received locally, the DPO will translate if necessary and forward it without undue delay to the Privacy Office.

A first answer will be provided to the Data Subject informing him or her that the complaint is under review and that he or she will receive an answer within a maximum of two months.

If the Privacy Office discovers individual wrongdoing, appropriate disciplinary measures will be taken, up to and including immediate termination of employment, to the extent permitted by applicable law.

Within a maximum of two months, the Data Subject will receive an answer informing him or her of the outcome of his or her complaint.

The Data Subject will be informed that if he or she is not satisfied by Amgen's answer, he or she can lodge a claim before the relevant Court or Data Protection Authority.

This complaint handling process will be made public through the publication of the BCRs as mentioned in section 7.

18 - Third Party Beneficiary Rights and Liability

A Data Subject whose Personal Information originates from a Regulated Country and who claims a breach of any obligations referenced in the BCR has the right to enforce the rules as a third-party beneficiary. These rights cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation. If applicable, liability is limited to the actual damage suffered.

To the extent permitted by applicable jurisdiction, Data Subjects can choose to lodge claims before:

- The jurisdiction of the Data Exporter, and if the Data Subject's Personal Information originates from an EEA Data Exporter, the competent jurisdiction shall be the place of establishment of the EEA Data Exporter, or
- Before the competent Data Protection Authorities.

Any Data Subject, who has suffered any breach of the obligations referred in the BCRs by the Data Exporter or the Data Importer is entitled to receive compensation from the Data Exporter for the damage suffered. If the Data Exporter or the Data Importer is held liable for a breach, it will to the extent to which it is liable, indemnify the other party for any cost, charge, damage, expense or loss it has incurred.

Each Data Exporter and Data Importer may be exempted from liability under the BCRs if it proves the member of the group outside of the EU has not violated BCRs or is not responsible for the damages caused to the Data Subject. However, the burden of proof remains with the Data Exporter and Data Importer.

The Data Importer acting as a Data Processor may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities. If a Data Subject wants to bring a claim against the Data Exporter but is not able to, arising out of a breach of the BCRs because the Data Exporter has factually disappeared or ceased to exist in law or became 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 or Data Importer by contract or by operation of law, the Data Subject can enforce its rights against such entity. The liability of the Data Importer shall be limited to its own processing operations under the BCRs.

19 – Mutual Assistance and Cooperation with Data Protection Authorities

Participating Companies are compelled to cooperate and assist each other to handle a request or complaint from a Data Subject or an investigation or inquiry by Data Protection Authorities.

Participating Companies will answer, in collaboration with the Chief Privacy Officer, BCR-related requests from the Data Protection Authority within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the competent Data Protection Authority with regard to implementation of the BCRs.

20 – BCRs Updating and Changes

Amgen reserves the right to change and/or update these BCRs at any time. Such updating of the BCRs may be necessary specifically as a result of changed legal requirements, significant changes to the structure of the Amgen group or official requirements imposed by the competent Data Protection Authorities.

Amgen will report any significant changes to the BCRs or to the list of Participating Companies to all other Participating Companies and to the Data Protection Authorities to take into account modifications of the regulatory environment and the company structure.

Some modifications might require a new authorization from the Data Protection Authorities.

The Chief Privacy Officer will keep a fully updated list of the Participating Companies of the BCRs, of the Regulated Countries that may be protected under the BCRs and track any updates to the rules as well as provide the necessary information to the Data Subjects or Data Protection Authorities upon request.

Amgen is committed that no transfer is made to a new Participating Companies under the guarantees of the BCRs until the new Participating Company is effectively bound by the BCRs and in compliance with the BCRs.

Any changes to the BCRs or to the list of Participating Companies will be reported once a year to the Data Protection Authorities granting the authorizations with a brief explanation regarding the reasons for the update.

Substantial modifications to the rules will also be communicated to the Data Subjects by any means according to Article 7 of the BCRs.

21 – Relationship between National Laws and the BCRs

Where the local legislation requires a higher level of protection for Personal Information it will take precedence over the BCRs. If the applicable local law provides a lower level of protection for Personal Information than the BCRs, BCRs will be applied.

In the event that obligations arising from the applicable local law are in conflict with the BCRs, the Participating Company shall inform the Chief Privacy Officer without undue delay.

In any event, Personal Information shall be processed in accordance to the applicable law as provided by the Article 4 of the Directive 95/46/EC and the relevant local legislation.