Amgen EU verbindliche interne Datenschutzvorschriften - Datenverantwortlicher (EU BCRs)

Zuletzt aktualisiert: 12. Dezember 2023

Einleitung

(A) Amgen ist ein führendes Biotech-Unternehmen, das sich für die Behandlung von Patienten mit schwerwiegenden Erkrankungen einsetzt. Diese verbindlichen internen Datenschutzvorschriften - Verantwortlicher („**EU BCRs**“) enthalten die Verpflichtungen von Amgen in Sachen Privatsphäre und Datenschutz, weil das Unternehmen sich dafür einsetzt, bei der Übermittlung und der Verarbeitung von personenbezogenen Daten zwischen beteiligten Unternehmen für einen angemessenen Schutz zu sorgen.

(B) Alle beteiligten Unternehmen und alle Angestellten setzen sich dafür ein, diese EU BCRs im Hinblick auf personenbezogene Daten innerhalb des Geltungsbereichs der EU BCRs einzuhalten, und sie sind gesetzlich daran gebunden. Verstöße können zu Disziplinarmaßnahmen führen, wie sie gemäß den Gesetzen am jeweiligen Standort zulässig sind. Der Chief Compliance Officer sorgt in Zusammenarbeit mit dem Chief Privacy Officer für die Durchsetzung der EU BCRs. Eine Liste der beteiligten Unternehmen finden Sie unter: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. Bei Fragen bezüglich dieser EU BCRs sind alle beteiligten Unternehmen per E-Mail an privacy@amgen.com erreichbar.

(C) Diese EU BCRs sind unter Bezugnahme auf die Datenschutzgesetze der EU eingeführt worden. Amgen Frankreich ist für die Einhaltung dieser EU BCRs seitens der beteiligten Unternehmen verantwortlich. Wie nachstehend beschrieben können Einzelpersonen diese EU BCRs gegen Amgen Frankreich als Drittbegünstigter durchsetzen. Diese EU BCRs stehen auf der Website von Amgen unter: www.amgen.com/bcr zur Verfügung. Alternativ wenden Sie sich bitte an privacy@amgen.com, um eine Kopie zu erhalten.

1. Anwendungsbereich

1.1. Die Amgen EU BCRs gelten für Übermittlungen und die Verarbeitung, jeweils automatisiert oder händisch, aller personenbezogenen Daten von betroffenen Personen, die von einem beteiligten Unternehmen durchgeführt wird, das als Datenverantwortlicher oder Datenverarbeiter für ein anderes beteiligtes Unternehmen auftritt, das in den nachstehenden Fällen als Datenverantwortlicher handelt:

1.1.1. Das beteiligte Unternehmen, von dem die personenbezogenen Daten verarbeitet werden, ist in der EU ansässig; oder

1.1.2. Das beteiligte Unternehmen, von dem die personenbezogenen Daten verarbeitet werden, ist nicht im EWR ansässig und hat personenbezogene Daten von einem beteiligten Unternehmen erhalten, das im EWR ansässig ist; oder

1.1.3. Bei Weiterleitungen von personenbezogenen Daten von Datenimporteuren an Datenimporteure.

1.2. Eine Übersicht der Datenflüsse gemäß diesen EU BCRs ist in Anlage 1 enthalten.

2. Definitionen

Begriffe	*Definitionen*
Amgen Frankreich	Amgen S.A.S., eine in Frankreich gegründete Gesellschaft mit eingetragenem Sitz in 25 quai du Président Paul Doumer, 92400 Courbevoie.
Geltendes Recht	Das Recht der EU und/oder (sofern zutreffend) das nationale oder lokale Recht des EWR-Vertragsstaats (insbesondere einschließlich der EU-Datenschutzgesetze).
Compliance Lead	Eine Person innerhalb der Sparte Healthcare Compliance in der Abteilung Worldwide Compliance and Business Ethics bei einem beteiligten Unternehmen, die über die delegierte Verantwortung zum Datenschutz und zum Schutz der Privatsphäre verfügt und die den Datenschutzbeauftragten vor Ort bei seinen Aufgaben und Tätigkeiten unterstützt, wenn der Compliance Lead nicht gleichzeitig der Datenschutzbeauftragte ist.
Einwilligung	Jede freiwillig erteilte, spezifische, informierte und eindeutige Angabe der Wünsche einer betroffenen Person, mit der die betroffene Person mittels einer Erklärung oder eindeutig zustimmenden Handlung ihre Zustimmung zur Verarbeitung ihrer eigenen personenbezogenen Daten erteilt.
Datenverantwortlicher	Jede Stelle, die Entscheidungen im Hinblick auf die Erhebung und Verarbeitung von personenbezogenen Daten fällt, einschließlich Entscheidungen über die Zwecke für die Verarbeitung der personenbezogenen Daten und wie sie erfolgt.
Datenexporteur	Ein beteiligtes Unternehmen, das als Datenverantwortlicher im EWR ansässig ist und das personenbezogene Daten an einen Datenimporteur überträgt.
Datenimporteur	Ein beteiligtes Unternehmen, das nicht im EWR ansässig ist und das entweder (a) personenbezogene Daten von einem Datenexporteur erhält oder (b) eine Weiterleitung von personenbezogenen Daten gemäß Artikel 1(c) dieser EU BCRs erhält.
Datenverarbeiter	Eine Person oder Stelle, die personenbezogene Daten im Auftrag eines Datenverantwortlichen verarbeitet.
Datenschutzbehörde	Eine unabhängige, öffentliche Datenschutzbehörde mit Sitz in einem EWR-Vertragsstaat.
Datenschutzbeauftragter	Eine Person, die vom Chief Privacy Officer von Amgen ernannt wurde und die für die Beaufsichtigung des Schutzes der Privatsphäre und des Datenschutzes vor Ort sowie die Umsetzung angemessener und notwendiger Kontrollen verantwortlich ist.
Betroffene Person	Eine natürliche Person, die unter Bezugnahme auf personenbezogene Daten direkt oder indirekt identifiziert werden kann. Die folgenden Personen können betroffene Personen sein (nicht abschließend): • Ein Patient / eine betroffene Person in einer klinischen Prüfung (möglicherweise auch ein Kind unter 18 Jahren) • Eine medizinische Fachperson

Begriffe	*Definitionen*
	• Angestellte • Anbieter oder Lieferant
EWR	Die Mitgliedsländer der Europäischen Union (Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Polen, Portugal, die Republik Zypern, Rumänien, Schweden, die Slowakei, Slowenien, Spanien, die Tschechische Republik und Ungarn) sowie Island, Liechtenstein und Norwegen (zusammen die „**EWR-Vertragsstaaten**“).
EU-Datenschutzgesetze	Die DSGVO und (sofern zutreffend) die lokalen oder nationalen Gesetze bezüglich des Datenschutzes und der Verarbeitung von personenbezogenen Daten sowie zur Umsetzung der DSGVO in einem betroffenen EWR-Vertragsstaat.
DSGVO	Die Datenschutzgrundverordnung ((EU) 2016/679).
Beteiligtes Unternehmen	Eine Gesellschaft im Amgen-Konzern, die den EU BCRs unterliegt.
Personenbezogene Daten	Jede Information, die sich auf eine betroffene Person bezieht, z. B. ein Name, eine Identifikationsnummer, Standortdaten, ein Online-Identifikator oder die sich auf einen oder mehrere spezifische Faktoren oder Informationen im Hinblick auf die körperliche, physiologische, genetische, geistige, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person bezieht. Zu den Beispielen für personenbezogene Daten gehören unter anderem: • Name, Adresse, Sozialversicherungsnummer, Führerscheinnummer, Kontodaten, Familiendaten oder medizinische Daten einer betroffenen Person, • Name, berufliche Ausbildung und Verschreibungspraktiken einer medizinischen Fachperson, • Die von Besucherinnen oder Besuchern einer Website von Amgen angegebene E-Mail-Adresse oder sonstige identifizierende Informationen. Die vorstehende Liste enthält lediglich Beispiele und ist nicht abschließend.
Verletzung des Schutzes personenbezogener Daten	Jede Sicherheitsverletzung, die zu unbeabsichtigten oder rechtswidrigen Zerstörungen, Verlusten, Änderungen, nicht autorisierten Offenlegungen oder Zugriffen auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.
Angestellte	Alle Angestellten und befristeten Angestellten (einschließlich Berater, Zeitarbeitnehmer und Leiharbeiter) in einem beteiligten Unternehmen.
Verarbeitung	Jeder Vorgang oder jede Reihe von Vorgängen, die mit oder ohne Hilfe automatisierter Verfahren im Zusammenhang mit personenbezogenen Daten (oder personenbezogenen Datensätzen) ausgeführt werden, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Begriffe	*Definitionen*
Sensible personenbezogene Daten	Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und die Verarbeitung von genetischen Daten und biometrischen Daten für den Zweck der eindeutigen Identifikation einer natürlichen Person und Gesundheitsdaten oder Daten zum Sexualleben einer natürlichen Person oder ihrer sexuellen Orientierung. Getrennt von den EU-Datenschutzgesetzen sieht Amgen auch Finanzinformationen sowie Informationen, die zur Begehung von Identitätsdiebstahl verwendet werden können (z. B. Sozialversicherungsnummer, Führerscheinnummer, Kreditkarten- oder sonstige Kontodaten), als sensible personenbezogene Daten an.
Technische und organisatorische Schutzmaßnahmen	Technische und organisatorische Maßnahmen, die dem Schutz der personenbezogenen Daten vor unbeabsichtigten oder rechtswidrigen Zerstörungen oder unbeabsichtigten Verlusten, Änderungen, nicht autorisierten Offenlegungen oder Zugriffen dienen, insbesondere in Fällen, in denen die Verarbeitung eine Übermittlung der Daten über ein Netzwerk umfasst, sowie vor allen sonstigen rechtswidrigen Formen der Verarbeitung.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem beteiligten Unternehmen, das als Datenverantwortlicher auftritt, und dem beteiligten Unternehmen, das als Datenverarbeiter auftritt. Bei Amgen wird ein Anbieter als Dritter angesehen. Abhängig von den jeweiligen Umständen kann ein Dritter im Hinblick auf die Verarbeitung von personenbezogenen Daten als Datenverantwortlicher oder Datenverarbeiter auftreten.
Anbieter	Natürliche oder juristische Personen, Firmen oder Organisationen, die den beteiligten Unternehmen im Rahmen einer vertraglichen Beziehung Waren und/oder Dienstleistungen zur Verfügung stellen und/oder die ein Empfänger von personenbezogenen Daten von einem solchen beteiligten Unternehmen sind, um diese Waren zu liefern und/oder diese Dienstleistungen zu erbringen.

Amgen wird die Bedingungen in diesen EU BCRs gemäß den EU-Datenschutzgesetzen auslegen.

3. Zweckbindung

3.1. Personenbezogene Daten müssen gemäß Artikel 5(1)(b) DSGVO für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.

3.2. Die personenbezogenen Daten werden nicht in einer Weise verarbeitet, die nicht mit dem geltenden Recht oder den legitimen Zwecken vereinbar ist, für die die Daten erhoben wurden. Datenimporteure sind verpflichtet, sich bei der Speicherung und/oder Weiterverarbeitung von personenbezogenen Daten oder bei der Verarbeitung von personenbezogenen Daten, die ihnen von einem anderen beteiligten Unternehmen übermittelt wurden, an die ursprünglichen Zwecke zu halten. Der Zweck der Verarbeitung von personenbezogenen Daten darf nur mit Einwilligung der betroffenen Person oder in dem nach geltendem Recht zulässigen Ausmaß geändert werden.

3.3. Für sensible personenbezogene Daten werden zusätzliche Schutzmaßnahmen angewendet, wie gemäß den EU-Datenschutzgesetzen vorgesehen.

4. Datenqualität und Proportionalität

4.1. Personenbezogene Daten müssen richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

4.2. Personenbezogene Daten müssen gemäß Artikel 5(1)(c) DSGVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

4.3. Die Verarbeitung personenbezogener Daten erfolgt gemäß der Zielsetzung einer Einschränkung der Erhebung, Verarbeitung und/oder Verwendung der personenbezogenen Daten auf das Notwendige, d. h. so wenig personenbezogene Daten wie möglich. Die Möglichkeit anonymer oder pseudonymisierter Daten muss in Erwägung gezogen werden, vorausgesetzt, dass die Kosten und Anstrengungen für den beabsichtigten Zweck verhältnismäßig sind.

4.4. Personenbezogene Daten, die nicht länger für den wirtschaftlichen Zweck benötigt werden, für den sie ursprünglich erhoben und gespeichert wurden, müssen gemäß den Aufbewahrungsfristen für Aufzeichnungen von Amgen gelöscht werden. Für den Fall, dass gesetzliche Aufbewahrungs- oder Sperrfristen gelten, werden die Daten gesperrt und nicht gelöscht. Am Ende der Aufbewahrungs- oder Sperrfristen werden die Daten gelöscht.

5. Gesetzliche Grundlage für die Datenverarbeitung

5.1. Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

5.1.1. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.

5.1.2. Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

5.1.3. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Datenverantwortliche laut geltendem Recht unterliegt.

5.1.4. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen, wie Leben, Gesundheit oder Sicherheit, der betroffenen Person oder einer anderen natürlichen Person zu schützen.

5.1.5. Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt erfolgt, die dem Datenverantwortlichen übertragen wurde.

5.1.6. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Datenverantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

5.2. Die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten erfolgt nur, wenn die Verarbeitung gemäß dem geltenden Recht zulässig ist und angemessene Schutzmaßnahmen für die Rechte und Freiheiten der betroffenen Personen getroffen werden.

6. Verarbeitung sensibler personenbezogener Daten

6.1. Wenn das beteiligte Unternehmen sensible personenbezogene Daten für einen bestimmten und legitimen Zweck verarbeiten muss, wird das beteiligte Unternehmen diese Verarbeitung nur vornehmen, wenn:

6.1.1. Die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat, es sei denn, dass das Verbot nach Artikel 9(1) DSGVO nicht durch die Einwilligung der betroffenen Person aufgehoben werden kann.

6.1.2. Die Verarbeitung erforderlich ist, damit der Datenverantwortliche die ihm aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen diesbezüglichen Pflichten nachkommen kann, soweit dies laut geltendem Recht oder aufgrund eines Tarifvertrags gemäß dem geltenden Recht zulässig ist, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht.

6.1.3. Die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

6.1.4. Die Verarbeitung auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

6.1.5. Die Verarbeitung sich auf sensible personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich zugänglich gemacht hat.

6.1.6. Die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

6.1.7. Die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist und auf der Grundlage des geltenden Rechts erfolgt, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

6.1.8. Die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des geltenden Rechts oder aufgrund eines Vertrags mit einer medizinischen Fachperson erforderlich ist, und wenn die Verarbeitung der sensiblen personenbezogenen Daten von oder in der Verantwortung einer medizinische Fachperson erfolgt, muss diese Fachperson laut geltendem Recht oder den Regeln, die von zuständigen Stellen in einem EWR-Vertragsstaat erlassen werden, oder einer anderen Person, die laut geltendem Recht oder den Regeln, die von den zuständigen Stellen in einem EWR-Vertragsstaat erlassen werden, ebenfalls dem Berufsgeheimnis unterliegt, dem Berufsgeheimnis unterliegen.

6.1.9. Die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des geltenden Rechts erforderlich ist, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere in Form des Berufsgeheimnisses, vorsieht.

6.1.10. Die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89(1) DSGVO auf der Grundlage des geltenden Rechts erforderlich ist, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

7. Transparenz und Auskunftsrechte

7.1. Alle beteiligten Unternehmen verarbeiten die personenbezogenen Daten auf transparente Art und Weise. Amgen verpflichtet sich dazu, die EU BCRs, einschließlich der Kontaktdaten, jederzeit vorzuhalten, sie allen betroffenen Personen leicht zugänglich zu machen und die betroffenen Personen über die Übermittlung und Verarbeitung ihrer personenbezogenen Daten zu informieren. Diese EU BCRs stehen auf der Website von Amgen unter: www.amgen.com/bcr zur Verfügung. Alternativ wenden Sie sich bitte an privacy@amgen.com, um eine Kopie zu erhalten. Amgen setzt verschiedene Kommunikationskanäle, z. B. Websites des Konzerns, einschließlich interner Websites und Newsletter, Verträge und spezifische Datenschutzerklärungen ein, um diese Anforderung an die Zugänglichkeit zu erfüllen. Außerdem informiert Amgen die betroffenen Personen mithilfe dieser Kommunikationskanäle unverzüglich über Aktualisierungen und Änderungen an den EU BCRs oder an der Liste der beteiligten Unternehmen.

7.2. Betroffene Personen, deren personenbezogene Daten von einem beteiligten Unternehmen verarbeitet werden, erhalten die in Artikel 13 und 14 DSGVO dargelegten Informationen.

7.3. Wenn die personenbezogen Daten nicht von einer betroffenen Person bereitgestellt werden, erübrigt sich die Pflicht zur Information der betroffenen Person, wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist oder wenn die Aufzeichnung oder Offenlegung gesetzlich ausdrücklich festgelegt ist.

8. Rechte auf Zugriff, Berichtigung, Löschung und Einschränkung der Daten

8.1. Jede betroffene Person hat das Recht, von dem beteiligten Unternehmen eine Bestätigung zu erhalten, ob die sie betreffenden personenbezogenen Daten verarbeitet werden oder nicht, und wenn das der Fall ist, Zugriff auf die personenbezogenen Daten und die Informationen zu erhalten, die gemäß Artikel 15(1) DSGVO zur Verfügung gestellt werden müssen. Die Bearbeitung dieser Anfrage, einschließlich der Möglichkeit zur Erhebung einer Gebühr oder des Zeitrahmens zur Beantwortung einer solchen Anfrage, unterliegen dem geltenden Recht, und die betroffene Person wird bei Einreichung ihrer Anfrage angemessen darauf hingewiesen.

8.2. Jede betroffene Person hat das Recht, eine Berichtigung, Löschung oder Einschränkung von personenbezogenen Daten zu erwirken, insbesondere in Fällen, in denen die Daten unvollständig oder unrichtig sind.

8.3. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten einzulegen, die auf der Erfüllung einer Aufgabe im öffentlichen Interesse oder den berechtigten Interessen des beteiligten Unternehmens oder eines Dritten (einschließlich eines auf diesen Gründen gestützten Profilings) basiert. Das beteiligte Unternehmen verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, dass es zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

8.4. Jede betroffene Person hat das Recht, der Verarbeitung ihrer personenbezogenen Daten für die Zwecke der Direktwerbung (kostenlos) zu widersprechen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Wenn die betroffene Person ihr Recht ausübt, der Verarbeitung ihrer personenbezogenen Daten für die Zwecke der Direktwerbung zu widersprechen, muss das beteiligte Unternehmen die Verarbeitung der personenbezogenen Daten für diesen Zweck einstellen.

8.5. Jede betroffene Person hat das Recht, eine Benachrichtigung von Dritten über die Korrektur, Löschung oder Einschränkung gemäß Artikel 19 DSGVO zu erwirken, denen die personenbezogenen Daten offengelegt wurden.

8.6. Jede betroffene Person hat gemäß Artikel 13(2)(f) DSGVO das Recht, die bei der automatischen Verarbeitung von personenbezogenen Daten involvierte Logik zu kennen.

8.7. Wenn die Verarbeitung auf der Einwilligung beruht, hat jede betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung hat keinen Einfluss auf die Rechtmäßigkeit der Verarbeitung, die vor dem Widerruf auf Grundlage der Einwilligung erfolgt ist.

8.8. Jede betroffene Person hat das Recht, sich über den gemäß Artikel 17 eingeführten internen Beschwerdemechanismus bei dem beteiligten Unternehmen über die Verarbeitung von personenbezogenen Daten zu beschweren.

8.9. Alle Anfragen gemäß diesem Artikel 8 (oder Artikel 9 nachstehend) sollten dem beteiligten Unternehmen über die E-Mail-Adresse privacy@amgen.com zugeschickt werden. Auch wenn die Einreichung von Anfragen per E-Mail nachdrücklich empfohlen wird, hindert das eine betroffene Person nicht daran, ihre Anfrage mündlich vorzubringen. Das beteiligte Unternehmen informiert die betroffene Person unverzüglich und spätestens innerhalb von einem Monat nach dem Eingang über das Ergebnis ihrer Anfrage (gegebenenfalls einschließlich der Gründe, warum keine Maßnahmen eingeleitet wurden, und der Möglichkeit zur Einreichung einer Beschwerde bei der zuständigen Datenschutzbehörde und/oder zur Einlegung eines gerichtlichen Rechtsbehelfs). Der Zeitraum von einem Monat kann bei Bedarf und unter Berücksichtigung der Komplexität und der Anzahl der Anfragen um zwei weitere Monate verlängert werden. Das beteiligte Unternehmen informiert die betroffene Person über eine solche Verlängerung innerhalb von einem Monat nach Eingang der Anfrage und begründet die Verzögerung. Jede Kommunikation, Maßnahme und/oder Information, die im Zusammenhang mit einer Anfrage gemäß diesem Artikel 8 (oder Artikel 9 nachstehend) erfolgt, wird der betroffenen Person kostenlos zur Verfügung gestellt. Sind die Anfragen einer betroffenen Person offensichtlich unbegründet oder unverhältnismäßig, insbesondere aufgrund ihres wiederholten Charakters, so kann das beteiligte Unternehmen entweder: (a) eine angemessene Gebühr verlangen, die den Verwaltungskosten für die Bereitstellung der Informationen oder der Kommunikation oder die Einleitung der verlangten Maßnahmen Rechnung trägt, oder (b) die Bearbeitung der Anfrage ablehnen. Es ist Sache des beteiligten Unternehmens, den offensichtlich unbegründeten oder unverhältnismäßigen Charakter der Anfrage nachzuweisen.

9. Automatisierte Entscheidungen im Einzelfall

9.1. Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, außer wenn die Entscheidung:

9.1.1. für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem beteiligten Unternehmen erforderlich ist,

9.1.2. aufgrund des geltenden Rechts gefordert oder zulässig ist, das auch angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht (mindestens einschließlich des Rechts auf Erwirkung eines menschlichen Eingreifens auf Seiten des beteiligten Unternehmens, zur Darlegung ihrer Sichtweise und zur Anfechtung der Entscheidung), oder

9.1.3. mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

10. Sicherheit und Vertraulichkeit

10.1. Amgen setzt angemessene technische und organisatorische Schutzmaßnahmen gegen die Verletzung des Schutzes der personenbezogenen Daten ein. Internationale Rahmenwerke, wie die ISO/IEC 27002, werden von Amgen verwendet, um diese Schutzmaßnahmen festzulegen.

10.2. Amgen hat Prozesse eingeführt, die dafür sorgen, dass die Verletzung des Schutzes der personenbezogenen Daten in Berichten erfasst, nachverfolgt und bei Bedarf angemessene Korrekturmaßnahmen ergriffen werden. Jede Verletzung des Schutzes der personenbezogenen Daten wird (einschließlich der Fakten im Hinblick auf die Verletzung des Schutzes der personenbezogenen Daten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen) dokumentiert, und die Dokumentation wird der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung gestellt. Beteiligte Unternehmen melden jede Verletzung des Schutzes der personenbezogenen Daten unverzüglich an Amgen Frankreich, den Chief Privacy Officer und die anderen betroffenen Datenschutzbeauftragten/Stellen und (wenn das beteiligte Unternehmen, bei dem die Verletzung des Schutzes der personenbezogenen Daten aufgetreten ist, als Datenverarbeiter handelt) auch an das beteiligte Unternehmen, das als Datenverantwortlicher handelt. In Verbindung mit dem Chief Privacy Officer wird die Verletzung des Schutzes der personenbezogenen Daten unverzüglich der zuständigen Datenschutzbehörde angezeigt (und wenn möglich nicht später als 72 Stunden nach Bekanntwerden der Verletzung des Schutzes der personenbezogenen Daten), außer wenn es unwahrscheinlich ist, dass dadurch ein Risiko für die Rechte und Freiheiten der betroffenen Personen entsteht. Wenn die Verletzung des Schutzes der personenbezogenen Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt, werden die betroffenen Personen ebenfalls unverzüglich benachrichtigt.

10.3. Risikobeurteilungen zur Informationssicherheit werden verwendet, um mögliche Bedrohungen für sensible personenbezogene Daten und die Umsetzung gegebenenfalls zusätzlicher Sicherheitskontrollen zu identifizieren.

10.4. Gemäß Artikel 32 DSGVO wird der aktuelle Stand der Technik bei der Umsetzung der Maßnahmen berücksichtigt.

10.5. Der Chief Information Security Officer und der Chief Privacy Officer arbeiten gemeinsam daran, die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten.

10.6. Die technischen und organisatorischen Schutzmaßnahmen werden zur Umsetzung der Datenschutzprinzipien aus Artikel 5 DSGVO, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aus Artikel 25 DSGVO und zur Förderung der praktischen Einhaltung der Anforderungen aus diesen EU BCRs entwickelt.

11. Beziehungen zu Datenverarbeitern (Amgen-Datenimporteur oder Anbieter)

11.1. Das beteiligte Unternehmen (das als Datenverantwortlicher handelt) wählt sorgfältig einen Datenverarbeiter aus, der entweder ein anderes beteiligtes Unternehmen oder ein Anbieter sein kann. Der Datenverarbeiter muss ausreichende Garantien hinsichtlich der dortigen technischen und organisatorischen Schutzmaßnahmen für die durchzuführende Verarbeitung vorlegen und muss für die Einhaltung dieser Maßnahmen sorgen.

11.2. Wenn die Auslagerung als notwendig erachtet wird, nachdem eine Bewertung der wirtschaftlichen Bedürfnisse und Risiken dieser Auslagerung stattgefunden hat, gehört die Beurteilung der Risikofaktoren zum Datenschutz und die Abwägung der wirtschaftlichen Bedürfnisse gegen die möglichen Risiken zum Prozess für die Auswahl eines Datenverarbeiters.

11.3. Das beteiligte Unternehmen, das als Datenverantwortlicher handelt, setzt gemäß dem geltenden Recht (und insbesondere gemäß den Anforderungen aus Artikel 28(3) DSGVO) schriftliche vertragliche Maßnahmen ein und weist den Datenverarbeiter unter anderem dazu an, dass:

11.3.1. der Datenverarbeiter nur gemäß den Anweisungen des beteiligten Unternehmens handelt, das als Datenverantwortlicher auftritt, und dass die Verarbeitung der personenbezogenen Daten für die eigenen Zwecke des Datenverarbeiters oder für die Zwecke eines Dritten verboten ist;

11.3.2. bestimmte Regeln bezüglich Sicherheit und Vertraulichkeit für den Datenverarbeiter gelten und dass er angemessene technische und organisatorische Maßnahmen ergreifen muss, um für einen Schutz zu sorgen, der dem Risiko bei der Verarbeitung entspricht;

11.3.3. die Personen, die zur Verarbeitung der personenbezogenen Daten bevollmächtigt sind, sich zur Vertraulichkeit verpflichtet haben müssen oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen müssen;

11.3.4. der Datenverarbeiter ohne die vorherige, spezifische oder allgemeine schriftliche Zustimmung des beteiligten Unternehmens, das als Datenverantwortlicher handelt, keinen anderen Datenverarbeiter beauftragen darf, und dass für diesen beauftragten Datenverarbeiter, wenn eine solche Zustimmung erteilt wird, die gleichen Datenschutzverpflichtungen wie im Vertrag oder einem anderen Rechtsakt zwischen dem beteiligten Unternehmen, das als Datenverantwortlicher auftritt, und dem Datenverarbeiter gelten;

11.3.5. er das beteiligte Unternehmen, das als Datenverantwortlicher auftritt, unter Berücksichtigung der Art der Verarbeitung durch angemessene technische und organisatorische Maßnahmen soweit wie möglich bei der Erfüllung der Verpflichtung des beteiligten Unternehmens zur Beantwortung von Anfragen zur Ausübung der Rechte von betroffenen Personen unterstützen muss;

11.3.6. er das beteiligte Unternehmen, das als Datenverantwortlicher auftritt, bei der Einhaltung der Verpflichtungen hinsichtlich der Sicherheit der Verarbeitung, der Benachrichtigung der zuständigen Datenschutzbehörde und der betroffenen Person im Falle einer Verletzung des Schutzes der personenbezogenen Daten, bei der Beurteilung von Auswirkungen auf den Datenschutz und bei der vorherigen Anhörung der zuständigen Datenschutzbehörde unterstützen muss und dabei die Art der Verarbeitung und die dem Datenverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden müssen;

11.3.7. er nach Wahl des beteiligten Unternehmen, das als Datenverantwortlicher auftritt, alle personenbezogenen Daten löschen oder an das beteiligte Unternehmen, das als Datenverantwortlicher auftritt, nach dem Ende der Erbringung von Dienstleistungen hinsichtlich der Verarbeitung zurückgeben und bestehende Kopien löschen muss, es sei denn, dass die EU-Datenschutzgesetze eine Speicherung der personenbezogenen Daten vorsehen;

11.3.8. er dem beteiligten Unternehmen, das als Datenverantwortlicher auftritt, alle notwendigen Informationen übergeben muss, um die Einhaltung der Verpflichtungen aus diesem Artikel 11 nachzuweisen, und dass er Audits, einschließlich Inspektionen, die von dem beteiligten Unternehmen, das als Datenverantwortlicher auftritt, oder von einem anderen von ihm beauftragten Auditor durchgeführt werden, zulassen und sich daran beteiligen muss.

11.4. Das beteiligte Unternehmen, das als Datenverantwortlicher auftritt, sorgt dafür, dass der Datenverarbeiter die vereinbarten technischen und organisatorischen Schutzmaßnahmen jederzeit vollumfänglich einhält.

11.5. Das beteiligte Unternehmen, das als Datenverantwortlicher auftritt, bleibt für die Legitimität der Verarbeitung verantwortlich und haftet weiterhin für die Rechte der betroffenen Person. In dem Maße, wie der Datenverarbeiter den EU-Datenschutzgesetzen unterliegt, haftet er gemäß diesen Gesetzen ebenso für seine Verpflichtungen und Verantwortlichkeiten als Datenverarbeiter.

11.6. Um für die vertraglichen Verpflichtungen aus diesem Artikel seitens der Datenverarbeiter zu sorgen, ist hier eine Vertragsvorlage mit dem Titel Anhang Datenschutzvertrag zur Verwendung von den beteiligten Unternehmen enthalten, die als Datenverantwortlicher auftreten. In Abhängigkeit von den spezifischen Umständen jeder vertraglichen Vereinbarung kann das beteiligte Unternehmen, das als Datenverantwortlicher handelt, abweichende Bestimmungen als die im Anhang Datenschutzvertrag aufgenommenen Bestimmungen verhandeln, aber die vertraglichen Bestimmungen müssen trotzdem wenigstens die in diesem Artikel 11 genannten Pflichten enthalten.

11.7. Jedes beteiligte Unternehmen, das als Datenverarbeiter auftritt und das den EU-Datenschutzgesetzen unterliegt, muss eine Aufzeichnung zu sämtlichen Kategorien von Verarbeitungsaktivitäten pflegen, die im Auftrag eines beteiligten Unternehmens durchgeführt werden, das als Datenverantwortlicher auftritt. Diese Aufzeichnung sollte schriftlich, einschließlich in elektronischer Form, gepflegt werden, sie ist dem Chief Privacy Officer und der zuständigen Datenschutzbehörde auf Anfrage vorzulegen und muss folgende Informationen enthalten: (A) Name und Kontaktdaten des beteiligten Unternehmens, das als Datenverarbeiter auftritt, und aller beteiligten Unternehmen, die als Datenverantwortlicher auftreten und in deren Namen es handelt, sowie gegebenenfalls deren Vertreter und Datenschutzbeauftragten; (b) die Kategorien der Datenverarbeitung, die im Auftrag aller beteiligten Unternehmen, die als Datenverantwortlicher auftreten, durchgeführt wird und (c) sofern zutreffend, die Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Nennung dieses Drittlands oder der internationalen Organisation und für den Fall von Übermittlungen, die auf Ausnahmen aus Artikel 49 DSGVO beruhen, die Dokumentation zu geeigneten Schutzvorkehrungen; und (d) wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Schutzmaßnahmen.

12. Einschränkungen bei der Übermittlung und Weiterleitung

12.1. Bei allen Übermittlungen von personenbezogenen Daten gemäß diesen EU BCRs an Dritte mit Sitz außerhalb des EWR werden die EU-Datenschutzgesetze zu Übermittlungen und Weiterleitungen von personenbezogenen Daten entweder über die Anwendung von Standardvertragsklauseln, wie sie im Durchführungsbeschluss der Kommission (EU) vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß DSGVO genehmigt wurden, oder durch andere angemessene Maßnahmen gemäß Kapitel V der DSGVO (ausnahmsweise einschließlich wenn eine Ausnahme für eine bestimmte Situation gemäß Artikel 49 DSGVO gilt) eingehalten.

12.2. Bei allen Übermittlungen von personenbezogenen Daten gemäß diesen EU BCRs an Datenverarbeiter mit Sitz außerhalb des EWR werden die EU-Datenschutzgesetze bezüglich Datenverarbeitern (und die in Artikel 11 vorstehend dargelegten Anforderungen) zusätzlich zu den in diesem Artikel 12 genannten Regeln zu Übermittlungen und Weiterleitungen von personenbezogenen Daten und den EU-Datenschutzgesetzen eingehalten.

12.3. Vor der Übermittlung von personenbezogenen Daten an einen Datenimporteur oder (im Hinblick auf laufende Übermittlungen) vor dem Inkrafttreten von aktualisierten nationalen Gesetzen vor Ort beurteilt der Datenexporteur in Abstimmung mit dem Chief Privacy Officer und Amgen Frankreich sowie mit Unterstützung des Datenimporteurs und unter Berücksichtigung der Umstände der Übermittlung, ob die nationalen Gesetze vor Ort den Datenimporteur an der Erfüllung seiner Pflichten aus den EU BCRs hindern, und er legt fest, ob möglicherweise erforderliche, zusätzliche Maßnahmen umgesetzt werden sollen. Diese Beurteilung berücksichtigt:

12.3.1. die spezifischen Umstände der Übermittlung (einschließlich der Zwecke, für die die personenbezogenen Daten übermittelt und verarbeitet werden, der Arten von Instanzen, die an der Verarbeitung beteiligt sind, des Wirtschaftssektors, in dem die Übermittlung erfolgt, sowie der Kategorien und des Formats der übermittelten personenbezogenen Daten, des Standorts der Verarbeitung (einschließlich der Speicherung) und der bei der Übermittlung verwendeten Kanäle);

12.3.2. die im Hinblick auf die spezifischen Umstände der Übermittlung relevanten Gesetze und Praktiken des Dritt-Bestimmungslandes (einschließlich der Gesetze und Praktiken, die eine Offenlegung der Daten gegenüber staatlichen Behörden erfordern oder diesen Behörden Zugriff auf die Daten einräumen) sowie die entsprechenden Einschränkungen und Schutzvorkehrungen; und

12.3.3. alle relevanten vertraglichen, technischen oder organisatorischen Schutzvorkehrungen, die bezüglich der Übermittlung eingerichtet wurden, einschließlich der Maßnahmen, die während der Übermittlung und der Verarbeitung der personenbezogenen Daten im Bestimmungsland angewandt werden.

Des Weiteren basiert eine derartige Beurteilung auf dem Verständnis, dass die Gesetze und Praktiken des Dritt-Bestimmungslandes die Grundrechte und Freiheiten der betroffenen Personen respektieren und nicht über das hinausgehen, was in einer demokratischen Gesellschaft zum Schutz der folgenden Ziele erforderlich und verhältnismäßig ist: (a) die nationale Sicherheit, (b) die Landesverteidigung, (c) die öffentliche Sicherheit, (d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, (e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit, (f) den Schutz der Unabhängigkeit der Justiz und von Gerichtsverfahren, (g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe; (h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die mit der Ausübung öffentlicher Gewalt für die vorstehend genannten Zwecke verbunden sind, (i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen und/oder (j) die Durchsetzung zivilrechtlicher Ansprüche.

Der Chief Privacy Officer überprüft und genehmigt die dokumentierte Beurteilung sowie alle vorgeschlagenen zusätzlichen Maßnahmen. Wenn die Beurteilung zu dem Ergebnis kommt, dass die Einführung zusätzlicher Maßnahmen notwendig ist, wird der Datenexporteur diese Maßnahmen ergreifen. Wenn keine zusätzlichen Maßnahmen eingesetzt werden können (oder bei entsprechender Anweisung seitens des Chief Privacy Officers oder der zuständigen Datenschutzbehörde), stellt der Datenexporteur die Übermittlung ein. Das Ergebnis der Beurteilung und die vorgeschlagenen zusätzlichen Maßnahmen werden erfasst und, soweit erforderlich, der zuständigen Datenschutzbehörde vorgelegt.

Der Chief Privacy Officer und Amgen Frankreich informieren alle beteiligten Unternehmen über die durchgeführte Beurteilung und die dabei ermittelten Ergebnisse, damit die identifizierten zusätzlichen Maßnahmen angewandt werden können, wenn gleichwertige Übermittlungen von anderen beteiligten Unternehmen durchgeführt werden, oder damit derartige Übermittlungen unterbrochen oder beendet werden, wenn wirksame zusätzliche Maßnahmen nicht eingesetzt werden können.

12.4. Der Datenimporteur informiert den Datenexporteur, Amgen Frankreich und den Chief Privacy Officer unverzüglich darüber, wenn er Grund zu der Annahme hat, dass Gesetze oder Praktiken für ihn gültig sind oder geworden sind, die ihn an der Erfüllung seiner Pflichten aus diesen EU BCRs hindern, einschließlich infolge einer Änderung der nationalen Gesetzgebung vor Ort im Drittland, wie in Artikel 12.3 beschrieben, oder einer Maßnahme wie beispielsweise einer Aufforderung zur Offenlegung, wie in Artikel 16.3 beschrieben. Zusätzlich überwachen die Datenexporteure (in Zusammenarbeit mit dem Chief Privacy Officer) und sofern angemessen mit Unterstützung der Datenimporteure, die Entwicklungen im Drittland laufend, in das die personenbezogenen Daten von den Datenexporteuren übermittelt wurden, die sich nachteilig auf die anfängliche Beurteilung des Schutzniveaus der personenbezogenen Daten und die Entscheidungen auswirken können, die im Hinblick auf derartige Übermittlungen getroffen wurden.

12.5. Im Anschluss an die Unterbrechung einer Übermittlung muss der Datenexporteur die Übermittlung oder die Reihe von Übermittlungen beenden, wenn der Datenimporteur nicht in der Lage ist, die EU BCRs einzuhalten und/oder die Einhaltung nicht innerhalb von einem Monat nach der Unterbrechung wiederhergestellt ist. In einem solchen Fall muss der Datenimporteur nach Wahl des Datenexporteurs entweder alle personenbezogenen Daten und Kopien dieser Daten zurückgeben oder zerstören, die vor der Unterbrechung übermittelt wurden.

12.6. Alle Ströme personenbezogener Daten, die nicht diesen EU BCRs unterliegen und/oder nicht von einem beteiligten Unternehmen mit Sitz in einem EWR-Vertragsstaat stammen, gelten nicht als Übermittlung von personenbezogenen Daten im Sinne dieser EU BCRs und unterliegen demzufolge auch nicht den Bestimmungen dieser EU BCRs.

13. Schulungsprogramm

13.1. Wie in Anlage 2 beschrieben stellt Amgen allen Angestellten angemessene und aktuelle Schulungen zu den Datenschutzgrundsätzen und speziell zu den EU BCRs zur Verfügung. Diese Schulung umfasst auch Informationen über die straf- und arbeitsrechtlichen Konsequenzen und/oder im Hinblick auf den Dienstvertrag von Angestellten, die gegen die EU BCRs verstoßen.

13.2. Diese Schulung ist vorgeschrieben und wird jährlich wiederholt. Die erfolgreiche Teilnahme an der Schulung wird dokumentiert.

13.3. Je nach Situation erhalten ausgewählte Angestellte, die ständig oder regelmäßig Zugriff auf personenbezogene Daten haben oder die an der Erhebung von personenbezogenen Daten oder der Entwicklung von Tools zur Verarbeitung personenbezogener Daten beteiligt sind, spezifische Schulungen.

13.4. Außerdem stellt das Global Privacy Compliance Team von Amgen angemessene Informationen und Ressourcen über den Datenschutz zur Verfügung, unter anderem auf dem Intranet-Portal von Amgen.

14. Audit- und Monitoring-Programm

14.1. Der Chief Privacy Officer sorgt dafür, dass alle beteiligten Unternehmen (und deren Einhaltung dieser EU BCRs) aus der Perspektive des Schutzes der Privatsphäre und des Datenschutzes in das Audit- und Monitoring-Programm aufgenommen werden. Umfassende Audits werden vom Team Interne Audits oder von unabhängigen, extern zertifizierten Auditoren regelmäßig durchgeführt, nicht seltener als alle 2 bis 3 Jahre (für beteiligte Unternehmen mit einem mittleren bis hohen Risikoprofil auf Grundlage der Methode zur Risikobeurteilung der Audit-Abteilung) und alle 4 bis 5 Jahre (für beteiligte Unternehmen mit einem geringen Risikoprofil auf Grundlage der Methode zur Risikobeurteilung der Audit-Abteilung). Der Geltungsbereich von umfassenden Audits beinhaltet die Angelegenheiten in Sachen des Datenschutzes und des Schutzes der Privatsphäre (einschließlich der Einhaltung dieser EU BCRs, sofern sie für ein beteiligtes Unternehmen anwendbar sind und von ihm genutzt werden). Zusätzlich zu den umfassenden Audits und unbeschadet der vorstehend genannten Zeiträume werden Audits mit anderen Geltungsbereichen einschließlich funktionsübergreifender und anlassbezogener Audits (z. B. zur Einhaltung der EU BCRs), beschränkte Audits zu einem oder mehreren Systemen zur Verarbeitung von personenbezogenen Daten und/oder beschränkte Audits von einer oder mehreren funktionalen Abteilungen (z. B. dem Team Global Privacy Compliance) durchgeführt. Das Audit-Programm wird in Abstimmung mit dem Chief Audit Executive und dem Chief Compliance Officer, der ein Senior Vice-President ist, entwickelt und verabschiedet. Der Chief Privacy Officer, der Chief Compliance Officer und der Chief Information Officer können jederzeit Ad hoc-Audits bezüglich der EU BCRs veranlassen. Zum Beispiel als Reaktion auf ein identifiziertes Compliance-Problem oder die Meldung einer maßgeblichen Nichteinhaltung, eine Verletzung des Schutzes der personenbezogenen Daten und/oder eine substanzielle Änderung an den EU-Datenschutzgesetzen. Das Audit-Programm umfasst alle Aspekte der EU BCRs, einschließlich der Methoden zur Gewährleistung, dass Korrekturmaßnahmen erfolgen.

14.2. Alle Audit-Berichte zu den EU BCRs werden dem Chief Compliance Officer und dem Chief Privacy Officer zeitnah kommuniziert. Außerdem werden die Audit-Zusammenfassungen und Befunde zu den EU BCRs sowie alle anderen relevanten Informationen über geeignete Ausschüsse (z. B. den Ausschuss Konzernverantwortung und Compliance und/oder den Prüfungsausschuss des Vorstands) regelmäßig an den Vorstand der Amgen Inc., den Vorstand von Amgen Frankreich und (beispielsweise und sofern zutreffend im Hinblick auf einen Befund, der behoben werden muss) an das jeweils beteiligte Unternehmen gemeldet. Der Ausschuss Konzernverantwortung und Compliance des Vorstands der Amgen Inc. tritt fünfmal pro Jahr zusammen. Das Thema Datenschutz & Schutz der Privatsphäre wird jährlich behandelt, üblicherweise im Rahmen der Oktober-Sitzung.

14.3. Die zuständige Datenschutzbehörde kann auf Anfrage eine Kopie der Audit-Berichte zu den EU BCRs erhalten.

14.4. Jedes beteiligte Unternehmen arbeitet bei Audits mit der zuständigen Datenschutzbehörde zusammen und akzeptiert das Audit seitens der zuständigen Datenschutzbehörde ohne Vorbehalte. Jede auditierte Gesellschaft muss den Chief Privacy Officer unverzüglich darüber in Kenntnis setzen, wenn sie eine Mitteilung über ein solches Audit erhält oder wenn ein solches Audit stattfindet.

15. Compliance und Überwachung der Compliance

15.1. Amgen ernennt geeignete Angestellte, gegebenenfalls einschließlich eines Netzwerks von Datenschutzbeauftragten, mit Unterstützung der obersten Geschäftsführung, um die Einhaltung der Datenschutzregeln zu überwachen und zu gewährleisten. Der Chief Privacy Officer ist für das Team Global Privacy Compliance zuständig, das die Amgen-Gesellschaften auf der ganzen Welt (einschließlich der beteiligten Unternehmen) als weltweites Sachverständigen-Team unterstützt.

15.2. Bei Amgen umfassen die Aufgaben des Chief Privacy Officers unter anderem:

15.2.1. die Beratung des Vorstands;

15.2.2. die Gewährleistung der weltweiten Datenschutz-Compliance (einschließlich der Gesamtverantwortung für die EU BCRs);

15.2.3. die regelmäßige Berichterstattung zur Datenschutz-Compliance (einschließlich an den Chief Compliance Officer); und

15.2.4. die Unterstützung der Ermittlungen von zuständigen Datenschutzbehörden.

15.3. Das Team Global Privacy Compliance besteht aus dem Chief Privacy Officer (der zusätzlich zu den vorstehenden Aufgaben mit der Beaufsichtigung des weltweiten Netzwerks der Datenschutzbeauftragten betraut ist), dem europäischen Datenschutzbeauftragten und sonstigen Datenschutzbeauftragten vor Ort. Das Team Global Privacy Compliance ist bei Amgen insgesamt für die weltweite Compliance in Sachen Datenschutz und Schutz der Privatsphäre zuständig.

15.4. Der europäische Datenschutzbeauftragte wurde von Amgen als Datenschutzbeauftragter für den EWR, Großbritannien und die Schweiz ernannt. Der europäische Datenschutzbeauftragte nimmt die Aufgaben wahr, die in Artikel 39 DSGVO aufgenommen sind. Amgen sorgt dafür, dass die Aufgaben und Pflichten des europäischen Datenschutzbeauftragten nicht zu einem Interessenkonflikt mit diesen Aufgaben führen. Der europäische Datenschutzbeauftragte berichtet direkt an den Chief Privacy Officer (der Teil der obersten Geschäftsführung von Amgen ist) und wird vom örtlichen Compliance Lead in Frankreich unterstützt. Der europäische Datenschutzbeauftragte kann den Chief Privacy Officer kontaktieren, wenn Fragen oder Probleme bei der Erfüllung seiner Pflichten auftreten. Der europäische Datenschutzbeauftragte ist erreichbar unter: privacy@amgen.com.

15.5. Auf lokaler Ebene sind die Datenschutzbeauftragten für die Bearbeitung lokaler Anfragen zum Datenschutz von betroffenen Personen, für die Gewährleistung der Compliance auf lokaler Ebene mit Unterstützung vom Team Global Privacy Compliance und für die Berichterstattung bei maßgeblichen Vorfällen im Bereich Datenschutz an den Chief Privacy Officer zuständig. Amgen pflegt ein Netzwerk aus Datenschutzbeauftragten und sorgt dafür, dass ein Datenschutzbeauftragter für jedes Land ernannt oder beauftragt wird, in dem Amgen mit einer Konzerngesellschaft (das beteiligte Unternehmen) vertreten ist und die Rechtsordnung des beteiligten Unternehmens eine solche Ernennung vorschreibt.

15.6. In der Regel sind die Datenschutzbeauftragten entweder die Compliance Leads vor Ort, die an die Abteilung Worldwide Compliance and Business Ethics berichten, oder sie werden von ihnen unterstützt. Das Team Global Privacy Compliance ist Teil der Abteilung Worldwide Compliance and Business Ethics und berichtet an diese Abteilung, die der Leitung des Chief Compliance Officer untersteht. Der Chief Compliance Officer trägt die Gesamtverantwortung für die rechtliche und behördliche Compliance des Amgen-Konzerns weltweit. In seltenen Fällen und aufgrund von spezifischen Umständen eines beteiligten Unternehmens oder sonstigen speziellen Umständen kann der Datenschutzbeauftragte aus einer anderen Funktion stammen, zum Beispiel aus dem Bereich Regulatory. In jedem Fall sorgt das Team Global Privacy Compliance dafür, dass die Datenschutzbeauftragten und die Compliance Leads angemessen geschult werden und über ein ausreichendes Maß an Managementfähigkeiten und Kompetenzen verfügen, um ihre Aufgaben zu erfüllen. Außerdem berichten die Datenschutzbeauftragten direkt an den Chief Privacy Officer und werden von den Angestellten im Team Global Privacy Compliance unterstützt, wenn sie zusätzliche Hilfestellungen benötigen.

15.7. Jedes beteiligte Unternehmen, das als Datenverantwortlicher auftritt, ist für die Einhaltung der EU BCRs verantwortlich und in der Lage, ihre Einhaltung nachzuweisen. Im Rahmen dieser Erfordernis müssen alle beteiligten Unternehmen:

15.7.1. eine Aufzeichnung aller Kategorien von Verarbeitungsaktivitäten pflegen, die gemäß den Anforderungen aus Artikel 30(1) DSGVO durchgeführt werden. Diese Aufzeichnung sollte schriftlich, einschließlich in elektronischer Form, gepflegt werden, sie ist dem Chief Privacy Officer und der zuständigen Datenschutzbehörde auf Anfrage vorzulegen und muss folgende Informationen enthalten: (a) Name und Kontaktdaten des beteiligten Unternehmens, das als Datenverantwortlicher auftritt, sowie seines Vertreters und Datenschutzbeauftragten; (b) die Zwecke der Verarbeitung; (c) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der personenbezogenen Daten; (d) die Kategorien von Empfängern, denen personenbezogene Daten offengelegt wurden oder werden, einschließlich der Empfänger in Drittländern oder internationalen Organisationen; (e) gegebenenfalls die Übertragungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des Drittlands oder der internationalen Organisation, und im Falle von Übermittlungen aufgrund von Ausnahmen eine Dokumentation der angemessenen Schutzvorkehrungen; (f) wenn möglich die geplanten Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten und (g) wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Schutzmaßnahmen.

15.7.2. Beurteilungen von Datenschutzauswirkungen bei Verarbeitungsaktivitäten durchführen, die gemäß Artikel 35 DSGVO wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten von natürlichen Personen führen. Wenn eine Beurteilung von Datenschutzauswirkungen aus Artikel 35 zeigt, dass die Verarbeitung ohne die von einem beteiligten Unternehmen zur Minimierung der Risiken ergriffenen Maßnahmen zu einem hohen Risiko führt, muss der Chief Privacy Officer vor der Verarbeitung angehört werden, der sich dann gemäß Artikel 36 DSGVO mit der zuständigen Datenschutzbehörde abstimmt.

16. Maßnahmen, wenn die nationale Gesetzgebung die Einhaltung der EU BCRs verhindert

16.1. Wenn ein beteiligtes Unternehmen Grund zu der Annahme hat, dass die für dieses Unternehmen anwendbaren Gesetze das beteiligte Unternehmen daran hindern, seinen Pflichten aus den EU BCRs nachzukommen, oder zu maßgeblichen Auswirkungen auf die Garantien führen, die von den Regeln aufgestellt werden, wird dieses Unternehmen den Chief Privacy Officer und Amgen Frankreich unverzüglich darüber informieren (es sei denn, dass diese Information von einer Strafverfolgungsbehörde verboten wurde, z. B. als strafrechtliches Verbot für die Wahrung der Vertraulichkeit einer strafrechtlichen Ermittlung).

16.2. Wenn ein Konflikt zwischen den nationalen Gesetzen vor Ort und den Verpflichtungen in den EU BCRs besteht, legt der Chief Privacy Officer in Abstimmung mit dem Justitiar und dem Datenschutzbeauftragten am Standort fest, welche rechtlich angemessenen Schritte erforderlich sind. Wenn nötig, stimmt sich der Chief Privacy Officer auch mit der zuständigen Datenschutzbehörde ab.

16.3. Wenn es wahrscheinlich ist, dass irgendeine gesetzliche Bestimmung, der ein beteiligtes Unternehmen in einem Drittland unterliegt, wesentliche, nachteilige Auswirkungen auf die in den EU BCRs enthaltenen Garantien hat, müssen der Chief Privacy Officer, Amgen Frankreich und der Datenexporteur vom Datenimporteur unverzüglich informiert werden, und der Chief Privacy Officer informiert die zuständige Datenschutzbehörde und (wenn möglich) die betroffenen Personen. Dazu gehören (a) jede rechtlich verbindliche Aufforderung zur Offenlegung von personenbezogenen Daten seitens einer Strafverfolgungsbehörde oder einer staatlichen Sicherheitsinstanz, und in einem solchen Fall sollte die zuständige Datenschutzbehörde unter Angabe der verlangten Daten, der beantragenden Stelle, der rechtlichen Grundlage und der gegebenen Antwort ganz eindeutig über die Aufforderung informiert werden (es sei denn, dass diese Information anderweitig verboten ist, beispielsweise im Rahmen eines strafrechtlichen Verbots zur Wahrung der Vertraulichkeit einer strafrechtlichen Ermittlung) und (b) jeder gemäß den Gesetzen des Bestimmungslandes erfolgende direkte Zugriff von staatlichen Behörden auf die personenbezogenen Daten, die gemäß diesen EU BCRs übermittelt werden, und in einem solchen Fall umfasst die Mitteilung alle Informationen, die einem beteiligten Unternehmen zur Verfügung stehen (es sei denn, dass diese Information anderweitig verboten ist, beispielsweise im Rahmen eines strafrechtlichen Verbots zur Wahrung der Vertraulichkeit einer strafrechtlichen Ermittlung).

16.4. Wenn die Unterbrechung und/oder Benachrichtigung in bestimmten Fällen verboten sind, setzt sich das beteiligte Unternehmen, das die Aufforderung erhält, nach Kräften für den Erhalt eines Verzichts auf dieses Verbot ein, um so viele Informationen wie ihm möglich und sobald wie möglich kommunizieren und (auf Anfrage des Datenexporteurs) nachweisen zu können, dass es dies getan hat.

16.5. Der Datenimporteur stellt dem Datenexporteur in regelmäßigen Abständen so viele relevante Informationen wie möglich zu den erhaltenen Aufforderungen zur Verfügung (insbesondere zur Anzahl der Aufforderungen, zur Art der verlangten personenbezogenen Daten, zur Identität der auffordernden Behörden, ob Aufforderungen angefochten wurden und was das Ergebnis derartiger Anfechtungen war). Der Datenimporteur bewahrt derartige Informationen so lange auf, wie die personenbezogenen Daten den Schutzmaßnahmen aus den EU BCRs unterliegen, und er stellt sie der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung. Wenn es dem Datenimporteur ganz oder teilweise verboten wird, dem Datenexporteur die vorstehenden Informationen zur Verfügung zu stellen, wird der Datenimporteur den Datenexporteur darüber unverzüglich in Kenntnis setzen.

16.6. In Zusammenarbeit mit dem Chief Privacy Officer überprüft der Datenimporteur die Rechtmäßigkeit einer Aufforderung zur Offenlegung seitens einer staatlichen Behörde, um festzulegen, ob sie in den Zuständigkeitsbereich der staatlichen Behörde fällt, von der die Aufforderung ausgeht. Der Datenimporteur ficht die Aufforderung an, wenn sich nach einer derartigen Beurteilung (in Zusammenarbeit mit dem Chief Privacy Officer) herausstellt, dass es berechtigte Gründe für die Annahme gibt, dass die Aufforderung gemäß den Rechten des Bestimmungslandes, einschlägigen Verpflichtungen im internationalen Recht und/oder Grundsätzen der internationalen Verständigung unrechtmäßig ist. Wenn der Datenimporteur glaubt, dass es berechtigte Gründe für die Annahme gibt, dass die Aufforderung unrechtmäßig ist, wird er Möglichkeiten zur

Berufung nutzen. Wenn eine Aufforderung angefochten wird, setzt der Datenimporteur einstweilige Verfügungen ein, um die Auswirkungen der Aufforderung auszusetzen, bis die zuständige gerichtliche Behörde eine Entscheidung in der Sache gefällt hat. Der Datenimporteur wird die verlangten personenbezogenen Daten nicht offenlegen, bis er gemäß dem geltenden Recht und der Verfahrensordnung des Bestimmungslandes dazu verpflichtet ist. Der Datenimporteur dokumentiert seine juristische Beurteilung und jede Anfechtung der Aufforderung zur Offenlegung, und er stellt diese Dokumentation dem Datenexporteur sowie auf Anfrage der zuständigen Datenschutzbehörde zur Verfügung, insoweit dies nach den Gesetzen des Bestimmungslandes zulässig ist.

16.7. Auf der Grundlage einer angemessenen Auslegung der Aufforderung stellt der Datenimporteur die zulässige Mindestmenge an Informationen zur Verfügung, wenn er auf eine Aufforderung zur Offenlegung reagiert.

16.8. In jedem Fall erfolgen Übermittlungen von personenbezogenen Daten durch ein beteiligtes Unternehmen an eine staatliche Behörde nicht umfassend, unverhältnismäßig und wahllos in einer Art und Weise, die über das hinausgeht, was in einer demokratischen Gesellschaft erforderlich ist.

16.9. Unbeschadet anderer Gründe für die Übermittlung gemäß Kapitel V DSGVO dürfen Urteile eines Gerichts oder Gerichtshofs oder Entscheidungen einer Verwaltungsbehörde in einem Drittland zur Verpflichtung eines Datenverantwortlichen oder Datenverarbeiters zur Übermittlung oder Offenlegung von personenbezogenen Daten von den beteiligten Unternehmen mit Sitz im EWR nur anerkannt oder in irgendeiner Weise umgesetzt werden, wenn sie auf einem internationalen Übereinkommen beruhen, beispielsweise Verträgen zur gegenseitigen Rechtshilfe, die zwischen dem ersuchenden Drittland und der EU oder einem EWR-Vertragsstaat gültig sind.

17. Interne Beschwerdemechanismen

17.1. Amgen nutzt seinen bestehenden Prozess zum Umgang mit Beschwerden auch für die Bearbeitung von Beschwerden oder Bedenken hinsichtlich der EU BCRs.

17.2. Jede betroffene Person kann sich jederzeit darüber beschweren, dass die EU BCRs von einem beteiligten Unternehmen nicht eingehalten werden. Derartige Beschwerden werden vom Team Global Privacy Compliance unter der Leitung des Chief Privacy Officers und in Zusammenarbeit mit den jeweiligen Datenschutzbeauftragten vor Ort bearbeitet.

17.3. Amgen empfiehlt, dass derartige Beschwerden schriftlich entweder per Post oder per E-Mail direkt an das Team Global Privacy Compliance oder an das beteiligte Unternehmen gerichtet werden. Das Team Global Privacy Compliance ist wie folgt erreichbar:

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

E-Mail: privacy@amgen.com

17.4. Sofern gemäß den für das beteiligte Unternehmen geltenden Gesetzen zulässig, können Angestellte von Amgen die Business Conduct Hotline nutzen, um eine Beschwerde bezüglich der EU BCRs zu melden.

17.5. Wenn die Beschwerde bei dem beteiligten Unternehmen vor Ort eingeht, wird sie bei Bedarf vom Datenschutzbeauftragten übersetzt und unverzüglich an das Team Global Privacy Compliance weitergeleitet.

17.6. Innerhalb von zehn (10) Werktagen erhält die betroffene Person eine erste Reaktion, mit der ihr mitgeteilt wird, dass ihre Beschwerde bearbeitet wird und dass sie unverzüglich und in jedem Fall innerhalb von einem Monat nach dem Eingang der Anfrage eine substanzielle Antwort erhält. Unter Berücksichtigung der Komplexität und der Anzahl der Anfragen kann diese Frist von einem Monat um maximal zwei weitere Monate verlängert werden, wobei die betroffene Person in diesem Fall entsprechend darüber informiert wird. Die substanzielle Antwort enthält Details zu unseren Befunden und zu den Maßnahmen, die Amgen umgesetzt hat oder vorschlägt. Wenn Amgen zu dem Schluss kommt, dass keine Maßnahmen ergriffen werden sollten, wird dies der betroffenen Person unter Angabe der Gründe für diese Schlussfolgerung erläutert.

17.7. Wenn die Beschwerde von Amgen anerkannt wird, setzt Amgen angemessene Abhilfemaßnahmen ein. Diese Maßnahmen werden fallweise vom Chief Privacy Officer und dem Team Global Privacy Compliance, dem Datenschutzbeauftragten vor Ort und gegebenenfalls von jeder anderen betroffenen Abteilung entschieden. Außerdem werden angemessene Disziplinarmaßnahmen ergriffen, die im zulässigen Ausmaß des geltenden Rechts bis zur Kündigung des Beschäftigungsverhältnisses oder der Beauftragung reichen können, wenn das Team Global Privacy Compliance ein Fehlverhalten von Einzelpersonen feststellt.

17.8. Die betroffene Person wird in einem Antwortschreiben über das Ergebnis ihrer Beschwerde informiert. Dieses Antwortschreiben erfolgt unverzüglich und in jedem Fall innerhalb von einem Monat nach dem Eingang der Beschwerde (mit ausreichend detaillierten Angaben, damit Amgen die Art der Beschwerde identifizieren kann und nur wenn angemessen notwendig, mit allen erbetenen Informationen, um die Identität des Beschwerdeführers zu bestätigen). Unter Berücksichtigung der Komplexität und der Anzahl der Anfragen kann diese Frist von einem Monat um maximal zwei weitere Monate verlängert werden, wobei die betroffene Person in diesem Fall entsprechend darüber informiert wird.

17.9. Die betroffene Person wird darüber informiert, dass sie eine Beschwerde bei den Gerichten eines EWR-Vertragsstaats oder bei der zuständigen Datenschutzbehörde einreichen kann, wenn sie mit der Antwort von Amgen nicht zufrieden ist. Allerdings ist es keine Voraussetzung, dass die betroffene Person zunächst das interne Beschwerdeverfahren von Amgen bemüht, bevor sie sich bei der zuständigen Datenschutzbehörde beschweren oder Klage vor den Gerichten eines EWR-Vertragsstaats einreichen kann.

17.10. Dieses Beschwerdeverfahren wird durch Veröffentlichung der EU BCRs bekanntgegeben, wie in Artikel 7 vorstehend erwähnt.

18. Drittbegünstigte und Haftung

18.1. Eine betroffene Person, deren personenbezogene Daten aus dem EWR stammen oder von den EU-Datenschutzgesetzen geschützt sind und die an ein beteiligtes Unternehmen außerhalb des EWR übermittelt werden, hat als Drittbegünstigte das Recht zur Durchsetzung der EU BCRs und das Recht auf gerichtlichen Rechtsschutz, auf die Erwirkung von Abhilfemaßnahmen und gegebenenfalls auf Ersatz der tatsächlich infolge eines Verstoßes gegen diese EU BCRs entstandenen Schäden. Jede derartige Beschwerde kann von der betroffenen Person an eine zuständige Datenschutzbehörde gerichtet werden (das kann die Datenschutzbehörde in dem EWR-Vertragsstaat sein, in dem sich die betroffene Person gewöhnlich aufhält, oder die Datenschutzbehörde an ihrem Arbeitsort oder die Datenschutzbehörde am Ort des behaupteten Verstoßes). Betroffene Personen können außerdem Klage bei einem zuständigen Gericht in einem EWR-Vertragsstaat einreichen (das können die Gerichte in dem EWR-Vertragsstaat sein, in dem das jeweils beteiligte Unternehmen ansässig ist, oder die Gerichte in dem EWR-Vertragsstaat, in dem sich die betroffene Person gewöhnlich aufhält). Eine betroffene Person kann bei der Ausübung ihres Rechts auf wirksame Rechtsmittel gegen ein beteiligtes Unternehmen von einer gemeinnützigen Instanz, Organisation oder Vereinigung vertreten werden, vorausgesetzt, dass eine solche Instanz, Organisation oder Vereinigung gemäß dem geltenden Recht ordnungsgemäß gegründet wurde, über satzungsgemäße Ziele verfügt, die mit dem öffentlichen Interesse vereinbar sind, und im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen im Hinblick auf den Schutz ihrer personenbezogenen Daten tätig ist. Die betroffene Person ist in der Lage, die folgenden Artikel als Drittbegünstigte durchzusetzen:

18.1.1. Artikel 1 (Anwendungsbereich), 2 (Definitionen), 3 (Zweckbindung), 4 (Datenqualität und Proportionalität), 5 (Gesetzliche Grundlage für die Datenverarbeitung) und 6 (Verarbeitung sensibler personenbezogener Daten);

18.1.2. Artikel 7 (Transparenz und Auskunftsrechte);

18.1.3. Artikel 8 (Rechte auf Zugriff, Berichtigung, Löschung und Einschränkung der Daten) und 9 (Automatisierte Entscheidungen im Einzelfall);

18.1.4. Artikel 10 (Sicherheit und Vertraulichkeit), 11 (Beziehungen zu Datenverarbeitern (Amgen-Datenimporteur oder Anbieter) und 12 (Einschränkungen bei der Übermittlung und Weiterleitung);

18.1.5. Artikel 16 (Maßnahmen, wenn die nationale Gesetzgebung die Einhaltung der EU BCRs verhindert) und 21 (Verhältnis zwischen der nationalen Gesetzgebung und den EU BCRs);

18.1.6. Artikel 18 (Drittbegünstigte und Haftung); und

18.1.7. Artikel 19 (Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden).

18.2. Zur Klarstellung: Die Rechte als Drittbegünstigte erstrecken sich nicht auf die Artikel und Elemente dieser EU BCRs, die sich auf die internen Mechanismen beziehen, die in den beteiligten Unternehmen oder im Amgen-Konzern eingeführt wurden, beispielsweise die Angaben zur Schulung (einschließlich Anlage 2), zu Audit-Programmen, zu den internen Compliance-Netzwerken und - Struktur und zum Mechanismus für die Aktualisierung der EU BCRs.

18.3. Amgen Frankreich übernimmt die Verantwortung für Maßnahmen, die zur Abhilfe von Handlungen der beteiligten Unternehmen mit Sitz außerhalb des EWR angemessen erforderlich sind, und stimmt zu, diese Maßnahmen zu ergreifen. Amgen Frankreich zahlt eine Entschädigung für alle wesentlichen oder nicht wesentlichen Schäden, die sich aus dem Verstoß gegen diese EU BCRs ergeben, es sei denn, dass es nachweisen kann, dass das beteiligte Unternehmen mit Sitz außerhalb des EWR nicht für das Ereignis verantwortlich ist, das Ursache für den Schaden war. Amgen Frankreich verfügt über ausreichende finanzielle Mittel und eine Versicherungsdeckung, um die Schäden aus den EU BCRs zu decken.

18.4. Jede betroffene Person, der infolge eines Verstoßes gegen diese EU BCRs von einem beteiligten Unternehmen ohne Sitz im EWR ein Schaden entstanden ist, hat das Recht, von Amgen Frankreich gegebenenfalls eine Entschädigung für den erlittenen Schaden zu erhalten, und die Gerichte oder andere zuständige Behörden im EWR sind entsprechend zuständig. Die betroffene Person besitzt die Rechte und Rechtsmittel gegen Amgen Frankreich, als hätte Amgen Frankreich anstelle des beteiligten Unternehmens ohne Sitz im EWR den Verstoß in der EU verursacht. Wenn das beteiligte Unternehmen ohne Sitz im EWR für einen solchen Verstoß verantwortlich ist oder dafür haftbar gemacht wird, entschädigt es Amgen Frankreich in dem Ausmaß, in dem es verantwortlich ist oder haftbar gemacht wird, für alle Kosten, Gebühren, Schäden, Auslagen oder Verluste, die Amgen Frankreich im Zusammenhang mit einem solchen Verstoß entstehen.

18.5. Im Falle einer Behauptung einer betroffenen Person, dass ihr ein Schaden entstanden ist, und sie gezeigt hat, dass dieser Schaden wahrscheinlich aufgrund eines Verstoßes gegen die EU BCRs verursacht wurde, liegt die Beweislast dafür, dass die Schäden, die der betroffenen Person durch einen Verstoß gegen die EU BCRs entstanden sind, nicht durch das jeweils beteiligte Unternehmen verursacht wurden, bei Amgen Frankreich. Wenn Amgen Frankreich zeigen kann, dass das beteiligte Unternehmen mit Sitz außerhalb des EWR nicht für das Ereignis verantwortlich ist, das den Schaden verursacht hat, ist es nicht für den Schaden haftbar oder verantwortlich.

19. Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden

19.1. Die beteiligten Unternehmen arbeiten zusammen und unterstützen einander bei der Bearbeitung von Anfragen oder Beschwerden einer betroffenen Person oder bei der Ermittlung oder einem Ersuchen seitens der zuständigen Datenschutzbehörde.

19.2. In Zusammenarbeit mit dem Chief Privacy Officer beantworten die beteiligten Unternehmen die Anfragen der zuständigen Datenschutzbehörde hinsichtlich der EU BCRs in einem Zeitrahmen, der angesichts der Umstände der Anfrage angemessen ist (und keinesfalls nach Ablauf der Frist, die von der zuständigen Datenschutzbehörde festgelegt wurde) und angemessen detailliert auf Grundlage der Informationen, die dem beteiligten Unternehmen angemessen zur Verfügung stehen. Im Hinblick auf die Umsetzung und die laufende Anwendung der EU BCRs müssen die beteiligten Unternehmen die Mitteilungen und Empfehlungen der zuständigen Datenschutzbehörde ausreichend berücksichtigen, und sie müssen alle formellen Entscheidungen und Bekanntmachungen einhalten, die von der zuständigen Datenschutzbehörde erlassen werden.

19.3. Jeder Streitfall hinsichtlich der ausgeübten Überwachung einer zuständigen Datenschutzbehörde zur Einhaltung dieser EU BCRs wird von den Gerichten des Mitgliedsstaats dieser Datenschutzbehörde gemäß dem geltenden Recht dieses Mitgliedsstaats entschieden.

20. Aktualisierungen und Änderungen der EU BCRs

20.1. Amgen behält sich das Recht vor, diese EU BCRs jederzeit zu ändern und/oder zu aktualisieren. Derartige Aktualisierungen der EU BCRs können spezifisch infolge neuer gesetzlicher Vorschriften, signifikanter Änderungen an der Struktur des Amgen-Konzerns oder offizieller Vorgaben erforderlich sein, die von der zuständigen Datenschutzbehörde gemacht werden.

20.2. Amgen informiert alle beteiligten Unternehmen und die zuständige Datenschutzbehörde unverzüglich über alle signifikanten Änderungen an den EU BCRs oder an der Liste der beteiligten Unternehmen, mit denen Änderungen am geltenden Recht, am regulatorischen Umfeld und/oder an der Konzernstruktur von Amgen berücksichtigt werden. Insbesondere wenn sich eine Änderung auf das von den EU BCRs gebotene Schutzniveau auswirkt, wird die zuständige Datenschutzbehörde vom Chief Privacy Officer unverzüglich und vorab mit einer knappen Erläuterung der Gründe für die Änderung informiert. Für einige Änderungen könnte eine erneute Zustimmung seitens der zuständigen Datenschutzbehörde erforderlich sein.

20.3. Der Chief Privacy Officer pflegt eine vollständig aktualisierte Liste der an den EU BCRs beteiligten Unternehmen, erfasst alle Aktualisierungen an den Regeln und stellt den betroffenen Personen oder den zuständigen Datenschutzbehörden auf Anfrage die nötigen Informationen zur Verfügung. Alle administrativen Änderungen an den EU BCRs werden den beteiligten Unternehmen regelmäßig mitgeteilt.

20.4. Unter den Garantien der EU BCRs finden Übermittlungen von personenbezogenen Daten an neue, beteiligte Unternehmen erst statt, nachdem die neuen, beteiligten Unternehmen wirksam an die EU BCRs gebunden sind und die EU BCRs von ihnen eingehalten werden.

20.5. Alle administrativen Änderungen an den EU BCRs oder an der Liste der beteiligten Unternehmen werden den beteiligten Unternehmen regelmäßig und der zuständigen Datenschutzbehörde mindestens einmal pro Jahr mit einer knappen Erläuterung der Gründe für die Aktualisierung mitgeteilt.

20.6. Substanzielle Änderungen an den EU BCRs werden den betroffenen Personen außerdem über die in Artikel 7 der EU BCRs genannten Wege mitgeteilt.

21. Verhältnis zwischen der nationalen Gesetzgebung und den EU BCRs

21.1. Wenn die vor Ort für ein beteiligtes Unternehmen geltenden nationalen Gesetze einen höheren Schutz für personenbezogene Daten vorsehen, gelten sie vorrangig vor den EU BCRs. Wenn die vor Ort für ein beteiligtes Unternehmen geltenden nationalen Gesetze einen geringeren Schutz für personenbezogene Daten als die EU BCRs vorsehen, werden die EU BCRs eingehalten.

21.2. Für den Fall, dass Pflichten gemäß den vor Ort für ein beteiligtes Unternehmen geltenden nationalen Gesetzen im Widerspruch zu den EU BCRs stehen, informiert das beteiligte Unternehmen den Chief Privacy Officer unverzüglich darüber und hält die zusätzlichen Vorschriften aus Artikel 16 vorstehend ein.

21.3. In jedem Fall werden die personenbezogenen Daten gemäß Artikel 5 DSGVO und allen lokal einschlägigen Gesetzen verarbeitet.

22. Schlussbestimmungen

22.1. Die EU BCRs treten mit der Zustimmung seitens der zuständigen Datenschutzbehörde in Kraft, und sie sind für die beteiligten Unternehmen nach Unterzeichnung des Dokuments zur Annahme der EU BCRs wirksam.

22.2. Übermittlungen an beteiligte Unternehmen erfolgen nur, wenn sie an diese EU BCRs gebunden sind. Wenn ein Datenimporteur nicht länger an die EU BCRs gebunden ist, muss er unverzüglich alle personenbezogenen Daten (einschließlich aller Kopien davon) zurückgeben oder löschen, die im Rahmen dieser EU BCRs übermittelt wurden, es sei denn, der Datenimporteur verpflichtet sich gesetzlich verbindlich zur Wahrung des Schutzes der personenbezogenen Daten gemäß Kapitel V DSGVO, dann darf er die personenbezogenen Daten weiter aufbewahren, die im Rahmen dieser EU BCRs übermittelt wurden.

22.3. Der Datenimporteur muss den Datenexporteur, Amgen Frankreich und den Chief Privacy Officer unverzüglich darüber informieren, wenn er aus irgendeinem Grund nicht in der Lage ist, diese EU BCRs einzuhalten (einschließlich der Situationen, die in Artikel 12.3 vorstehend beschrieben sind). Wenn der Datenimporteur gegen diese EU BCRs verstößt oder nicht in der Lage ist, sie einzuhalten, muss der Datenexporteur den Chief Privacy Officer darüber informieren und die Übermittlung personenbezogener Daten unterbrechen.

22.4. Nach Wahl des Datenexporteurs muss der Datenimporteur unverzüglich alle personenbezogenen Daten (einschließlich Kopien davon) zurückgeben oder löschen, die gemäß diesen EU BCRs übermittelt wurden, und dies dem Datenexporteur bescheinigen, wenn:

22.4.1. der Datenexporteur die Übermittlung der personenbezogenen Daten unterbrochen hat und die Einhaltung dieser EU BCRs nicht innerhalb eines angemessenen Zeitraums und in jedem Fall innerhalb von einem Monat nach der Unterbrechung wiederhergestellt werden kann; oder

22.4.2. der Datenimporteur maßgeblich gegen diese EU BCRs verstoßen hat; oder

22.4.3. der Datenimporteur es unterlässt, eine verbindliche Entscheidung eines zuständigen Gerichts oder einer zuständigen Datenschutzbehörde bezüglich seiner Verpflichtungen aus diesen EU BCRs einzuhalten.

Bis die personenbezogenen Daten gelöscht oder zurückgegeben wurden, muss der Datenimporteur die Einhaltung dieser EU BCRs weiterhin gewährleisten. Wenn die vor Ort für den Datenimporteur geltenden nationalen Gesetze eine Rückgabe oder Löschung der personenbezogenen Daten verbieten, die gemäß diesen EU BCRs übermittelt werden, muss der Datenimporteur die Einhaltung dieser EU BCRs weiterhin gewährleisten und darf die personenbezogenen Daten nur in dem Ausmaß und so lang verarbeiten, wie dies gemäß diesen vor Ort geltenden nationalen Gesetzen vorgeschrieben ist.

23. Anlagen

Die angehängten Anlagen sind integraler Bestandteil der EU BCRs.

Anlage 1: Übersicht der Datenströme bei Amgen

Anlage 2: Übersicht zum Schulungsprogramm bei Amgen

Anlage 1: Übersicht der Datenströme bei Amgen

Betroffene Personen	Datenkategorien	Zwecke	Übermittlung
Angestellte	Identifikationsdaten wie Name, Anschrift, Geburtsdatum und -ort, Einstellungsdatum, Sozialversicherungsnummern, Kreditkartennummern, Bankkonto- und Finanzdaten sowie Führerschein- und Ausweisnummern Urlaubsansprüche und Leistungen, Beschwerden, Bonus, Beförderungen, Überprüfungen und Beurteilungen, Arbeitsunterlagen, Informationen bezüglich der Kranken- und Sozialversicherung, Pensionspläne und Details zu Aktienoptionen Persönliche Steuer- und Finanzinformationen Sensible Daten wie die nationale Herkunft, sofern nach dem lokalen Recht zulässig	Personalmanagement, IT-Support und Verwaltungszwecke im Zusammenhang mit dem Beschäftigungsverhältnis und Leistungen oder die Verwaltung von Leistungen im Anschluss an die Beschäftigung sowie zur Einhaltung der rechtlichen, administrativen und unternehmerischen Pflichten von Amgen	Die weltweiten Datenzentren von Amgen befinden sich in den USA, wo auch der Hauptsitz der Amgen Inc. ansässig ist. Die Daten fließen von Amgen Frankreich (oder dem jeweiligen Datenexporteur) an Amgen Inc in den Vereinigten Staaten oder an beteiligte Unternehmen in der Schweiz. Dort dürfen die Daten: − einfach gespeichert und aufbewahrt werden − für die Bereitstellung weltweiter Statistiken und Berichte analysiert werden − innerhalb des Amgen-Konzerns an andere beteiligte Unternehmen weitergeleitet werden, wenn der Zugriff darauf für bestimmte Angestellte oder geschäftliche Funktionen bei diesen beteiligten Unternehmen erforderlich ist (z. B.: ein Angestellter, der sich auf eine Stelle außerhalb seines Landes bewirbt oder der an einen Manager außerhalb seines Landes berichten muss). In den meisten Fällen handeln derart beteiligte Unternehmen als
Medizinische Fachpersonen	Name, geschäftliche Kontaktdaten einschließlich Telefonnummer und E-Mail-Adresse, Fachgebiet Beruflicher Hintergrund (Lebenslauf) Teilnahme an sonstiger Forschung Finanzdaten (Abrechnungs- und Zahlungsdaten)	Verwaltung und Management der professionellen und wissenschaftlichen Aktivitäten von Amgen - Forschung & Entwicklung (beispielsweise Beteiligung an medizinischer Forschung, klinischen Studien, professionellen Meetings oder Kongressen) Werbung für die Produkte und Dienstleistungen von Amgen Offenlegung von Finanzinformationen, wenn dies laut geltendem Recht oder der Einhaltung des Branchenkodex vorgeschrieben ist Regulatorische Compliance, beispielsweise Sicherheits-Monitoring und Meldung unerwünschter Ereignisse	

Anbieter / Lieferanten	Name der Person, Name der Organisation, geschäftliche Kontaktdaten Abrechnungs- und Zahlungsdaten	Verarbeitung der Zahlungen an Anbieter und Lieferanten Regulatorische Compliance zum Beispiel zur Steuergesetzgebung	Datenverantwortliche, abhängig von den geschäftlichen Bedürfnissen können die beteiligten Unternehmen aber auch als Datenverarbeiter handeln (z. B. bei der Erbringung von Supportleistungen des IT Help Desks oder bei der Unterstützung des HR Connect Service Centres).
Teilnehmer an klinischen Prüfungen (möglicherweise einschließlich Kindern unter 18 Jahren, wenn ein pädiatrischer Patient an einer von Amgen gesponserten klinischen Studie teilnimmt).	Kodierte Daten - Patientenname und Kontaktdaten werden durch eine intern generierte Identifikationsnummer ersetzt. Nur das Prüfzentrum (Krankenhaus/Forschungsstandort) bewahrt die Liste zur Verknüpfung der Identifikationsnummer mit dem Patientennamen auf. Indirekte Identifikatoren wie das Geburtsjahr oder -datum (das vollständige Geburtsdatum wird nur bei pädiatrischen Studien erhoben), Geschlecht, Größe, Gewicht. Notwendige Gesundheitsdaten, wie im Protokoll zur Forschungsstudie dargelegt. Sonstige Daten, die im Hinblick auf den Patienten für die Durchführung der Forschung erforderlich sind, einschließlich ethnischer Zugehörigkeit, familiärer Situation (z. B. Anzahl Kinder), Drogen- und Alkoholkonsum, Medikamente, allgemeine Angewohnheiten oder Verhaltensweisen, berufliche Situation wie Arbeitsplatz, Arbeitslosigkeit, Teilnahme an anderen Studien.	Verwaltung und Management der biomedizinischen Forschung (klinische Prüfungen, Beobachtungsstudien)	
Patienten (einschließlich Kindern unter 18 Jahren, wenn ein unerwünschtes Ereignis bei der Anwendung eines Amgen-Produkts im Falle von pädiatrischen Indikationen vorliegt).	Indirekte Identifikatoren des Patienten wie Alter, Geburtsjahr oder -datum, Patienteninitialen (sofern gemäß den lokalen Gesetzen zulässig), Geschlecht, Gewicht / Größe oder Patientenidentifikationsnummer (mit Ausnahme der Identifikatoren im nationalen Gesundheitssystem).	Regulatorische Compliance und Pharmakovigilanz, beispielsweise Sicherheits-Monitoring und Meldung unerwünschter Ereignisse (sofern gemäß den lokalen Gesetzen zulässig)	

	Daten bezüglich der Identifikation des Amgen-Produkts, z. B. das verwendete Arzneimittel oder Medizinprodukt, die Seriennummern von Medizinprodukten, Verabreichungsmethode oder Dosierungen des Produkts, Los-/Chargennummern des Produkts. Gesundheitsdaten einschließlich der verabreichten Behandlungen, der Ergebnisse von Untersuchungen, der Art des/der unerwünschten Ereignisse(s), persönliche oder familiäre medizinische Anamnese, zugehörige Erkrankungen oder Ereignisse, Risikofaktoren, Informationen zu Verschreibungen, zur Verwendung von Medikamenten und zum therapeutischen Vorgehen von medizinischen Fachpersonen, die an der Behandlung der Erkrankung des Patienten beteiligt sind. Sonstige Daten, die sich auf den Patienten beziehen und die für die Beurteilung von unerwünschten gesundheitlichen Ereignissen gemäß den Verpflichtungen zur regulatorischen Compliance erforderlich sind, beispielsweise ethnische Zugehörigkeit, Berufsleben, Drogen- und Alkoholkonsum, Medikamente und/oder allgemeine Angewohnheiten oder Verhaltensweisen.		

Anlage 2: Übersicht zum Schulungsprogramm bei Amgen

Schulungsprogramm zum Datenschutz und zum Schutz der Privatsphäre / zur Bewusstseinsbildung

Das Schulungsprogramm zum Datenschutz und zum Schutz der Privatsphäre soll dafür sorgen, dass alle Angestellten von Amgen hinsichtlich der EU BCRs von Amgen sowie der gesetzlichen Pflichten mit Auswirkung auf die Verarbeitung von personenbezogenen Daten angemessen geschult sind. Dieses Programm umfasst verschiedene Elemente.

Allgemeine Schulung für alle Angestellten von Amgen

Alle Angestellten von Amgen müssen im Rahmen der Schulung zum Verhaltenskodex jährlich an einer Online-Schulung zum Datenschutz teilnehmen. Diese Schulung ist vorgeschrieben, sie wird überwacht und dauert üblicherweise 75 Minuten. Diese Schulung umfasst die EU BCRs und Informationen über die straf- und arbeitsrechtlichen Konsequenzen und/oder im Hinblick auf den Dienstvertrag von Angestellten, die gegen die EU BCRs verstoßen.

Spezifische Schulung für Datenschutzbeauftragte

Alle Datenschutzbeauftragten von Amgen werden regelmäßig und auf einer Need-to-know-Basis im Rahmen von Telefonkonferenzen der Datenschutzbeauftragten, die vom Team Global Privacy Compliance durchgeführt werden, und Datenschutz-Workshops am Standort und/oder online zu neuen Prozessen geschult. Alle Datenschutzbeauftragten haben Zugang zu einer Wiki-Seite, auf der häufig gestellte Fragen beantwortet werden und die zudem Leitlinien und Links zu externen Ressourcen enthält.

Spezifische Schulungen für Angestellte

Auf einer Need-to-know-Basis können spezifische Schulungen entweder online oder am Standort oder über die Veröffentlichung von Informationen im Intranet von Amgen stattfinden. Diese Schulungen können sich an spezifische Gruppen richten, von denen personenbezogene Daten entweder täglich bearbeitet werden oder die andere Gruppen unterstützen, die personenbezogene Daten verarbeiten. Beispielsweise werden die Audit-Gruppe, die F&E-Funktionen und die Rechtsabteilung regelmäßig geschult. Dazu gehören Informationen zu den Verfahren für den Umgang mit Aufforderungen zum Zugriff auf personenbezogene Daten seitens staatlicher Behörden, sofern sie für spezifische Angestellte relevant sind. Diese Schulung kann entweder auf regionaler oder nationaler Ebene durchgeführt werden. Auf einer Need-to-know-Basis können weitere, spezifische Schulungen zu den EU BCRs entwickelt werden.

Bewusstsein

Das Intranet von Amgen umfasst eine eigene Seite zum Schutz der Privatsphäre und zum Datenschutz, die Links zu anderen internen oder externen Ressourcen enthält.

Beim Sentinel-Programm, einem weltweiten Programm für mehr Bewusstsein der Angestellten von Amgen für das Thema Informationssicherheit, arbeitet das Team Global Privacy Compliance von Amgen mit der Abteilung Informationssicherheit zusammen.

Schulungs-Support

Alle Schulungen zum Schutz der Privatsphäre werden vom Team Global Privacy Compliance entwickelt und vom Chief Privacy Officer freigegeben. Die Schulungen können entweder direkt von einem Mitglied des Teams Global Privacy Compliance oder von einem Datenschutzbeauftragten vor Ort im Rahmen eines „train-the-trainer“-Modells gehalten werden.