Amgen EU Binding Corporate Rules – Controller (EU BCRs)

Last Updated: 12 December 2023

Introduction

(A) Amgen is a biotechnology leader committed to serving patients with grievous illness. These EU Binding Corporate Rules – Controller ("**EU BCRs**") express Amgen's commitment to privacy and data protection as it strives to provide adequate protection for the transfers and Processing of Personal Data between Participating Companies.

(B) All Participating Companies and all Personnel are committed to respecting, and are legally bound by, these EU BCRs in respect of Personal Data within the EU BCRs' scope. Non-compliance can lead to disciplinary sanctions, as permitted by local law. The Chief Compliance Officer in liaison with the Chief Privacy Officer ensures that the EU BCRs will be enforced. A list of Participating Companies can be found here: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. All Participating Companies can be contacted at privacy@amgen.com for any question concerning these EU BCRs.

(C) These EU BCRs have been adopted in reference to the EU Data Protection Laws. Amgen France is responsible for ensuring compliance by the Participating Companies with these EU BCRs. Individuals can enforce these EU BCRs against Amgen France as a third-party beneficiary as described below. These EU BCRs are available on Amgen's website: www.amgen.com/bcr. Alternatively, please contact Amgen on privacy@amgen.com to request a copy.

1. Scope

1.1. Amgen EU BCRs apply to transfers and Processing, automated or manual, of all Personal Data of Data Subjects performed by a Participating Company operating as Data Controller or operating as a Data Processor for another Participating Company acting as Data Controller in any of the following cases:

1.1.1. the Participating Company which Processes the Personal Data is established in the EU; or

1.1.2. the Participating Company which Processes the Personal Data is not established in the EEA and has received the Personal Data from a Participating Company established in the EEA; or

1.1.3. to onward transfers of Personal Data from Data Importers to Data Importers.

1.2. An overview of the data flows pursuant to these EU BCRs is available at Appendix 1.

2. Definitions

Terms	*Definitions*
Amgen France	Amgen S.A.S., a company incorporated in France whose registered office is at 25 quai du Président Paul Doumer, 92400 Courbevoie.
Applicable Law	The law of the EU and/or (as applicable) the national or local law of the EEA Member States (including without limitation the EU Data Protection Laws).
Compliance Lead	A person within the Healthcare Compliance division of the Worldwide Compliance and Business Ethics department at a Participating Company who has delegated responsibility for data protection and privacy and, where distinct from the local Data Protection Officer, supports the local Data Protection Officer with its responsibilities and tasks.
Consent	Any freely given specific, informed and unambiguous indication of a Data Subject's wishes, by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him/her.
Data Controller	Any entity which makes decisions with regard to the collection and Processing of Personal Data, including decisions about the purposes for, and manner in which, Personal Data is Processed.
Data Exporter	A Participating Company operating as a Data Controller established in the EEA that transfers Personal Data to a Data Importer.
Data Importer	A Participating Company which is not established in the EEA that either (a) receives Personal Data from a Data Exporter or (b) receives an onward transfer of Personal Data pursuant to Article 1(c) of these EU BCRs.
Data Processor	A person or entity that processes Personal Data on behalf of a Data Controller.
Data Protection Authority (DPA)	An independent public data protection authority established by an EEA Member State.
Data Protection Officer	A person who has been nominated by Amgen's Chief Privacy Officer as being responsible for the oversight of Privacy and Data Protection at local level as well as the implementation of appropriate and required controls.
Data Subject	A natural person who can be identified, directly or indirectly, by reference to Personal Data. A Data Subject may be (without limitation): • a patient / clinical trial data subject (which may include a child under the age of 18) • a healthcare professional

Terms	*Definitions*
	• an employee • a vendor or supplier
EEA	The member states of the European Union (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden) and Iceland, Liechtenstein and Norway (all being "**EEA Member States**").
EU Data Protection Laws	The GDPR and (as applicable) the local or national law relating to data protection and the Processing of Personal Data and implementing the GDPR of a relevant EEA Member State.
GDPR	The General Data Protection Regulation ((EU) 2016/679).
Participating Company	A legal entity from the Amgen group that is bound by the EU BCRs.
Personal Data	Any information relating to a Data Subject such as a name, an identification number, location data, an online identifier or to one or more factors specific to or information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of Personal Data may include the following: • A Data Subject'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 healthcare professional, • The email address and other identifying information provided by someone visiting an Amgen website. The above list is indicative only and not exhaustive.
Personal Data Breach	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Personnel	All staff members and contingent workers (including consultants, temporary agency workers and contract workers) of any Participating Company.
Processing	Any operation or set of operations which is performed on Personal Data (or sets of Personal Data), whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

Terms	*Definitions*
	dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Separately to the EU Data Protection Laws, Amgen also considers financial information and 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) as Sensitive Personal Data.
Technical and Organizational Security Measures	Technological and organizational measures aimed at protecting Personal Data 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.
Third Party	A natural or legal person, public authority, agency or any other body other than the Data Subject, the Participating Company acting as Data Controller and a Participating Company acting as Data Processor. At Amgen, a Vendor is considered a Third Party. Depending on the circumstances, a Third Party may act as a Data Controller or a Data Processor in relation to the Processing of Personal Data.
Vendor	Any natural or legal person, business or organization that provides goods and/or services to a Participating Company under a contractual relationship and/or is a recipient of Personal Data from such Participating Company in order to render those good and/or services.

Amgen shall interpret the terms in these EU BCRs in accordance the EU Data Protection Laws.

3. Purpose Limitation

3.1. Personal Data shall be Processed for explicit, specified and legitimate purposes pursuant to Article 5(1)(b) of the GDPR.

3.2. Personal Data will not be Processed in ways that are incompatible with the legitimate purposes for which the Personal Data was collected or Applicable Law. Data Importers are obligated to adhere to original purposes when storing and/or further Processing of Personal Data or Processing Personal Data transferred to them by another Participating Company. The purpose of Personal Data Processing may only be changed with the Consent of the Data Subject or to the extent permitted by Applicable Law.

3.3. Sensitive Personal Data will be provided with additional safeguards such as provided by the EU Data Protection Laws.

4. Data Quality and Proportionality

4.1. Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

4.2. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed, pursuant to Article 5(1)(c) of the GDPR.

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

4.4. Personal Data which is no longer required for the business purpose for which it was originally collected and stored must be deleted according to Amgen's 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 Data

5.1. Processing of Personal Data is only permissible if at least one of the following prerequisites is fulfilled:

5.1.1. The Data Subject has given his or her Consent to the Processing of his or her Personal Data for one or more specific purposes.

5.1.2. The Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

5.1.3. The Processing is necessary for compliance with a legal obligation to which the Data Controller is subject under Applicable Law.

5.1.4. The Processing is necessary in order to protect the vital interests, such as life, health or safety, of the Data Subject or of another natural person.

5.1.5. 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 Data Controller.

5.1.6. The Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

5.2. Processing of Personal Data relating to criminal convictions and offences shall be carried out only when the Processing is authorised by Applicable Law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

6. Processing of Sensitive Personal Data

6.1. If, according to a specific and legitimate purpose, the Participating Company needs to Process Sensitive Personal Data, the Participating Company will only do so if:

6.1.1. The Data Subject has given explicit Consent to the Processing of those Sensitive Personal Data for one or more specified purposes, except where Applicable Law provides that the prohibition in Article 9(1) of the GDPR may not be lifted by the Data Subject.

6.1.2. The Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment and social security and social protection law in so far as it is authorized by Applicable Law or by a collective agreement pursuant to Applicable Law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

6.1.3. The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving his Consent.

6.1.4. 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 outside that body without the Consent of the Data Subjects.

6.1.5. The Processing relates to Sensitive Personal Data which are manifestly made public by the Data Subject.

6.1.6. The Processing of Sensitive Personal Data is necessary for the establishment, exercise or defence of legal claims.

6.1.7. The Processing is necessary for reasons of substantial public interest, on the basis of Applicable Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

6.1.8. The Processing of the Sensitive Personal Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Applicable Law or pursuant to contract with a health professional, and where those Sensitive Personal Data are Processed by or under the responsibility of a health professional such professional must be subject to the obligation of professional secrecy under Applicable Law or rules established by competent bodies in an EEA Member State or by another person also subject to an obligation of secrecy under Applicable Law or rules established by competent bodies in an EEA Member State.

6.1.9. The Processing of Sensitive Personal Data is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Applicable Law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy.

6.1.10. The Processing of Sensitive Personal Data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on Applicable Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

7. Transparency and Information Rights

7.1. All Participating Companies shall process Personal Data in a transparent manner. Amgen is committed to making the EU BCRs, including contact information, readily available and easily accessible to every Data Subject and to informing Data Subjects of the transfer and Processing of their Personal Data. These EU BCRs are available on Amgen's website: www.amgen.com/bcr. Alternatively, please contact Amgen on privacy@amgen.com to request a copy. Amgen will also use various communication means such as corporate websites, including internal websites and newsletters, contracts, and specific privacy notices to meet this accessibility requirement. In addition, Amgen will inform Data Subjects, using these means of communication, of any updates or changes to the EU BCRs or to the list of Participating Companies without undue delay.

7.2. Data Subjects whose Personal Data is Processed by a Participating Company shall be provided with the information set out in Articles 13 and 14 of the GDPR.

7.3. Where the Personal 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 Restriction of Data

8.1. Every Data Subject has the right to obtain from the Participating Company confirmation as to whether or not Personal Data concerning him or her are being Processed, and, where that is the case, access to the Personal Data and the information required to be provided by Article 15(1) of the GDPR. 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 Law and communicated appropriately to the Data Subject when he/she submits his/her request.

8.2. Every Data Subject has the right to obtain the rectification, erasure or restriction of Personal Data in particular where the data are incomplete or inaccurate.

8.3. Every Data Subject has the right to object, at any time on grounds relating to their particular situation, to the Processing of their Personal Data based on the performance of a task carried out in the public interest or the legitimate interests of the Participating Company or a Third Party (including profiling based on those grounds). The Participating Company shall no longer Process the Personal Data unless it demonstrates compelling legitimate grounds for the

Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

8.4. Every Data Subject has the right to object (free of charge) to the Processing of Personal Data relating to him or her for the purposes of direct marketing, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject exercises their right to object to the Processing of Personal Data relating to him or her for the purposes of direct marketing, the Participating Company must cease Processing the Personal Data for that purpose.

8.5. Every Data Subject has the right to obtain the notification to Third Parties to whom the Personal Data have been disclosed of any rectification, erasure, or restriction, pursuant to Article 19 of the GDPR.

8.6. Every Data Subject has the right to know the logic involved in any automatic Processing of Personal Data, pursuant to Article 13(2)(f) of the GDPR.

8.7. Where Processing is based on Consent, every Data Subject has the right to withdraw their Consent at any time. The withdrawal of Consent shall not affect the lawfulness of Processing based on Consent before its withdrawal.

8.8. Every Data Subject has the right to complain to the Participating Company regarding the Processing of Personal Data through the internal complaint mechanism provided pursuant to Article 17.

8.9. Any requests under this Article 8 (or Article 9 below) should be sent to the Participating Company at: privacy@amgen.com. While making requests by email is strongly encouraged, this does not preclude a Data Subject making a verbal request. The Participating Company shall inform the Data Subject without delay of the outcome of their request and at the latest within one month of receipt of the request (including where applicable the reasons for not taking action and the possibility of lodging a complaint with the competent DPA and/or seeking a judicial remedy). That period of one month may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Participating Company shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Any communication, action and/or information provided in relation to a request under this Article 8 (or Article 9 below) shall be provided to the Data Subject free of charge. Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Participating Company may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The Participating Company shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

9. Automated Individual Decisions

9.1. The Data Subject shall have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless that decision:

9.1.1. is necessary for entering into, or the performance of, a contract between the Data Subject and the Participating Company;

9.1.2. is required or authorized by Applicable Law which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests (including at least the right to obtain human intervention on the part of the Participating Company, to express his or her point of view and to contest the decision); or

9.1.3. is based on the Data Subject's explicit Consent.

10. Security and Confidentiality

10.1. Amgen implements appropriate Technical and Organizational Security Measures, to protect against and detect Personal Data Breaches. International frameworks, such as ISO/IEC 27002, are used by Amgen to determine these security measures.

10.2. Amgen has processes in place to ensure that Personal Data Breaches are subject to reporting, tracking and appropriate corrective actions, as necessary. Any Personal Data Breach shall be documented (including the facts relating to the Personal Data Breach, its effects and the remedial action taken) and the documentation shall be made available to the competent DPA on request. Participating Companies shall notify without undue delay any Personal Data Breach to Amgen France, the Chief Privacy Officer and the other relevant privacy officer/function, and (where the Participating Company suffering a Personal Data Breach acts as Data Processor) to the Participating Company acting as Data Controller. Personal Data Breaches shall, in conjunction with the Chief Privacy Officer, be notified to the competent DPA without undue delay (and where feasible not later than 72 hours after becoming aware of the Personal Data Breach) unless it is unlikely to result in a risk to the rights and freedoms of Data Subjects. Where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, it shall also be notified to Data Subjects without undue delay.

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

10.4. The implementation of the measures will have regard to the state of the art, pursuant to Article 32 of the GDPR.

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

10.6. The Technical and Organizational Security Measures shall be designed to implement the data protection principles under Article 5 of the GDPR, data protection by design and default principles pursuant to Article 25 of the GDPR and to facilitate compliance with the requirements set by these EU BCRs in practice.

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

11.1. The Participating Company (acting as Data Controller) will carefully choose a Data Processor that can be either another Participating Company or a Vendor. The Data Processor must provide sufficient guarantees regarding their Technical and Organizational Security Measures governing the Processing to be carried out and must ensure compliance with those measures.

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

11.3. The Participating Company acting as Data Controller, utilizing written contractual means will, in accordance with Applicable Law (and in particular the requirements of Article 28(3) of the GDPR), instruct the Data Processor, among other things:

11.3.1. the Data Processor shall act only on instructions from the Participating Company acting as Data Controller and that the Processing of Personal Data for the Data Processor's own purposes or for the purposes of a Third Party is prohibited;

11.3.2. on the rules relating to the security and confidentiality to be incumbent on the Data Processor and to implement appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk of the Processing;

11.3.3. persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

11.3.4. the Data Processor shall not engage another Data Processor without the prior specific or general written authorisation of the Participating Company acting as Data Controller and, where such authorisation is given, the same data protection obligations as set out in the contract or other legal act between the Participating Company acting as Data Controller and the Data Processor shall be imposed on that other Data Processor;

11.3.5. taking into account the nature of the Processing, it must assist the Participating Company acting as Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Participating Company's obligation to respond to requests for exercising the Data Subject's rights;

11.3.6. it must assist the Participating Company acting as Data Controller in ensuring compliance with the obligations relating to security of Processing, notification of a Personal Data Breach to the competent DPA, communication of a Personal Data Breach to the Data Subject, data protection impacts assessments and prior consultation with the competent DPA, taking into account the nature of Processing and the information available to the Data Processor;

11.3.7. at the choice of the Participating Company acting as Data Controller, it must delete or return all the Personal Data to the Participating Company acting as Data Controller after the end of the provision of services relating to the Processing, and delete existing copies unless EU Data Protection Law requires storage of the Personal Data;

11.3.8. it must make available to the Participating Company acting as Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Article 11 and allow for and contribute to audits, including inspections, conducted by the Participating Company acting as Data Controller or another auditor mandated by it.

11.4. The Participating Company acting as Data Controller shall ensure that the Data Processor remains fully compliant with the agreed Technical and Organizational Security Measures.

11.5. The Participating Company acting as Data Controller retains responsibility for the legitimacy of Processing and is still liable for the Data Subject's rights. To the extent the Data Processor is subject to the EU Data Protection Laws, it shall also be liable for its obligations and responsibilities as a Data Processor under such laws.

11.6. In order to provide for the contractual obligations set out in this Article on Data Processors, a contractual template titled the Data Privacy Schedule is provided for use by Participating Companies acting as Data Controller. The Participating Company acting as Data Controller may, depending on the specific circumstances of each contractual arrangement, negotiate different provisions to those set out in the Data Privacy Schedule, but the contractual provisions must still cover, at a minimum, the obligations set out above in this Article 11.

11.7. Each Participating Company acting as a Data Processor which is subject to the EU Data Protection Laws must maintain a record of all categories of Processing activities carried out on behalf of a Participating Company acting as Data Controller. This record should be maintained in writing, including in electronic form, shall be made available to the Chief Privacy Officer and the competent DPA on request, and shall contain the following information: (a) the name and contact details of the Participating Company acting as a Data Processor and of each Participating Company acting as Data Controller on behalf of which it is acting, and, where applicable, its representative, and DPO; (b) the categories of Processing carried out on behalf of each Participating Company acting as Data Controller; and (c) where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers which rely on a derogation under Article 49 if the GDPR, documentation of the suitable safeguards; and (d) where possible, a general description of the Technical and Organisational Security Measures.

12. Restrictions on Transfers and Onward Transfers

12.1. All transfers of Personal Data subject to these EU BCRs to Third Parties located outside of the EEA shall respect the EU Data Protection Laws on transfers and onward transfers of Personal Data either by making use of the standard contractual clauses authorized under Commission Implementing Decision (EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR or by another adequate means according to Chapter V of the GDPR (including, exceptionally, if a derogation applies to a specific situation in accordance with Article 49 of the GDPR).

12.2. All transfers of Personal Data subject to these EU BCRs to Data Processors located outside of the EEA shall respect the EU Data Protection Laws relating to Data Processors (and the requirements set out in Article 11 above) in addition to the rules on transfers and onward transfers of Personal Data set out in this Article 12 and in the EU Data Protection Laws.

12.3. Before transferring Personal Data to a Data Importer or (in respect of ongoing transfers) before any updated local national law enters into force, the Data Exporter shall, in conjunction with the Chief Privacy Officer and Amgen France, with the assistance of the Data Importer and taking into account the circumstances of the transfer, evaluate if local national law will prevent the Data Importer from fulfilling its obligations under the EU BCRs and determine whether any required supplementary measures should be implemented. Such assessment will take account of:

12.3.1. the specific circumstances of the transfer (including the purposes for which the Personal Data are transferred and Processed, the types of entities involved in the Processing, the economic sector in which the transfer occurs, the categories and format of the Personal Data transferred, the location of the Processing (including storage) and the transmission channels used);

12.3.2. the laws and practices of the third country of destination relevant in view of the specific circumstances of the transfer (including those requiring the disclosure of data to public authorities or authorising access by such authorities) and the applicable limitations and safeguards; and

12.3.3. any relevant contractual, technical or organizational safeguards put in place in respect of the transfer, including measures applied during the transmission and to the Processing of the Personal Data in the country of destination.

Furthermore, such assessment shall be based on the understanding that laws and practices of the third country of destination respect the fundamental rights and freedoms of the Data Subject and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the following objectives: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest, in particular important economic or financial interests, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) monitoring, inspection or regulatory functions connected to the exercise of official authority in the cases referred to in the preceding objectives; (i) the protection of the Data Subject or the rights and freedoms of others; and/or (j) the enforcement of civil law claims.

The Chief Privacy Officer shall review and approve the documented assessment and any proposed supplementary measures. Where the outcome of the assessment demonstrates the need to implement supplementary measures, the Data Exporter shall implement those measures. If no supplementary measures can be put in place (or if instructed by the Chief Privacy Officer or a competent DPA), the Data Exporter shall suspend the transfer. The outcome of the assessment and proposed supplementary measures shall be recorded and provided to the competent DPA where required.

The Chief Privacy Officer and Amgen France will inform all Participating Companies of the assessment carried out and of its results so that the identified supplementary measures can be applied where the same type of transfers are carried out by other Participating Companies or, where effective supplementary measures cannot be put in place, such transfers are suspended or terminated.

12.4. The Data Importer shall promptly notify the Data Exporter, Amgen France and the Chief Privacy Officer if it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under these EU BCRs, including following a change in the local national laws in the third country as described in Article 12.3 or a measure such as a disclosure request as described in Article 16.3. In addition, the Data Exporters shall (in conjunction with the Chief Privacy Officer) monitor, on an ongoing basis, and where appropriate with the assistance of the Data Importers, developments in the third

countries to which the Data Exporters have transferred Personal Data that could adversely affect the initial assessment of the level of protection of Personal Data and the decisions taken in respect of such transfers.

12.5. Following a suspension of a transfer, the Data Exporter must terminate the transfer or set of transfers if the Data Importer is unable to comply with the EU BCRs and/or compliance is not restored within one month of the suspension. In such case, the Data Importer must, at the choice of the Data Exporter, either return or destroy all Personal Data that have been transferred prior to the suspension, and any copies thereof.

12.6. Any Personal Data flows not subject to these EU BCRs and/or not originating from a Participating Company established in an EEA Member State are not considered a transfer of Personal Data under these EU BCRs and are, accordingly, not subject to the requirements of these EU BCRs.

13. Training Program

13.1. As described in Appendix 2, Amgen provides appropriate and up-to-date training on privacy principles and more specifically on the EU BCRs to all Personnel. This training also includes information regarding the consequences under criminal and employment law and/or their contract for services for Personnel who breach the EU BCRs.

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

13.3. Specific trainings will be provided on a case by case basis to Personnel who have permanent or regular access to Personal Data, or who are involved in the collection of Personal Data or in the development of tools used to Process Personal Data.

13.4. In addition, Amgen's Global Privacy Compliance Team provides appropriate information and resources related to privacy, including on the Amgen intranet portal.

14. Audit and Monitoring Program

14.1. The Chief Privacy Officer ensures that all Participating Companies (and their compliance with these EU BCRs) are included within the audit and monitoring program from a privacy and data protection perspective. Comprehensive audits are carried out on a regular basis, no less frequently than every 2 to 3 years (for Participating Companies with a medium to high risk profile based on the Audit department's risk assessment methodology) and every 4 to 5 years (for Participating Companies with a low risk profile based on the Audit department's risk assessment methodology), by the Internal Audit Team or independent, external certified auditors. Comprehensive audits include data protection and privacy matters within their scope (including compliance with these EU BCRs, where applicable to and used by a Participating Company). In addition to comprehensive audits, and without prejudice to the timeframes set out above, other scopes of audit are carried out including cross-functional or issue-specific audits (e.g., compliance with the EU BCRs), a limited audit of one or more Personal Data Processing systems and/or a limited audit of one or more functional departments (e.g., the Global Privacy Compliance Team). The audit program is developed and agreed to in cooperation with the Chief Audit Executive and the Chief Compliance Officer who is a Senior Vice-President. The Chief Privacy Officer, the Chief Compliance Officer, and the Chief Information Officer can initiate ad hoc EU BCRs-related audits at any time. For example, in response to any identified compliance issue or a report of substantive non-

compliance, a Personal Data Breach and/or a substantive change in the EU Data Protection Laws. The audit program covers all aspects of the EU BCRs including methods of ensuring that corrective actions will take place.

14.2. All EU BCRs audit reports are communicated to the Chief Compliance Officer and to the Chief Privacy Officer in a timely manner. The EU BCRs audit summaries and findings, as well as other relevant information, are also regularly reported to the Board of Directors of Amgen Inc. via appropriate committees (e.g., Corporate Responsibility and Compliance Committee and/or Audit Committee of the Board), to the board of directors of Amgen France and (where appropriate, for example, in relation to a finding requiring remedy) to the relevant Participating Company. The Corporate Responsibility and Compliance Committee of the Board of Directors of Amgen, Inc. meets five times a year. Privacy & Data Protection is covered annually, typically in the October meeting.

14.3. The competent DPA can receive a copy of EU BCRs-related audit reports upon request.

14.4. Each Participating Company shall cooperate with and shall accept, without restrictions, to be audited by the competent DPA. Each audited entity must inform the Chief Privacy Officer immediately if it receives notice of such audit or such an audit takes place.

15. Compliance and Supervision of Compliance

15.1. Amgen appoints appropriate Personnel, including where applicable a network of Data Protection Officers, with top management support to oversee and ensure compliance with data protection rules. The Chief Privacy Officer is in charge of the Global Privacy Compliance Team which is a global team providing expert support worldwide for Amgen entities (including Participating Companies).

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

15.2.1. advising the board of management;

15.2.2. ensuring data protection compliance at a global level (including having overall responsibility for the EU BCRs);

15.2.3. reporting regularly on data protection compliance (including to the Chief Compliance Officer); and

15.2.4. working with the competent DPA's investigations.

15.3. The Global Privacy Compliance Team includes the Chief Privacy Officer (who, in addition to the responsibilities noted above, oversees the global network of Data Protection Officers), the European Data Protection Officer and other local Data Protection Officers. The Global Privacy Compliance Team has overall responsibility for data protection and privacy compliance worldwide at Amgen.

15.4. The European Data Protection Officer has been appointed by Amgen as the Data Protection Officer for the EEA, the UK and Switzerland. The European Data Protection Officer has the tasks set out in Article 39 of the GDPR. Amgen will ensure that that the tasks and duties of the European Data Protection Officer do not result in a conflict of interests with such tasks. The European Data Protection Officer has a direct reporting line to the Chief Privacy Officer (who forms part of the highest management level for Amgen) and is supported by the local

Compliance Lead in France. The European Data Protection Officer may contact the Chief Privacy Officer if any questions or problems arise during the performance of their duties. The European Data Protection Officer can be contacted at: privacy@amgen.com

15.5. 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 Global Privacy Compliance Team 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 has a corporate entity (the Participating Company) and the applicable law of the jurisdiction of such Participating Company require such appointment.

15.6. Usually, Data Protection Officers either are, or are supported by, the local Compliance Leads who report into the Worldwide Compliance and Business Ethics department. The Global Privacy Compliance Team is a part of, and reports into, the Worldwide Compliance and Business Ethics department which is headed by the Chief Compliance Officer. The Chief Compliance Officer has overall responsibility for the Amgen group's legal and regulatory compliance worldwide. Rarely, due to the specific circumstances of a Participating Company or other special circumstances, the Data Protection Officer may come from another function, for example Regulatory. In any event, the Global Privacy Compliance Team ensures that the Data Protection Officers and Compliance Leads are trained appropriately and have a sufficient level of management and expertise to fulfil his or her role. In addition, the Data Protection Officers have a direct reporting line to the Chief Privacy Officer and are supported by Global Privacy Compliance Team Personnel in the event they need any additional guidance.

15.7. Every Participating Company acting as Data Controller shall be responsible for and be able to demonstrate compliance with the EU BCRs. As part of this requirement, all Participating Companies:

15.7.1. must maintain a record of all categories of Processing activities carried out in line with the requirements as set out in Article 30(1) of the GDPR. This record should be maintained in writing, including in electronic form, shall be made available to the Chief Privacy Officer and the competent DPA on request, and shall contain the following information: (a) the name and contact details of the Participating Company acting as Data Controller, its representative and DPO; (b) the purposes of the Processing; (c) a description of the categories of Data Subjects and of the categories of Personal Data; (d) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers which rely on a derogation, documentation of the suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of Personal Data; and (g) where possible, a general description of the Technical and Organisational Security Measures.

15.7.2. carry out data protection impact assessments for Processing operations that are likely to result in a high risk to the rights and freedoms of natural persons in accordance with Article 35 of the GDPR. Where a data protection impact assessment under Article 35 indicates that the Processing would result in a high risk in the absence of measures taken by the Participating Company to mitigate the risk,

the Chief Privacy Officer must be consulted prior to Processing, who shall then consult with the competent DPA in accordance with Article 36 of the GDPR.

16. Actions in Case of National Legislation Preventing Respect of the EU BCRs

16.1. Where a Participating Company has reason to believe that the laws applicable to it prevents the Participating Company from fulfilling its obligations under the EU BCRs or has a substantial effect on the guarantees provided by the rules, it 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) and Amgen France.

16.2. Where there is conflict between local national law and the commitments in the EU 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 competent DPA.

16.3. Where any legal requirement a Participating Company is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the EU BCRs, the Chief Privacy Officer, Amgen France, and the Data Exporter shall be promptly notified by the Data Importer, and the Chief Privacy Officer shall notify the competent DPA and (where possible) the Data Subjects. This includes (a) any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body, and in such a case, the competent DPA should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure and the response provided (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), and (b) any direct access by public authorities to Personal Data transferred pursuant to these EU BCRs in accordance with the laws of the country of destination, and in such case such notification shall include all information available to such Participating Company (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

16.4. If in specific cases the suspension and/or notification are prohibited, the Participating Company receiving the request will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate (upon the request of the Data Exporter) that it did so.

16.5. The Data Importer will provide the Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, the number of requests, the type of Personal Data requested, the identity of the requesting authorities, whether requests have been challenged and the outcome of such challenges). The Data Importer will retain such information for as long as the Personal Data are subject to the safeguards provided by the EU BCRs and will make it available to the competent DPA upon request. If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the foregoing information, the Data Importer will, without undue delay, inform the Data Exporter accordingly.

16.6. The Data Importer will, in conjunction with the Chief Privacy Officer, review the legality of a request for disclosure by a public authority to determine whether it falls within the powers granted to the requesting public authority. The Data Importer will challenge the request if, after such assessment, it concludes (in conjunction with the Chief Privacy Officer) there are

reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and/or principles of international comity. If the Data Importer believes there are such reasonable grounds to consider the request unlawful, it will pursue possibilities of appeal. When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. The Data Importer will not disclose the Personal Data requested until required to do so under the applicable law and procedural rules of the country of destination. The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter and, upon request, to the competent DPA.

16.7. The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

16.8. In any event, transfers of Personal Data by a Participating Company to any public authority shall not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

16.9. For Participating Companies located in the EEA, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a Data Controller or Data Processor to transfer or disclose Personal Data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or an EEA Member State, without prejudice to other grounds for transfer pursuant to Chapter V GDPR.

17. Internal Complaint Mechanisms

17.1. Amgen will utilize its existing complaint handling process to incorporate handling of any EU BCRs-related complaints or concerns.

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

17.3. Amgen recommends that such complaints are provided in writing either by postal mail or email directly to the Global Privacy Compliance Team or to the Participating Company. The Global Privacy Compliance Team may be contacted using the contact details below:

Address: 25 quai du Président Paul Doumer, 92400 Courbevoie.

Email: privacy@amgen.com

17.4. Amgen Personnel may l, when acceptable according to the laws applicable to the Participating Company, use the Business Conduct Hotline to report an EU BCRs complaint.

17.5. If the complaint is received locally by the Participating Company, the DPO will translate if necessary and forward it without undue delay to the Global Privacy Compliance Team.

17.6. An initial response will be provided to the Data Subject within ten (10) working days informing him/her that their complaint is under consideration and that he or she will receive

substantive response without undue delay and in any event within one month of receipt of the request. Taking into account the complexity and number of the requests, the one-month period may be extended by a maximum of two further months, in which case the Data Subject shall be informed accordingly. The substantive response will include details about our findings and any action Amgen has or proposes to take. If Amgen determines that no action should be taken, this shall be explained to the Data Subject together with reasons for this determination.

17.7. If the complaint is upheld by Amgen, then Amgen will implement appropriate remedial measures. Those measures will be decided on a case by case basis by the Chief Privacy Officer and the Global Privacy Compliance Team, the local DPO and, where applicable, any other relevant department. Furthermore, if the Global Privacy Compliance Team discovers individual wrongdoing, appropriate disciplinary measures will be taken, up to and including termination of employment or engagement, to the extent permitted by Applicable Law.

17.8. The Data Subject will receive an answer informing him/her of the outcome of his complaint. This shall be without undue delay and in any event within one month of receiving the complaint (with sufficient details for Amgen to identify the nature of the complaint and, only where reasonably necessary, with any information requested to confirm the complainant's identity). Taking into account the complexity and number of the requests, the one-month period may be extended by a maximum of two further months, in which case the Data Subject shall be informed accordingly.

17.9. The Data Subject will be informed that if he/she is not satisfied by Amgen's answer, he/she can lodge a claim before the courts of an EEA Member State or the competent DPA. However, it is not a requirement that a Data Subject first go through Amgen's complaint handling process before he or she can complain to the competent DPA or bring a claim before the courts of an EEA Member State.

17.10. This complaint handling process will be made public through the publication of the EU BCRs as mentioned in Article 7 above.

18. Third Party Beneficiary Rights and Liability

18.1. A Data Subject whose Personal Data originates from the EEA or is protected by the EU Data Protection Laws and is transferred to Participating Companies outside the EEA shall have the right to enforce the EU BCRs as a third-party beneficiary and shall have the right to seek judicial redress, obtain remedies and, where appropriate, compensation for actual damage suffered as a result of breach of these EU BCRs. Any such claims can be brought by the Data Subject before a competent DPA (which may be the DPA in the EEA Member State in which the Data Subject habitually resides, or the DPA of his/her place of work or the DPA of the place of the alleged infringement). Data Subjects may also bring a claim before a competent court in an EEA Member State (which may be the courts of the EEA Member State where the relevant Participating Company has an establishment or the courts of the EEA Member State where the Data Subject has his/her habitual residence). A Data Subject may be represented in the exercise of its right to an effective judicial remedy against a Participating Company by a not-for-profit body, organisation, or association provided such body, organisation or association has been properly constituted in accordance with Applicable Law, has statutory objectives which are in the public interest, and is active in the field of the protection of Data Subjects' rights and freedoms relating to the protection of their Personal Data. The Data Subject shall be able to enforce the following Articles as a third party beneficiary:

18.1.1. Articles 1 (Scope), 2 (Definitions), 3 (Purpose Limitation), 4 (Data Quality and Proportionality), 5 (Legal Basis for Processing Personal Data) and 6 (Processing Sensitive Personal Data);

18.1.2. Article 7 (Transparency and Information Rights);

18.1.3. Articles 8 (Rights of Access, Rectification, Erasure and Restriction of Data) and 9 (Automated Individual Decisions);

18.1.4. Article 10 (Security and Confidentiality), 11 (Relationships with Data Processors (Amgen Data Importer or Vendor) and 12 (Restriction on Transfers and Onward Transfers);

18.1.5. Articles 16 (Actions in Case of National Legislation Preventing Respect of the EU BCRs) and 21 (Relationship between National Laws and the EU BCRs);

18.1.6. Article 18 (Third Party Beneficiary Rights and Liability); and

18.1.7. Article 19 (Mutual Assistance and Cooperation with the DPAs).

18.2. For the avoidance of doubt, the third party beneficiary rights do not extend to those Articles and elements of these EU BCRs which pertain to internal mechanisms implemented within Participating Companies or the Amgen group such as details regarding training (including Appendix 2), audit programmes, internal compliance networks and structure and the mechanism for updating the EU BCRs.

18.3. Amgen France accepts responsibility for and agrees to take such action as is reasonably necessary to remedy the acts of Participating Companies established outside the EEA. Amgen France shall pay compensation for any material or non-material damages resulting from the violation of these EU BCRs, unless it can demonstrate that the Participating Company established outside the EEA is not responsible for the event giving rise to the damage. Amgen France has sufficient financial means and insurance cover to cover damages under the EU BCRs.

18.4. Any Data Subject who has suffered damage arising from a breach of these EU BCRs by a Participating Company not established in the EEA is entitled, where appropriate, to receive compensation from Amgen France for the damage suffered and the courts or other competent authorities in the EEA shall have jurisdiction. The Data Subject shall have the rights and remedies against Amgen France as if the violation had been caused by Amgen France in the EU instead of the Participating Company not established in the EEA. If the Participating Company not established in the EEA is responsible or held liable for such breach, it will to the extent to which it is responsible or liable, indemnify Amgen France for any cost, charge, damage, expense or loss Amgen France incurs in relation to such breach.

18.5. In the event of a claim by a Data Subject that he/she has suffered damage and has established it is likely that such damage occurred because of a breach of these EU BCRs, the burden of proof to show that the damages suffered by the Data Subject due to a breach of these EU BCRs are not attributable to relevant Participating Company shall rest with Amgen France. If Amgen France can demonstrate that the Participating Company established outside the EEA is not responsible for the event giving rise to the damage, it shall not be liable or responsible for the damage.

19. Mutual Assistance and Cooperation with the DPAs

19.1. Participating Companies shall cooperate and assist each other to handle a request or complaint from a Data Subject or an investigation or inquiry by the competent DPA.

19.2. Participating Companies will answer, in collaboration with the Chief Privacy Officer, EU BCRs-related requests from the competent DPA within an appropriate timeframe in view of the circumstances of the request (and in any event no later than any deadline imposed by the competent DPA) and in an appropriate detail based on the information reasonably available to the Participating Company. In relation to the implementation and ongoing application of the EU BCRs, Participating Companies shall give due consideration to the communications and recommendations of the competent DPA and shall comply with any formal decisions or notices issued by the competent DPA.

19.3. Any dispute related to a competent DPA's exercise of supervision of compliance with these EU BCRs will be resolved by the courts of the member state of that DPA, in accordance with that member state's Applicable Law.

20. EU BCRs Updating and Changes

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

20.2. Amgen will promptly and without undue delay report any significant changes to the EU BCRs or to the list of Participating Companies to all other Participating Companies and to the competent DPA to take into account modifications of Applicable Law, the regulatory environment and/or the Amgen group structure. In particular where a modification would affect the level of protection offered by the EU BCRs, the Chief Privacy Officer will promptly communicate such modification in advance to the competent DPA with a brief explanation of the reasons for the modification. Some modifications might require a new approval from the competent DPA.

20.3. The Chief Privacy Officer will keep a fully updated list of the Participating Companies of the EU BCRs and track any updates to the rules as well as provide the necessary information to the Data Subjects or the competent DPA upon request. Any administrative changes to the EU BCRs will be reported to Participating Companies on a regular basis.

20.4. No transfer of Personal Data will be made to a new Participating Company under the guarantees of the EU BCRs until the new Participating Company is effectively bound by the EU BCRs and in compliance with the EU BCRs.

20.5. Any administrative changes to the EU BCRs or to the list of Participating Companies will be reported to the Participating Companies on a regular basis and reported at least once a year to the competent DPA with a brief explanation regarding the reasons for the update.

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

21. Relationship between National Laws and the EU BCRs

21.1. Where the local national laws applicable to a Participating Company require a higher level of protection for Personal Data it will take precedence over the EU BCRs. If the local national laws applicable to a Participating Company provide a lower level of protection for Personal Data than the EU BCRs, the EU BCRs will be applied.

21.2. In the event that obligations arising from the local national laws applicable to a Participating Company are in conflict with the EU BCRs, the Participating Company shall inform the Chief Privacy Officer without undue delay and shall comply with the additional requirements set out in Article 16 above.

21.3. In any event, Personal Data shall be Processed in accordance with Article 5 of the GDPR and relevant local legislation.

22. Final Provisions

22.1. The EU BCRs shall be effective upon approval by the competent DPA and be applicable to the Participating Companies upon signing the EU BCRs Adoption Agreement.

22.2. No transfer shall be made to a Participating Company unless it is bound by these EU BCRs. Where a Data Importer ceases to be bound by the EU BCRs, it must promptly return or delete all Personal Data (including copies thereof) that has been transferred under these EU BCRs, except that provided the Data Importer provides legally binding obligations to maintain protection of the Personal Data in accordance with Chapter V of the GDPR it may retain Personal Data that has been transferred under these EU BCRs.

22.3. The Data Importer must promptly inform the Data Exporter, Amgen France and the Chief Privacy Officer if it is unable for any reason to comply with these EU BCRs (including the situations described in Article 12.3 above). Where the Data Importer is in breach of these EU BCRs, or is unable to comply with them, the Data Exporter must notify the Chief Privacy Officer and suspend the transfer of Personal Data.

22.4. At the choice of the Data Exporter, the Data Importer must immediately return or delete all Personal Data (including copies thereof) that has been transferred under these EU BCRs, and shall certify the same to the Data Exporter, where:

22.4.1. the Data Exporter has suspended the transfer of Personal Data, and compliance with these EU BCRs is not restored within a reasonable time, and in any event within one month of the suspension; or

22.4.2. the Data Importer is in material breach of these EU BCRs; or

22.4.3. the Data Importer fails to comply with a binding decision of a competent court or competent DPA regarding its obligations under these EU BCRs.

Until the Personal Data has been deleted or returned, the Data Importer must continue to ensure compliance with these EU BCRs. If local national laws applicable to the Data Importer prohibit the return or deletion of the Personal Data transferred under these EU BCRs, the Data Importer must continue to ensure compliance with these EU BCRs and only Process the Personal Data to the extent and for as long as required under such local national laws.

23. Appendices

The attached appendixes are integrally part of the EU BCRs.

Appendix 1: Overview of Amgen Data Flows

Appendix 2: Overview of Amgen Training Program

Appendix 1: Overview of Amgen Data Flows

Data subjects	Categories of data	Purposes	Transfer
Employee	Identification data such as name, address, date and place of birth, hire date, social security numbers, credit card numbers, bank account and financial information, and driver's license and government-issued identification card numbers Vacations and benefits, grievances, bonuses, promotions, reviews and evaluations, work records, information related to health and welfare coverage, retirement plan and stock option details Tax and financial personal information Sensitive data such as national origin, when permitted by local law	Personnel management, information technology support and administration purposes in connection with the employment relationship and benefits, or the administration of post-employment benefits, as well as to comply with Amgen's legal, administrative and corporate obligations	Amgen global data bases are located in the USA where Amgen Inc., the headquarters, is based. Data are flowing from Amgen France (or the relevant Data Exporter) to Amgen Inc. in the United States or to Participating Companies in Switzerland. Then, the data may: - simply be stored and maintained there - be analyzed to provide global statistics and reports - be shared onward inside the Amgen group to other Participating Companies where there is a business need for such access by specific personnel or business functions at those Participating Companies (ex: an employee applying for a job outside his country or having to report to a manager based outside of his country). In most cases, such Participating Companies will act as Data Controllers, but depending
Healthcare Professionals	Name, business contact information including phone number and email address, field of expertise Professional background (resume) Participation in other research Financial information (billing and payment information)	Administration and management of Amgen's professional and scientific activities – Research & Development (for example, participation in medical research, clinical studies, professional meetings or congresses) Promotion of Amgen's products and services Disclosure of financial information when required by applicable law or adherence to industry code Regulatory compliance such as safety monitoring and adverse event reporting	

Vendors / Suppliers	Individual name, organization name, business contact information Billing and payment information	Processing of payments to vendors and suppliers Regulatory compliance such as tax law	on the business need, Participating Companies may also act as Data Processors (ex: in providing IT Help Desk support or providing support relating to the HR Connect Service Centre).
Clinical Trial Data Subjects (which may include children under the age of 18 where there is a pediatric patient involved in a clinical study sponsored by Amgen).	Coded data – patient name and contact information is replaced with an internally generated identification number. Only the clinical trial site (hospital/research location) maintains the list to tie the identification number back to the patient name. Indirect identifiers such as year or date of birth (full date of birth is only collected for pediatric studies), sex, weight, height. Health data necessary as outlined within the research study protocol. Other data relating to the patient necessary for the conduct of the research including ethnicity, family situation (such as number of children), consumption of drugs, alcohol, drugs, general habits or behaviors, professional situation such as job, unemployment, participation in other research.	Administration and management of biomedical research (clinical trials, observatory studies)	
Patients (which may include children under the age of 18 where there is an adverse event involving the use of an Amgen product with a pediatric indication).	Indirect identifiers of the patient such as age, year or date of birth, patient initials (as permitted by local law), sex, weight / height, or identification number of the patient (excluding national health identifiers).	Regulatory compliance and pharmacovigilance such as safety monitoring and adverse event reporting (when permitted by local law)	

	Data relating to the identification of the Amgen product such as product or device used, serial numbers of devices, delivery method or dosage of product, lot / batch numbers of product. Health data including treatments administered, results of examinations, nature of any undesirable effect(s), personal or family medical history, associated illnesses or events, risk factors, information relating to the prescription and use of medicines and to the therapeutic conduct of the health professionals involved in the management of the patient's disease. Other data relating to the patient necessary for the assessment of the adverse health event in accordance with regulatory compliance obligations such as ethnicity, professional life, consumption of drugs, alcohol, drugs, and/or general habits or behaviors.		

Appendix 2: Overview of Amgen Training Program

Privacy and Data Protection Training / Awareness Program

The Privacy and Data Protection Training Program strives to ensure that all Amgen Personnel are properly trained regarding Amgen EU BCRs as well as any legal obligations that impact Processing of Personal Data. This program contains various elements.

General training for all Amgen Personnel

All Amgen Personnel must perform an annual online training on data protection as part of the Code of Conduct Training. This training is mandatory and monitored and usually takes around 75 minutes to complete. This training includes the EU BCRs and information regarding the consequences under criminal and employment law and/or their contract for services for Personnel who breach the EU BCRs.

Specific training to DPOs

All Amgen DPOs are regularly trained on new processes through regular DPO calls performed by the Global Privacy Compliance Team and privacy workshops onsite and/or online on a need-to-know basis. All DPOs have access to a wiki page that answers the most frequently asked questions and provides guidance as well as links to external resources.

Specific training to Personnel

Specific training may be delivered on a need-to-know basis either online or onsite or through posting information on the Amgen intranet. This training may be focused on specific groups that may either Process Personal Data on a daily basis or support other groups that Process Personal Data. For instance, the audit group, R&D functions, and the legal department are regularly trained. This includes information on procedures for managing requests for access to Personal Data by public authorities, where relevant to specific Personnel. This training can happen either at a regional level or on a country level. Further specific EU BCRs training may be developed on a need-to-know basis.

Awareness

Amgen has a dedicated page on its intranet on Privacy and Data Protection that provides links to other resources either internally or externally.

Amgen's Global Privacy Compliance Team collaborates with the Information Security department on the Sentinel program which is a global program to raise awareness of Amgen Personnel on information security.

Training support

All privacy-related trainings are developed by the Global Privacy Compliance Team and approved by the Chief Privacy Officer. The training may either be directly performed by a Global Privacy Compliance Team member or by a local DPO on a "train the trainer" model.