Die verbindlichen Unternehmensregeln von Amgen (BCR - Binding Corporate Rules) – Öffentliches Dokument

Deutsche Übersetzung der Verbindlichen Unternehmensrichtlinie

Einführung:

Amgen ist führend in der Biotechnologie und hat sich dem Dienst an Patienten mit schweren Krankheiten verschrieben.

Die verbindlichen Unternehmensregeln von Amgen (BCR - Binding Corporate Rules) spiegeln die Verpflichtung von Amgen zur Wahrung der Privatsphäre und zum Datenschutz wider, indem sie für Übermittlung und Verarbeitung von personenbezogenen Daten bei/zwischen den Unternehmen von Amgen einen angemessenen Schutz festlegen.

Alle Gesellschaften innerhalb des Amgen-Konzerns und alle Mitarbeiter sind verpflichtet, sich an die BCR zu halten. Die Nichteinhaltung dieser Regeln kann zu disziplinarischen Maßnahmen in dem nach den örtlichen Gesetzen zulässigen Umfang führen.

Der für Compliance zuständige Chief Compliance Officer ist in Zusammenarbeit mit dem für Datenschutz zuständigen Chief Privacy Officer dafür verantwortlich, die Durchsetzung dieser Regeln sicherzustellen.

Die BCR wurden aufgrund der derzeitigen EU-Regeln zum Datenschutz beschlossen, der EU-Richtlinien 95/46/EG und 2002/58/EG.

1 – Geltungsbereich

Die BCR von Amgen gelten für jede Übermittlung und Verarbeitung, ob automatisiert oder manuell, aller personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten, Aktionären und Patienten sowie allen anderen betroffenen Personen, die von einem beteiligten Unternehmen von Amgen in einem der folgenden Fälle als Datenverantwortlichem vorgenommen werden:

a) das beteiligte Unternehmen von Amgen, das die personenbezogenen Daten verarbeitet, hat seinen Sitz in einem regulierten Land oder

b) das beteiligte Unternehmen von Amgen, das die personenbezogenen Daten verarbeitet, hat seinen Sitz nicht in einem regulierten Land („Datenimporteur“) und hat die

personenbezogenen Daten von einem beteiligten Unternehmen von Amgen erhalten, das seinen Sitz in einem regulierten Land wie in § 2 definiert hat (dem „Datenexporteur“).

Diese BCR gelten darüber hinaus auch für die Übermittlung personenbezogener Daten zwischen zwei Datenimporteuren.

2 – Definitionen

Begriffe	Definitionen
Personenbezogene Daten	Daten, die sich auf eine Person beziehen, deren Identität offensichtlich ist oder aus den Informationen direkt oder indirekt abgeleitet werden kann. Alternativ können personenbezogene Daten auch als Informationen definiert werden, die entweder allein oder in Kombination mit anderen Informationen eine bestimmte Person identifizieren oder genutzt werden können, um diese zu kontaktieren oder aufzufinden. Beispiele von personenbezogenen Daten können, je nach örtlichen Datenschutzgesetzen, unter anderem die folgenden Daten umfassen: • Name, Anschrift, Sozialversicherungsnummer, Führerscheinnummer, Kontoangaben, familiäre Informationen oder medizinische Daten einer Person, • Name, berufliche Ausbildung und Verschreibungspraktiken eines Arztes, • E-Mail-Adresse und andere identifizierende Informationen, die von einem Besucher einer Internetseite von Amgen bereitgestellt werden. Die obige Liste ist lediglich beispielhaft und nicht erschöpfend.
Sensible personenbezogene Daten	Folgende Informationen über eine betroffene Person: • Informationen über den medizinischen oder Gesundheitszustand (bezogen auf physische oder geistige Gesundheit) • Finanzielle Informationen • Informationen über rassische oder ethnische Herkunft • Informationen über politische Meinungen • Informationen über religiöse oder philosophische Überzeugungen • Informationen über die Mitgliedschaft in Gewerkschaften • Informationen über das Sexualleben • Informationen über Vorstrafen oder vorausgegangene Verhaftungen Amgen betrachtet auch Informationen als sensible Informationen, die genutzt werden könnten, um Identitätsdiebstahl zu begehen, also etwa Sozialversicherungsnummer, Führerscheinnummer, Kreditkarten- oder andere Bankdaten.
betroffene Person	Die Person, auf die sich die personenbezogenen Daten beziehen. Eine betroffene Person kann unter anderem sein: • Ein Patient/Verbraucher/Teilnehmer an einer klinischen Studie

	• Eine medizinische Fachkraft (z. B. Arzt oder Krankenschwester) • Ein Mitarbeiter (derzeitig, ehemals oder im Ruhestand) • Ein Auftragnehmer/Einzelunternehmer/Anbieter/Berater
Verantwortlicher (Datenverantwortlicher)	Jede juristische Person, die Entscheidungen in Bezug auf die Erfassung und Verarbeitung von personenbezogenen Daten trifft, einschließlich der Entscheidungen darüber, für welche Zwecke und auf welche Weise die personenbezogenen Daten verarbeitet werden.
Auftragsverarbeiter	Eine natürliche oder juristische Person, die im Namen/Auftrag des Datenverantwortlichen personenbezogene Daten verarbeitet.
(Daten-)Verarbeitung	Jeder Arbeitsablauf und jede Zusammenstellung verschiedener Arbeitsabläufe, die an den personenbezogenen Daten vorgenommen werden, ob automatisiert oder nicht. Darunter fallen beispielsweise Erfassung, Betrachtung, Zugriff, Speicherung, Aufzeichnung, Organisation, Übernahme oder Änderung, Abfrage, Bezugnahme, Nutzung, Weitergabe durch Übermittlung, Veröffentlichung oder Verfügbarmachung auf andere Weise, Abgleich oder Kombination, Sperrung, Löschung oder Vernichtung.
Dritter	Eine natürliche oder juristische Person, eine öffentliche Behörde oder eine andere Körperschaft mit Ausnahme der betroffenen Person, des Datenverantwortlichen und der Personen, die zur Datenverarbeitung autorisiert sind und unter der direkten Befehlsgewalt des Datenverantwortlichen stehen. Bei Amgen wird auch ein Anbieter als Dritter betrachtet.
Anbieter	Jede Person, jedes Unternehmen oder jede Organisation, die Waren und/oder Dienstleistungen für Amgen bereitstellen oder in einer vertraglichen Beziehung zu Amgen stehen und/oder von Amgen personenbezogene Daten empfangen, die Voraussetzung für die Bereitstellung der Waren und/oder Dienstleistungen sind.
Datenschutzbehörden (DPA - Data Protection Agencies)	Eine oder mehrere öffentliche Behörden, die innerhalb ihres Zuständigkeitsbereichs verantwortlich für die Überwachung der Bestimmungen sind, die von den Mitgliedstaaten aufgrund der EU-Richtlinie 95/46 verabschiedet wurden. Diese Behörden handeln bei der Ausübung der ihnen übertragenen Aufgaben vollständig unabhängig.
Reguliertes Land	Ein Land innerhalb des Europäischen Wirtschaftsraums (EWR) oder ein Land mit einem angemessenen Niveau des Datenschutzes, anerkannt durch eine Entscheidung der EU-Kommission, oder sämtliche anderen Länder, die BCR als legitimes Verfahren für die Übermittlung von personenbezogenen Daten außerhalb ihres Zuständigkeitsbereichs anerkennen, dies sind: Andorra, Argentien, Faröer Inseln, Guernsey, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay .

Datenexporteur	Ein Unternehmen von Amgen, mit Sitz in einem regulierten Land, das als Datenverantwortlicher agiert und personenbezogene Daten an ein anderes Unternehmen von Amgen übermittelt, das seinen Sitz nicht in einem regulierten Land hat (Datenimporteur).
Datenimporteur	Ein Unternehmen von Amgen, das seinen Sitz nicht in einem regulierten Land hat und von einem Datenexporteur personenbezogene Daten erhält.
Technische und organisatorische Sicherheitsmaßnahmen	Auf den Schutz der personenbezogenen Daten abzielende Maßnahmen, die insbesondere Folgendes verhindern sollen: Unbeabsichtigte oder ungesetzliche Vernichtung oder unbeabsichtigte Verluste und Änderungen, unbefugte Weitergabe oder unbefugte Zugriffe in Bezug auf personenbezogene Daten, insbesondere, wenn die Verarbeitung eine Übermittlung über ein Netzwerk erfordert, sowie alle anderen Formen ungesetzlicher Verarbeitung.
Beteiligtes Unternehmen	Eine juristische Person des Amgen-Konzerns, die durch die BCR rechtlich gebunden ist.
Einwilligung	Die freiwillig und informiert erfolgende Anzeige der Wünsche einer betroffenen Person, durch die die betroffenen Person seine Einwilligung zur Erfassung und Verarbeitung seiner personenbezogenen Daten erteilt.
Datenschutzbeauftragter (Data Protection Officer)	Ein Mitarbeiter eines Unternehmens, der vom Management dieses Unternehmens oder dieser Geschäftseinheit als derjenige benannt wurde, der für die Überwachung der Einhaltung des Datenschutzes auf lokaler Ebene ebenso verantwortlich ist wie für die Umsetzung angemessener und erforderlicher Kontrollen.

Im Rahmen der BCR legt Amgen diesen Begriff in Einklang mit den EU-Richtlinien 95/46/EG und 2002/58/EG aus. Diese Richtlinien werden nachfolgend als EU-Richtlinie bezeichnet.

3 – Einschränkung des Zwecks

Personenbezogene Daten werden für die ausdrücklichen, speziellen und legitimen Zwecke nach Artikel 6.1 (b) der EU-Richtlinie 95/46 verarbeitet.

Personenbezogene Daten werden nicht auf eine Weise verarbeitet, die mit den legitimen Zwecken unvereinbar ist, für die die personenbezogenen Daten erfasst wurden. Datenimporteure sind verpflichtet, sich bei der Speicherung und/oder Weiterverarbeitung oder Nutzung der von einem anderen beteiligten Unternehmen an sie übermittelten Daten an die ursprünglichen Zwecke zu halten. Der Zweck der Datenverarbeitung kann lediglich mit Einwilligung der betroffenen Person oder in dem nach den lokalen Gesetzen zulässigen Umfang verändert werden, denen der die Daten übermittelnde Datenexporteur unterliegt.

Bei sensiblen Daten werden zusätzliche Sicherheitsvorkehrungen getroffen, so wie die EU-Direktive 95/46/EG dies vorsieht.

4 – Qualität und Verhältnismäßigkeit der Daten

Personenbezogene Daten müssen den Tatsachen entsprechen und falls erforderlich regelmäßig aktualisiert werden. Es sind geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass unzutreffende oder unvollständige Daten korrigiert oder gelöscht werden.

Personenbezogene Daten müssen angemessen und relevant im Sinn von Artikel 6.1 (c) der EU-Direktive 95/46 sein.

Die Datenverarbeitung orientiert sich am Zweck der Beschränkung der Erfassung, Verarbeitung und/oder Nutzung der personenbezogenen Daten auf das notwendige Maß. Mit anderen Worten: Es sind so wenige personenbezogene Daten wie möglich zu erfassen, zu bearbeiten und/oder zu nutzen. Es muss die Möglichkeit anonymer oder mit einem Pseudonym versehener Daten genutzt werden, solange der dafür erforderliche Aufwand an Kosten und Zeit in Anbetracht des gewünschten Zwecks angemessen ist.

Personenbezogene Daten, die für den geschäftlichen Zweck, für den sie ursprünglich erfasst und gespeichert worden sind, nicht mehr benötigt werden, sind entsprechend der Richtlinie von Amgen zur Aufbewahrung von Aufzeichnungen zu löschen. Wenn gesetzliche Aufbewahrungs- oder Sperrfristen Anwendung finden, sind die Daten nicht zu löschen, sondern zu sperren. Sie werden dann nach Ablauf der Aufbewahrungs- oder Sperrfrist gelöscht.

5 – Rechtliche Grundlage für die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn zumindest eine der nachfolgend genannten Voraussetzungen gegeben ist:

- Die betroffenen Person hat freiwillig und unmissverständlich ihre/seine informierte Einwilligung zur Verabreitung erteilt.
- Die Verarbeitung ist für die Erfüllung eines Vertrags oder einer ähnlichen Vertrauensbeziehung erforderlich, dessen/deren Partei die betroffenen Person ist, oder sie ist vor Vertragsschluss erforderlich, um auf Anforderung der betroffenen Person gewisse Maßnahmen zu ergreifen.
- Die Verarbeitung ist für die Einhaltung gesetzlicher Verpflichtungen erforderlich, denen der Datenverantwortliche unterliegt, oder sie ist nach den geltenden Gesetzen oder Verordnungen vorgeschrieben oder erlaubt.
- Die Verarbeitung ist zum Schutz wesentlicher Interessen der betroffenen Person erforderlich. Darunter fallen Leben, Gesundheit oder Sicherheit.
- Die Verarbeitung ist für die Durchführung einer Aufgabe erforderlich, die im öffentlichen Interesse vorgenommen wird oder im Rahmen der Ausübung einer öffentlichen Befugnis, die dem Datenverantwortlichen oder eines Dritten erteilte wurde, dem/der gegenüber die Datenweitergabe erfolgt.
- Die Verarbeitung ist für die Zwecke legitimer Interessen erforderlich, die vom Datenverantwortlichen oder eines Dritten verfolgt werden, denen gegenüber die Weitergabe der Daten erfolgt. Eine Ausnahme gilt hier dann, wenn die legitimen Interessen der betroffenen Person in Bezug auf seine Grundrechte und seine Freiheiten diese Interessen überwiegen.

6 – Verarbeitung sensibler Daten

Wenn Amgen sensible personenbezogene Daten für einen bestimmten und legitimen Zweck verarbeiten muss, wird Amgen dies nur dann tun, wenn:

- Die betroffenen Person ihre/seine ausdrückliche Einwilligung zur Verarbeitung dieser sensiblen Daten erteilt hat und auch dann nur, wenn die geltenden Gesetze diese Verarbeitung (trotz Einwilligung) nicht verbieten
- die Verarbeitung für die Zwecke der Erfüllung der Verpflichtungen und die Ausübung der speziellen Rechte des Datenverantwortlichen im Bereich des Arbeitsrechts erforderlich ist, soweit das nationale Recht dies unter Einhaltung angemessener Sicherheitsvorkehrungen zulässt
- die Verarbeitung zum Schutz wesentlicher Interessen der betroffenen Person oder in dem Fall, dass die betroffenen Person physisch oder rechtlich zur Erteilung der Einwilligung außerstande ist, einer anderen Person erforderlich ist
- die Verarbeitung im Rahmen legitimer Aktivitäten unter angemessenen Garantien durch eine Stiftung, einen Verband oder eine andere nicht auf Gewinn ausgerichtete Körperschaft mit politischen, philosophischen, religiösen oder gewerkschaftlichen Zielen erfolgt. Dabei ist jedoch Bedingung, dass die Verarbeitung sich ausschließlich auf die Mitglieder dieser Körperschaft oder auf Personen bezieht, die in Zusammenhang mit deren Zwecken regelmäßig mit der Körperschaft in Kontakt stehen und dass die Daten ohne Einwilligung der betroffenen Person nicht an Dritte weitergegeben werden
- die Verarbeitung sich auf sensible Daten bezieht, die von der betroffenen Person selbst offenkundig öffentlich gemacht wurden oder werden
- die Verarbeitung der sensiblen Daten für die Begründung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist
- die Verarbeitung der sensiblen Daten für den Zweck der Präventivmedizin, der medizinischen Diagnose, der Bereitstellung von Betreuung oder Behandlung oder das Management von Gesundheitsdiensten erforderlich ist. Voraussetzung ist dabei jeweils, dass diese sensiblen Daten durch eine medizinische Fachkraft aus dem Bereich des Gesundheitswesens verarbeitet werden, die nach nationalem Recht oder nach von einer nationalen zuständigen Körperschaft erlassenen Regeln der Schweigepflicht unterliegt oder aber durch eine andere Person, die ebenfalls einer gleichwertigen Schweigepflicht unterliegt.

7 – Transparenz und Informationsrecht

Alle beteiligten Unternehmen haben die personenbezogenen Daten auf eine transparente Weise zu verarbeiten.
Amgen verpflichtet sich, die BCR einschließlich der entsprechenden Kontaktdaten jeder betroffenen Person leicht zugänglich zu machen und die betroffenen Person über die Übermittlung und Verarbeitung ihrer personenbezogenen Daten zu informieren.

Um dies erreichen zu können, wird Amgen verschiedene Kommunikationsmethoden einsetzen wie die Internetseite des Unternehmens, einschließlich interner Seiten und Newsletter, Verträge und spezielle Datenschutzhinweise, die geeigneten anderen Kommunikationen hinzugefügt werden.

Den betroffenen Personen, deren personenbezogene Daten von einem beteiligten Unternehmen verarbeitet werden, sind die folgenden Informationen zur Verfügung zu stellen:

- die Identität des/der Datenverantwortlichen und ggf. dessen Vertreter;
- der Verarbeitungszweck, für den die Daten bestimmt sind;
- der Ursprung der Daten (außer wenn die personenbezogenen Daten direkt von der betroffenen Personerfasst werden);

- sämtliche weiteren Informationen wie:
  i) die Empfänger oder Kategorien von Empfängern der Daten,
  ii) das Bestehen des Rechts zum Zugriff auf die Daten und zur Korrektur der auf die betroffenen Person bezogenen Daten, sofern diese weiteren Informationen unter Berücksichtigung der speziellen Umstände der Datenerfassung erforderlich sind, um in Bezug auf die betroffenen Person eine angemessene Verarbeitung sicherzustellen.

Wenn die Daten nicht direkt von der betroffenen Personselbst stammen, gilt die Pflicht zur Information der betroffenen Person dann nicht, wenn die Bereitstellung solcher Informationen unmöglich ist oder einen unverhältnismäßig hohen Aufwand erfordern würde oder wenn die Aufzeichnung und Weitergabe ausdrücklich gesetzlich erlaubt ist.

8 – Die Rechte auf Zugriff, Korrektur, Löschung und Sperrung in Bezug auf die Daten

Jede betroffene Person hat das Recht, sich ohne sonstige Beschränkungen in angemessenen Zeitabständen Informationen in verständlicher Form darüber zu verschaffen, welche Daten verarbeitet werden. Dieses Recht umfasst auch die Angabe verfügbarer Informationen zur Datenquelle. Die Erfüllung einer entsprechenden Anfrage der betroffenen Person, einschließlich der Möglichkeit, eine Gebühr dafür zu erheben und der Frist, innerhalb derer eine solche Anfrage zu beantworten ist, unterliegt den geltenden Gesetzen. Die betroffene Person ist bei einer solchen Anfrage auf die entsprechenden Regeln hinzuweisen.

Jede betroffenen Person hat das Recht, eine Korrektur, Löschung oder Sperrung der Daten zu verlangen, insbesondere dann, wenn die Daten unvollständig oder unzutreffend sind.

Jede betroffenen Person hat das Recht, jederzeit aus zwingenden legitimen Gründen, die sich auf seine besondere Situation beziehen, der Verarbeitung seiner personenbezogenen Daten zu widersprechen. Eine Ausnahme gilt nur dort, wo gesetzliche oder aufsichtsrechtliche Anforderungen die Verarbeitung verlangen. Soweit der Widerspruch gerechtfertigt ist, muss die Verarbeitung eingestellt werden.

Jede betroffenen Person hat das Recht (ohne dass dafür eine Gebühr anfällt), der Verarbeitung seiner personenbezogenen Daten für die Zwecke des Direktmarketings zu widersprechen.

Jede betroffenen Person hat nach Artikel 12 (c) der EU-Richtlinie 95/46 das Recht, eine Benachrichtigung der Drittenüber eine Korrektur, Löschung oder Sperrung von Daten zu verlangen, an die seine Daten weitergegeben wurden.

Jede betroffenen Person hat nach Artikel 12 (a) der EU-Richtlinie 95/46 das Recht, über die Logik informiert zu werden, die eine automatische Verarbeitung der Daten bestimmt.

9 – Automatisierte Einzelentscheidungen

Automatisierte Verfahren werden lediglich als Werkzeug für den Entscheidungsfindungsprozess eingesetzt. Es findet in Bezug auf eine betroffene Person keine Bewertung oder Entscheidung statt, die ihn wesentlich berührt und ausschließlich aufgrund einer automatisierten Verarbeitung seiner Daten erfolgt, es sei denn, dass diese Entscheidung:

- im Rahmen der Eingehung oder Erfüllung eines Vertrags erfolgt. Voraussetzung ist jedoch, dass das Verlangen nach Eingehung oder Erfüllung eines Vertrags von der

betroffenen Person stammt und dass diesem Verlangen nachgegeben wurde oder dass geeignete Maßnahmen zum Schutz der legitimen Interessen der betroffenen Person getroffen wurden, wie etwa eine Vereinbarung, die es ihr/ihm erlaubt, ihre/seine Ansicht zu ergänzen oder

- nach einem Gesetz zulässig ist, das gleichzeitig Maßnahmen zur Sicherung der legitimen Interessen der betroffenen Person vorsieht.

10 – Sicherheit und Vertraulichkeit

Amgen setzt angemessene technische und organisatorische Sicherheitsmaßnahmen ein. Diese dienen dem Schutz vor und der Entdeckung von unbeabsichtigter oder ungesetzlicher Vernichtung, Verlusten, Änderungen, unbefugter Weitergabe oder unbefugten Zugriffen in Bezug auf personenbezogene Daten, insbesondere wenn die Verarbeitung eine Übermittlung über ein öffentliches Netzwerk erfordert, sowie allen anderen möglichen Formen ungesetzlicher Verarbeitung. Amgen setzt internationale Rahmenwerke wie die ISO/IEC 27002 ein, um diese Sicherheitsmaßnahmen festzulegen.

Bei Amgen bestehen Prozesse, die sicherstellen, dass mögliche Datenschutzvorfälle der Meldung und Nachverfolgung sowie angemessenen Korrekturmaßnahmen unterliegen, je nach Notwendigkeit.

Es werden Risikobewertungen der Informationssicherheit durchgeführt, um mögliche Bedrohungen für sensible personenbezogene Daten zu identifizieren. Außerdem werden, wo diese angemessen sind, zusätzliche Sicherheitskontrollen eingesetzt.

Die Umsetzung dieser Maßnahmen erfolgt entsprechend Artikel 17.1 der EU-Richtlinie 95/46 unter Beachtung modernster Technik.

Der Chief Information Security Officer (Leiter Informationssicherheit) arbeitet mit dem Chief Privacy Officer (Leiter Datenschutz) zusammen, um die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten.

11 – Beziehungen zu Auftragsverarbeitern (Datenimporteuren oder Anbietern von Amgen)

Der Datenverantwortliche wird sorgfältig einen Auftragsverarbeiter auswählen. Dieser kann entweder ein beteiligtes Unternehmen von Amgen oder ein Anbieter sein. Der Auftragsverarbeiter muss in Bezug auf seine technischen Sicherheitsmaßnahmen und die organisatorischen Maßnahmen, die diese Verarbeitung regeln, ausreichende Garantien abgeben und die Einhaltung dieser Maßnahmen gewährleisten.

Wenn nach einer Bewertung der geschäftlichen Bedürfnisse und der damit verbundenen Risiken eine Auslagerung (Outsourcing) für erforderlich gehalten wird, hat der Prozess der Auswahl des Anbieters eine Evaluation der datenschutzbezogenen Risikofaktoren zu umfassen und die geschäftlichen Bedürfnisse gegenüber den potenziellen Risiken abzuwägen.

Der Datenverantwortliche wird dem Anbieter über schriftliche vertragliche Bestimmungen in Einklang mit dem geltenden Recht insbesondere folgende Anweisungen erteilen:

(i) der Auftragsverarbeiter hat ausschließlich den Anweisungen des Datenverantwortlichen entsprechend zu handeln. Eine Verarbeitung der Daten für

die eigenen Zwecke des Auftragsverarbeiters oder für die Zwecke Dritter ist verboten und

(ii) der Auftragsverarbeiter unterliegt den Pflichten zur Sicherheit und Vertraulichkeit.

Der Datenverantwortliche hat sicherzustellen, dass der Auftragsverarbeiter die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen durchgehend einhält.

Der Datenverantwortliche bleibt weiterhin verantwortlich für die Legitimität der Datenverarbeitung und haftet der betroffenen Person weiterhin bei einer Verletzung der Rechte der betroffenen Person.

Damit dem Auftragsverarbeiter die erwähnten vertraglichen Pflichten auferlegt werden können, wird eine Vertragsvorlage mit dem Titel Datenschutzsvereinbarungbereitgestellt. Im Hinblick auf die spezielle vertragliche Situation kann der Datenverantwortliche auch anderslautende Bestimmungen aushandeln, soweit diese die oben dargelegten Verpflichtungen abdecken.

12 – Beschränkungen der Übermittlung und Weiterleitung

Als Auftragsverarbeiter agierende Anbieter sind durch schriftliche Vereinbarungen zu binden, die verlangen, dass der Anbieter ausschließlich nach den Anweisungen des Datenverantwortlichen handelt und für die Umsetzung angemessener Maßnahmen zur Wahrung von Sicherheit und Vertraulichkeit verantwortlich ist.

Alle Datenübermittlungen an Anbieter mit Sitz außerhalb der EU geschehen unter Beachtung der europäischen Regeln zu grenzüberschreitenden Datenflüssen. Dies geschieht entweder, indem die Standardvertragsklauseln der EU verwendet werden, die die EU-Kommission genehmigt hat, oder durch andere gleichwertige vertragliche Methoden entsprechend der Artikel 25 und 26 der EU-Richtlinie.

Alle Datenübermittlungen an als Datenverantwortliche fungierende Anbieter mit Sitz außerhalb der EU erfolgen unter Beachtung der sich auf die Auftragsverarbeiter beziehenden Regeln der EU-Richtlinie, zusätzlich zur Beachtung der Regeln zu grenzüberschreitenden Datenflüssen.

13 – Schulungsprogramm

Amgen bietet allen Mitarbeitern verpflichtende Schulungen zu den Datenschutzgrundsätzen und insbesondere zu den BCR an. Diese Schulung umfasst auch Informationen über die Konsequenzen von Verstößen gegen die BCR für die Mitarbeiter nach sowohl Straf- als auch Arbeitsrecht.

Diese Schulung ist eine Pflichtschulung, die jährlich zu wiederholen ist. Die erfolgreiche Teilnahme an der Schulung wird dokumentiert.

Auf Einzelfallbasis werden für die Mitarbeiter, die dauerhaft oder regelmäßig Zugang zu personenbezogenen Daten haben oder in die Erfassung personenbezogener Daten oder die Entwicklung von Werkzeugen zur Verarbeitung personenbezogener Daten involviert sind, spezielle weitere Schulungen angeboten.

Zusätzlich stellt die Datenschutzabteilung (Privacy Office) von Amgen geeignete Informationen und Ressourcen zum Datenschutz, im Intranet-Portal von Amgen oder auf anderen Kanälen bereit.

14 – Audits und Überwachungsprogramm

Amgen wird weiterhin Datenschutz-Audits auch mit der Überprüfung der Umsetzung der verbindlichen Unternehmensregeln von Amgen (BCR - Binding Corporate Rules) initieren. Das Compliance-Programm von Amgen wird entsprechend aktualisiert, um die BCR zu integrieren. Zusätzlich wird Amgen seine reguläre Datenschutzüberwachung fortsetzen, die auf lokaler Ebene von den Datenschutzbeauftragten in ihrer Eigenschaft als Leiter der Compliance Abteilungen vorgenommen wird.

Das Audit-Programm deckt alle Aspekte der BCR ab, einschließlich der Methoden zur Sicherstellung, dass Korrekturmaßnahmen ergriffen werden.

Diese Audits werden regelmäßig durch das damit beauftragte interne Audit-Team durchgeführt.

Das Audit-Programm wird in Zusammenarbeit mit dem Chief Audit Executive und dem Chief Compliance Officer entwickelt und festgelegt.

Der Chief Privacy Officer, der Chief Compliance Officer und der Chief Information Officer können jederzeit einzelfallbezogene BCR-Audits in die Wege leiten.

Alle BCR-Audits werden zeitnah dem Chief Compliance Officer und dem Chief Privacy Officer gegenüber kommuniziert. Die Zusammenfassungen und Ergebnisse der BCR-Audits werden ebenso wie andere in diesem Zusammenhang relevante Informationen regelmäßig dem Vorstand gegenüber berichtet, und zwar über entsprechende Ausschüsse (wie etwa den Ausschuss für die Verantwortung und Compliance des Unternehmen und/oder den Revisionsausschuss des Vorstands).

Den Datenschutzbehörden kann auf Anfrage eine Kopie der auf die BCR bezogenen Audit-Berichte zur Verfügung gestellt werden.

Jedes beteiligte Unternehmen ist sich bewusst, dass jederzeit eine Überprüfung durch die Datenschutzbehörden erfolgen kann. Die beteiligten Unternehmen werden sich bei allen auf die BCR bezogenen Problemen an die Vorgaben der Datenschutzbehörden halten. Jedes überprüfte Unternehmen muss den Chief Privacy Officer umgehend darüber informieren, wenn eine solche Überprüfung angekündigt wird.

15 – Einhaltung der BCR und Überwachung der Einhaltung

Amgen ernennt geeignete Mitarbeiter, darunter auch ein Netzwerk aus Datenschutzbeauftragten, deren Aufgabe es ist, mit Unterstützung der obersten Managementebene die Einhaltung dieser Regeln zu beaufsichtigen und sicherzustellen.

Die Zuständigkeiten des Chief Privacy Officers bei Amgen umfassen unter anderem folgende:

- die Beratung des Vorstands,

- das Sicherstellen der Einhaltung der Datenschutzregelungen auf globaler Ebene,
- die regelmäßige Berichterstattung über die Einhaltung der Datenschutzregelungen und
- die Zusammenarbeit mit den Datenschutzbehörden bei entsprechenden Untersuchungen.

Der Chief Privacy Officer leitet die globale Datenschutzabteilung (Privacy Office), die aus einem Team besteht, das den Unternehmen von Amgen weltweit fachkundige Unterstützung bietet.

Auf lokaler Ebene sind die Datenschutzbeauftragten verantwortlich für den Umgang mit lokalen Datenschutzanfragen der betroffenen Person, das Sicherstellen der Einhaltung der Datenschutzregelungen auf lokaler Ebene mit Unterstützung der Datenschutzabteilung und die Berichterstattung von wesentlichen Datenschutzproblemen gegenüber dem Chief Privacy Officer. Amgen unterhält ein Netzwerk von Datenschutzbeauftragten und stellt sicher, dass für jedes Land, in dem ein Unternehmen von Amgen (das beteiligte Unternehmen) geschäftlich aktiv ist, ein Datenschutzbeauftragter ernannt und beauftragt wird. Die Ernennung eines Datenschutzbeauftragten erfolgt in Absprache mit dem Manager des Datenschutzbeauftragten vor Ort, ebenso wie mit der Personalabteilung vor Ort.

Üblicherweise sind Datenschutzbeauftragte die Compliance Manager, die vor Ort für die Einhaltung der Regelungen zuständig und der globalen Abteilung für Compliance und Geschäftsethik unterstellt sind. Die Datenschutzabteilung ist ebenfalls der globalen Abteilung für Compliance und Geschäftsethik unterstellt. In seltenen Fällen kann der Datenschutzbeauftragte aufgrund der Besonderheiten des Amgen-Unternehmens oder spezieller Umstände auch einer anderen Funktion entstammen, wie etwa einer mit aufsichtsrechtlichenFragen befassten Funktion. Auf jeden Fall hat die Datenschutzabteilung sicherzustellen, dass die Datenschutzbeauftragten angemessen geschult werden und über ein ausreichendes Maß an Führungsqualitäten und Sachkenntnis verfügen, um ihre Funktion als Datenschutzbeauftragte wahrnehmen zu können. Zusätzlich verfügen die Datenschutzbeauftragten über eine direkte Verbindung zum Chief Privacy Officer ebenso wie zu den Mitarbeitern der Datenschutzabteilung, falls sie zusätzliche Unterstützung benötigen.

16 – Vorgehen in den Fällen, in denen die nationale Gesetzgebung eine Umsetzung der BCR verhindert

Wenn ein Mitglied des Konzerns Grund zur Annahme hat, dass die für sie/ihn geltende Gesetzgebung das Unternehmen davon abhält, seinen sich aus den BCR ergebenden Verpflichtungen nachzukommen und wesentliche Auswirkungen auf die durch diese Regeln bereitgestellten Garantien hat, wird dieses Mitglied unverzüglich den Chief Privacy Officer davon in Kenntnis setzen(Eine Ausnahme gilt nur dort, wo eine Strafverfolgungsbehörde dies verbietet, so wie dies beispielsweise nach strafrechtlichen Regeln der Fall ist, um die Vertraulichkeit der Ermittlungen zu bewahren).

Bei einem Konflikt zwischen dem nationalen Recht und den sich aus den BCR ergebenden Verpflichtungen wird der Chief Privacy Officer das weitere Vorgehen in Absprache mit dem Rechtsberater und dem Datenschutzbeauftragten vor Ort festlegen und entscheiden, welche angemessenen rechtlichen Maßnahmen erforderlich sind. Falls dies notwendig sein sollte, wird der Chief Privacy Officer sich dabei auch mit den zuständigen Datenschutzbehörden absprechen.

17 – Interner Beschwerdemechanismus

Amgen wird seinen bestehenden Prozess für den Umgang mit Beschwerden erweitern und nutzen, um den Umgang mit auf die BCR bezogenen Beschwerden oder Bedenken zu integrieren.

Jede betroffene Person kann jederzeit eine Beschwerde mit der Behauptung vorbringen, dass sich ein beteiligtes Unternehmen nicht an die BCR hält. Zuständig für die Bearbeitung dieser Beschwerden ist die Datenschutzabteilung (Privacy Office) unter der Leitung des Chief Privacy Officer und in Zusammenarbeit mit dem jeweiligen Datenschutzbeauftragten vor Ort.

Amgen empfiehlt, dass solche Beschwerden schriftlich entweder per Post oder E-Mail direkt gegenüber der Datenschutzabteilung oder dem betreffenden Unternehmen vorzubringen sind. Die betroffenen Personen können, soweit dies nach den geltenden Gesetzen akzeptabel ist, mit den BCR zusammenhängende Beschwerden auch bei der Business Conduct Hotline vorbringen.

Wenn eine Beschwerde vor Ort vorgebracht wird, hat der Datenschutzbeauftragte diese ggf. zu übersetzen und unverzüglich an die Datenschutzabteilungweiterzuleiten.

Die betroffene Person erhält eine erste Antwort auf die Beschwerde. Darin wird ihr/ihm mitgeteilt, dass die Beschwerde in Bearbeitung ist und eine abschließende Beantwortung innerhalb einer Frist von zwei Monaten erfolgen wird.

Wenn die Datenschutzabteilung ein individuelles Fehlverhalten feststellt, werden in dem Ausmaß, in dem das geltende Recht dies erlaubt, geeignete disziplinarische Maßnahmen ergriffen. Dies kann bis hin zu und einschließlich einer Kündigung des Beschäftigungsverhältnisses reichen.

Die betroffenen Person wird innerhalb einer Frist von höchstens zwei Monaten eine abschließende Antwort auf seine Beschwerde erhalten, die die betroffenen Person über den Ausgang des Beschwerdeverfahrens informiert.

Dabei wird die betroffene Person auch darüber informiert, dass sie/er im Fall der Unzufriedenheit mit der Antwort von Amgen berechtigt ist, eine Klage/Beschwerde vor dem zuständigen Gericht oder der zuständigen Datenschutzbehörde vorzubringen.

Dieser Prozess für den Umgang mit Beschwerden wird durch eine Veröffentlichung der BCR wie in § 7 erwähnt öffentlich bekanntgemacht.

18 – Rechte von Drittbegünstigten und Haftung

Eine betroffene Person, deren personenbezogene Daten ihren Ursprung in einem regulierten Land haben und das einen Verstoß gegen die Verpflichtungen behauptet, die in den BCR festgelegt werden, hat das Recht, diese Regeln als Drittbegünstigter durchzusetzen. Diese Rechte umfassen die gerichtlichen Rechtsmittel bei Verletzungen der garantierten Rechte und das Recht auf Schadensersatz. Im Falle einer Haftung ist diese auf den tatsächlich eingetretenen Schaden beschränkt.

Soweit die relevanten gesetzlichen Zuständigkeitsregeln dies erlauben, kann die betroffenen Person Ansprüche bei folgenden Stellen vorbringen:

- bei einem Gericht am Gerichtsstand des Datenexporteurs, und falls die personenbezogenen Daten der betroffenen Person ihren Ursprung bei einem EWR-Datenexporteur haben, ist der Gerichtsstand der Ort, an dem der EWR-Datenexporteur seinen Sitz hat oder
- vor den zuständigen Datenschutzbehörden.

Jede betroffenen Person, die von einer Verletzung der in den BCR festgehaltenen Verpflichtungen durch den Datenexporteur oder Datenimporteur betroffen ist, hat einen Anspruch auf Schadensersatz für den erlittenen Schaden. Wenn der Datenimporteur oder der Datenexporteur für einen Verstoß gegen die Regeln der BCR haften, hat der Haftende den anderen im Ausmaß seiner Haftung in Bezug auf alle Kosten, Gebühren, Schäden, Auslagen oder Verluste schad- und klaglos zu stellen, die dieser erleidet.

Sowohl Datenexporteur als auch Datenimporteur können von einer Haftung nach den BCR befreit sein, wenn sie nachweisen, dass das Mitglied des Konzerns, das sich außerhalb der EU befindet, nicht gegen die BCR verstoßen hat oder nicht verantwortlich für den der betroffenen Person entstandenen Schaden ist. Die Beweislast liegt dabei jedoch bei Datenexporteur und Datenimporteur.

Der Verstoß eines ihm unterstellten Verarbeiters (Unter-Verarbeiters) gegen die sich aus den BCR ergebenden Verpflichtungen befreit den als Auftragsverarbeiter fungierenden Datenimporteur nicht von seiner Haftung. Wenn die betroffene Person Ansprüche gegen den Datenexporteur geltend machen möchte, dazu jedoch infolge eines Verstoßes gegen die BCR nicht in der Lage ist, weil der Datenexporteur faktisch verschwunden ist, rechtlich nicht mehr existiert oder insolvent wurde, kann die betroffene Person ihre Rechte direkt gegenüber dem Datenimporteur geltend machen. Wenn eine juristische Person als Rechtsnachfolger die gesamten gesetzlichen Verpflichtungen von Datenexporteur oder Datenimporteur durch Vertrag oder von Gesetzes wegen übernommen hat, kann die betroffene Person ihre Rechte gegenüber diesem Rechtsnachfolger geltend machen. Die Haftung des Datenimporteurs ist beschränkt auf seine eigenen Verarbeitungsmaßnahmen, die er nach den BCR durchführt.

19 – Gegenseitige Unterstützung und Zusammenarbeit mit den Datenschutzbehörden

Die beteiligten Unternehmen sind dazu verpflichtet, beim Umgang mit einer Anforderung oder Beschwerde einer betroffenen Person oder einer Ermittlung oder Untersuchung durch Datenschutzbehörden zusammenzuarbeiten und sich gegenseitig zu unterstützen.

Die beteiligten Unternehmen werden auf die BCR-bezogenen Anfragen der Datenschutzbehörden in Absprache mit dem Chief Privacy Officer innerhalb einer angemessenen Frist und auf angemessene Weise beantworten und den Rat und die Entscheidungen der zuständigen Datenschutzbehörden in Bezug auf die BCR befolgen.

20 – Aktualisierung und Änderungen der BCR

Amgen behält sich das Recht vor, die BCR jederzeit zu ändern und/oder zu aktualisieren. Eine solche Aktualisierung der BCR kann insbesondere aufgrund geänderter gesetzlicher Anforderungen, wesentlicher Änderungen in der Struktur des Amgen-Konzerns oder offizieller Auforderungen der zuständigen Datenschutzbehörden vorgenommen werden, erforderlich werden.

Amgen wird wesentliche Änderungen der BCR oder der Liste der beteiligten Unternehmen allen anderen beteiligten Unternehmen und den Datenschutzbehörden mitteilen, damit diese die Änderungen im regulatorischen Umfeld und in der Unternehmensstruktur berücksichtigen können.

Manche Änderungen erfordern möglicherweise eine erneute Genehmigung durch die Datenschutzbehörden.

Der Chief Privacy Officer pflegt eine aktuelle Liste aller teilnehmenden Unternehmen und der regulierten Ländern die nach den BCR geschützt sein können. Er wird weiterhin alle Aktualisierungen der Regeln nachverfolgen und auf Anforderung den betroffenen Personenoder Datenschutzbehörden die notwendigen Informationen zur Verfügung stellen.

Amgen verpflichtet sich, dass keine Übermittlungen an neue beteiligte Unternehmen stattfinden, die unter die Garantien der BCR fallen, bis das neue beteiligte Unternehmen effektiv durch die BCR gebunden ist und sich daran hält.

Alle Veränderungen der BCR oder der Liste der beteiligten Unternehmen werden einmal jährlich den Datenschutzbehörden gemeldet, die die entsprechenden Genehmigungen erteilen. Dieser Meldung wird eine kurze Erklärung der Gründe für die Aktualisierungen beigefügt.

Wesentliche Änderungen der Regeln werden darüber hinaus auch den betroffenen Personengegenüber kommuniziert, und zwar über die Methoden wie in § 7 der BCR vorgesehen.

21 – Die Beziehung zwischen den nationalen Gesetzen und den BCR

Dort, wo die örtliche Gesetzgebung höhere Anforderungen an den Schutz von personenbezogenen Daten stellt, geht diese den BCR vor. Dort, wo die örtliche Gesetzgebung geringere Anforderunge an den Schutz von personenbezogenen Daten stellt als die BCR, sind die BCR anzuwenden.

Falls die sich aus den geltenden örtlichen Gesetzen ergebenden Verpflichtungen mit den Anfoderungen aus den BCR ergebenen im Widerspruch stehen, hat das beteiligte Unternehmen unverzüglich den Chief Privacy Officer darüber zu informieren.

Personenbezogene Daten werden in jedem Fall in Einklang mit dem geltenden Recht verarbeitet, so wie dies in Artikel 4 der EU-Richtlinie 95/46/EG festgelegt ist, sowie den entsprechenden lokalen gesetzlichen Regelungen.