Amgen UK Binding Corporate Rules (UK BCRs)

Introduction

Amgen is a biotechnology leader committed to serving patients with grievous illness. These UK Binding Corporate Rules ("**UK 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 Participating Companies.

All Amgen Participating Companies and all Personnel are committed to respecting, and are legally bound by, these UK BCRs in respect of Personal Information within the UK 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 UK 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 UK BCRs.

These UK BCRs have been adopted in reference to the UK Data Protection Laws. Amgen UK is responsible for ensuring compliance by the Amgen Participating Companies with these UK BCRs. Individuals can enforce these UK BCRs against Amgen UK as a third-party beneficiary as described below. These UK 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

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

a) the Amgen Participating Company which Processes the Personal Information is established in the UK; or

b) the Amgen Participating Company which Processes the Personal Information is not established in the UK and has received the Personal Information from an Amgen Participating Company established in the UK; or

c) to onward transfers of Personal Information from Data Importers to Data Importers.

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

2 – Definitions

Terms	*Definitions*
Amgen UK	Amgen Limited, a company incorporated in England and Wales under company number 02354269 and whose registered office is at 216 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, England, CB4 0WA.
Applicable Law	The law of the United Kingdom or a part of the United Kingdom (including without limitation the UK Data Protection Laws).
Compliance Lead	A person within the Healthcare Compliance division of the Worldwide Compliance and Business Ethics department at an Amgen 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 Information relating to him/her.
Data Controller	Any entity which makes decisions with regard to the collection and Processing of Personal Information, including decisions about the purposes for, and manner in which, Personal Information is Processed.
Data Exporter	An Amgen Participating Company operating as a Data Controller established in the UK that transfers Personal Information to a Data Importer.
Data Importer	An Amgen Participating Company which is not established in the UK that either (a) receives Personal Information from a Data Exporter or (b) receives an onward transfer of Personal Information pursuant to Article 1(c) of these UK BCRs.
Data Processor	A person or entity that processes Personal Information on behalf of a Data Controller.
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 Information. A Data Subject may be (without limitation): • a patient / clinical trial data subject (which may include a child under the age of 18)

Terms	***Definitions***
	• a healthcare professional • an employee • a vendor or supplier
Participating Company	A legal entity from the Amgen group that is bound by the UK BCRs.
Personal Information	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 Information 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.
Personnel	All staff members and contingent workers (including consultants, temporary agency workers and contract workers) of any Amgen Participating Company.
Privacy Incident	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed.
Processing	Any operation or set of operations which is performed on Personal Information (or sets of Personal Information), whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive Personal Information	Personal Information 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 UK Data Protection Laws, Amgen also considers financial information and information that could be used to perpetrate

Terms	*Definitions*
	identity theft (e.g., Social Security Number, driver's license number, credit card or other bank account information) as Sensitive Personal Information.
Technical and Organizational Security Measures	Technological and organizational 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.
Third Party	A natural or legal person, public authority, agency or any other body other than the Data Subject, the Amgen Participating Company acting as Data Controller and an Amgen 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 Information.
Vendor	Any natural or legal person, business or organization that provides goods and/or services to an Amgen Participating Company under a contractual relationship and/or is a recipient of Personal Information from such Amgen Participating Company in order to render those good and/or services.
UK ICO	The UK Information Commissioner's Office, as the UK's independent data protection authority.
UK	The United Kingdom.
UK Data Protection Laws	The UK GDPR, the Data Protection 2018 and any other data protection law or regulation applicable in the UK from time to time.
UK GDPR	The retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020/1586).

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

3 – Purpose Limitation

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

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

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

4 - Data Quality and Proportionality

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

Personal Information 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 UK GDPR.

Personal Information 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 considered, 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'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 Information

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

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

- 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.

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

- 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.

- 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.

- 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.

6 – Processing of Sensitive Personal Information

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

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

- 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.

- 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.

- 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.

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

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

- 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.

- The Processing of the Sensitive Personal Information 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 Information 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 the UK or by another person also subject to an obligation of secrecy under Applicable Law or rules established by competent bodies in the UK.

- The Processing of Sensitive Personal Information 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.

- The Processing of Sensitive Personal Information 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 UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) 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

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

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

Where the Personal Information 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

Every Data Subject has the right to obtain from the Participating Company confirmation as to whether or not Personal Information concerning him or her are being Processed, and, where that is the case, access to the Personal Information and the information required to be provided by Article 15(1) of the UK 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.

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

Every Data Subject has the right to object, at any time on grounds relating to their particular situation, to the Processing of their Personal Information 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 Information 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.

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, 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 Information relating to him or her for the purposes of direct marketing, the Participating Company must cease Processing the Personal Information for that purpose.

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

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

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.

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

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 UK ICO 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

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:

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

- 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

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

10 – Security and Confidentiality

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

Amgen has processes in place to ensure that Privacy Incidents are subject to reporting, tracking and appropriate corrective actions, as necessary. Any Privacy Incident shall be documented (including the facts relating to the Privacy Incident, its effects and the remedial action taken) and the documentation shall be made available to the UK ICO on request. Furthermore, Participating Companies shall notify without undue delay any Privacy Incident to Amgen UK and the Chief Privacy Officer and the other relevant privacy officer/function and, where the Privacy Incident is likely to result in a high risk to their rights and freedoms, Data Subjects.

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 32 of the UK GDPR.

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

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

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

The Amgen Participating Company (acting as Data Controller) will carefully choose a Data Processor that can be either another Amgen 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.

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.

The Amgen 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 UK GDPR), instruct the Data Processor that, among other things:

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

(ii) 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;

(iii) persons authorised to Process the Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iv) the Data Processor shall not engage another Data Processor without the prior specific or general written authorisation of the Amgen 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 Amgen Participating Company acting as Data Controller and the Data Processor shall be imposed on that other Data Processor;

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

(vi) it must assist the Amgen Participating Company acting as Data Controller in ensuring compliance with the obligations relating to security of Processing, notification of a Privacy Incident to the ICO, communication of a Privacy Incident to the Data Subject, data protection impacts assessments and prior consultation with the ICO, taking into account the nature of Processing and the information available to the Data Processor;

(vii) at the choice of the Amgen Participating Company acting as Data Controller, it must delete or return all the Personal Information to the Amgen Participating Company acting as Data Controller after the end of the provision of services relating to the Processing, and delete existing copies unless UK Data Protection Law requires storage of the Personal Information;

(viii) it must make available to the Amgen 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 Amgen Participating Company acting as Data Controller or another auditor mandated by it.

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

The Amgen 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 UK Data Protection Laws, it shall also be liable for its obligations and responsibilities as a Data Processor under such laws.

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 Amgen Participating Companies acting as Data Controller. The Amgen 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.

12 – Restrictions on Transfers and Onward Transfers

All transfers of Personal Information to Third Parties located outside of the UK shall respect the UK Data Protection Laws on transfers and onward transfers of Personal Information either by making use of the standard contractual clauses authorized under Paragraph 7 of Schedule 21 of the Data Protection Act 2018 or by another adequate means according to Chapter V of the UK GDPR.

All transfers of Personal Information to Data Processors located outside of the UK shall respect the UK 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 Information set out in this Article 12 and in the UK Data Protection Laws.

13 – Training Program

As described in Appendix 2, Amgen provides appropriate training on privacy principles and more specifically on the UK 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 UK BCRs.

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

Specific trainings will be provided on a case by case basis to Personnel 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 Global Privacy Compliance Team provides appropriate information and resources related to privacy, for instance, on the Amgen intranet portal.

14 – Audit and Monitoring Program

The Chief Privacy Officer ensures that all Participating Companies (and their compliance with these UK 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 frequent than every 2 to 3 years (for Amgen 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 Amgen 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 UK 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 UK BCRs), a limited audit of one or more Personal Information 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 UK BCR-related audits at any time. For example, in response to any identified compliance issue or a report of substantive non-compliance, a Privacy Incident and/or a substantive change in the UK Data Protection Laws. The audit program covers all aspects of the UK BCRs including methods of ensuring that corrective actions will take place.

All UK BCR audit reports are communicated to the Chief Compliance Officer and to the Chief Privacy Officer in a timely manner. The UK BCR 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 UK 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.

The UK ICO can receive a copy of UK BCR-related audit reports upon request.

Each Participating Company shall cooperate with and shall accept, without restrictions, to be audited by the UK ICO. 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

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).

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

- advising the board of management;
- ensuring data protection compliance at a global level (including having overall responsibility for the UK BCRs);
- reporting regularly on data protection compliance (including to the Chief Compliance Officer); and
- working with the UK ICO's investigations.

The Global Privacy Compliance Team includes the Chief Privacy Officer, Head of Global Privacy (who reports to the Chief Privacy Officer and 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.

The European Data Protection Officer has been appointed by Amgen as the Data Protection Officer for the EU/EEA, the UK and Switzerland. The European Data Protection Officer has the tasks set out in Article 39 of the UK GDPR. The European Data Protection Officer has a direct reporting line to the Head of Global Privacy and the Chief Privacy Officer as well as senior management at Amgen UK and is supported by the local Compliance Lead in the UK.

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.

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 for 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 an Amgen 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.

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

- 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 UK GDPR. This record should be maintained in writing, including in electronic form, and shall be made available to the Chief Privacy Officer and the UK ICO on request;

- 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 UK 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 UK ICO in accordance with Article 36 of the UK GDPR.

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

Where a Participating Company has reason to believe that the laws applicable to it prevents the Participating Company from fulfilling its obligations under the UK 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 UK.

Where there is conflict between local national law and the commitments in the UK 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 UK ICO.

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 UK BCRs, the Chief Privacy Officer (and Amgen UK) shall be promptly notified, and the Chief Privacy Officer shall notify the UK ICO. This includes any legally binding request for disclosure of the Personal Information by a law enforcement authority or state security body. In such a case, the UK ICO should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the

confidentiality of a law enforcement investigation). 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 that it did so. If, despite having used its best efforts, the Participating Company receiving the request is not able to notify the UK ICO, the Participating Company, in conjunction with the Chief Privacy Officer, shall annually provide general information on the requests it receives to the UK ICO.

In any event, transfers of Personal Information 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.

17 – Internal Complaint Mechanisms

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

Any Data Subject may complain, at any time, that any Participating Company is not complying with the UK 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.

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: Amgen Limited, 216 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, CB4 0WA, UK. Email: privacy@amgen.com

Amgen Personnel may as well, when acceptable according to the laws applicable to the Participating Company, use the Business Conduct Hotline to report a UK BCRs complaint.

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.

An initial response will be provided to the Data Subject within ten (10) working days informing that his/her 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.

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.

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.

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 UK courts or the UK ICO. 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 UK ICO or bring a claim before the UK courts.

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

18 - Third Party Beneficiary Rights and Liability

A Data Subject whose Personal Information originates from the UK or is protected by the UK Data Protection Laws and is transferred to Participating Companies outside the UK shall have the right to enforce the UK 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 UK BCRs. Any such claims can be brought by the Data Subject before the UK ICO. Data Subjects may also bring a claim before a competent court in the UK. The Data Subject shall be able to enforce the following Articles as a third party beneficiary:

- Articles 1, 2, 3, 4, 5 and 6;
- Article 7;
- Articles 8 and 9;
- Article 10, 11 and 12;
- Articles 16 and 21;
- Article 18; and
- Article 19.

For the avoidance of doubt, the third party beneficiary rights do not extend to those Articles and elements of these UK 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 UK BCRs.

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

Any Data Subject who has suffered damage arising from a breach of these UK BCRs by a Participating Company not established in the UK is entitled, where appropriate, to receive compensation from Amgen UK for the damage suffered and the courts or other competent authorities in the UK shall have jurisdiction. The Data Subject shall have the rights and remedies against Amgen UK as if the

violation had been caused by Amgen UK in the UK instead of the Participating Company not established in the UK. If the Participating Company not established in the UK is responsible or held liable for such breach, it will to the extent to which it is responsible or liable, indemnify Amgen UK for any cost, charge, damage, expense or loss Amgen UK incurs in relation to such breach.

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 UK BCRs, the burden of proof to show that the damages suffered by the Data Subject due to a breach of these UK BCRs are not attributable to relevant Participating Company shall rest with Amgen UK. If Amgen UK can demonstrate that the Participating Company established outside the UK 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 UK ICO

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 UK ICO.

Participating Companies will answer, in collaboration with the Chief Privacy Officer, UK BCRs-related requests from the UK ICO within an appropriate timeframe in view of the circumstances of the request (and in any event no later than any deadline imposed by the UK ICO) 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 UK BCRs, Participating Companies shall give due consideration to the communications and recommendations of the UK ICO and shall comply with any formal decisions or notices issued by the UK ICO.

20 – UK BCRs Updating and Changes

Amgen reserves the right to change and/or update these UK BCRs at any time. Such update of the UK 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 UK ICO.

Amgen will promptly report any significant changes to the UK BCRs or to the list of Participating Companies to all other Participating Companies and to the UK ICO to take into account modifications of Applicable Law, the regulatory environment and/or the Amgen group structure. Some modifications might require a new approval from the UK ICO.

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

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

Any administrative changes to the UK 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 UK ICO 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 UK BCRs.

21 – Relationship between National Laws and the UK BCRs

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

In the event that obligations arising from the local national laws applicable to a Participating Company are in conflict with the UK 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.

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

22 – Final Provisions

The UK BCRs shall be effective upon approval by the UK ICO and be applicable to the Amgen Participating Companies upon signing the UK BCRs Adoption Agreement.

23 – Appendices

The attached appendixes are integrally part of the UK BCRs.

Appendix 1: Overview of Amgen UK's Data Flows

Appendix 2: Overview of Amgen Training Program

Appendix 1: Overview of Amgen UK 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 Finance 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 UK (or the relevant Data Exporter) to Amgen Inc. in the United States or to Amgen 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 Amgen 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 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).
Healthcare Professionals	Name, business phone number, business email address and Field of expertise Professional background (resume) Participation to other research Financial information (billing and payment information)	Administration and management of Amgen's professional and scientific activities – R&D (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 "sunshine act" Regulatory compliance such as safety monitoring, adverse event reporting or transparency requirements	
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	
Clinical Trial Data Subjects / Patients (which may include children under the age of 18 where (1) there is a pediatric patient involved in a clinical	Coded data, health data, date of birth, place of birth, sex, weight, height, ethnicity, family situation (such as marital status, children), financial situation such as reimbursement, professional situation such as job, unemployment, participation to other research;	Administration and management of biomedical research (clinical trial, observatory studies) Regulatory compliance such as safety monitoring and adverse event reporting (when permitted by local law)	

study sponsored by Amgen, or (2) there is an adverse event involving the use of an Amgen product with a pediatric indication)	commutes, consumption of drugs, alcohol, drugs, and general habits or behaviors (when permitted by local law)		

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 UK BCRs as well as any legal obligations that impact Processing of Personal Information. 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. By the end of Q2 2022, this training will also include the UK BCRs and information regarding the consequences under criminal and employment law and/or their contract for services for Personnel who breach the UK BCRs. See "Specific training to Personnel" below for the specific training on the UK BCRs which will be provided in the interim.

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 on UK BCRs will be provided to the DPOs, including a communication package to cascade the UK BCRs requirements to their local management team.

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 Information on a daily basis or support other groups that Process Personal Information. For instance, the audit group, R&D functions, and the legal department are regularly trained. This training can happen either at a regional level or on a country level. Prior to the inclusion of UK BCRs training as part of the Code of Conduct Training in 2022, the UK BCRs will be assigned as an online read and acknowledge training to existing and new Personnel promptly following the approval of the UK BCRs by the ICO. This training must be completed within 30 days of assignment. Further specific UK 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.