



Openbaar document: Bindende bedrijfsvoorschriften (BCR's) van Amgen

Nederlandse vertaling van de Amgen BCR's

Inleiding:

Amgen is een toonaangevend biotechnologisch bedrijf dat zich inzet voor mensen bij het bestrijden van ernstige ziekten.

De bindende bedrijfsvoorschriften (Binding Corporate Rules, BCR's) vormen de uitdrukking van Amgen's streven naar adequate privacy- en gegevensbescherming bij de doorgifte en verwerking van Persoonsgegevens tussen de verschillende entiteiten van Amgen.

Alle entiteiten binnen Amgen en alle medewerkers van Amgen verplichten zich tot naleving van de BCR's. Niet-naleving kan leiden tot disciplinaire acties, voorzover toegestaan door lokale wetgeving.

De Chief Compliance Officer zorgt samen met de Chief Privacy Officer voor naleving van de uiteengezette regels.

De BCR's zijn mede vastgesteld op basis van de huidige toepasselijke Europese teksten op het gebied van gegevensbescherming, namelijk EU-Richtlijnen 95/46/EG en 2002/58/EG.

1 – Reikwijdte

De BCR's van Amgen zijn van toepassing op de geautomatiseerde of handmatige doorgifte en verwerking van alle persoonsgegevens van werknemers, klanten, leveranciers, aandeelhouders, patiënten en alle overige betrokkenen door een van de bedrijven van Amgen die als verwerkingsverantwoordelijke optreden in de volgende gevallen:

- a) het bedrijf van Amgen dat de persoonsgegevens verwerkt, is in een gereguleerd land gevestigd; of
- b) het bedrijf van Amgen dat de persoonsgegevens verwerkt, is niet in een gereguleerd land gevestigd (“Gegevensimporteur”) en heeft de persoonsgegevens ontvangen van een bedrijf van Amgen dat wel in een gereguleerd land is gevestigd, als gedefinieerd in Artikel 2 (“Gegevensexporteur”).

Deze BCR's zijn ook van toepassing op verdere doorgifte van persoonsgegevens door gegevensimporteurs aan gegevensimporteurs.

2 – Definitie

Termen	Definitie
--------	-----------

<p>Persoonsgegevens</p>	<p>Gegevens betreffende een persoon van wie de identiteit op basis van die gegevens, ofwel direct ofwel indirect, duidelijk is of kan worden vastgesteld. Ook kunnen persoonsgegevens worden gezien als gegevens die, ofwel losstaand ofwel in combinatie met andere gegevens, de identiteit van een individuele persoon kunnen vaststellen, of als gegevens die gebruikt kunnen worden om contact met hem of haar op te nemen of hem of haar te lokaliseren. Afhankelijk van lokale privacy- en gegevensbeschermingwetgeving, zijn dit enkele voorbeelden van persoonsgegevens:</p> <ul style="list-style-type: none"> • Naam, adres, burgerservicenummer, rijbewijsnummer, bank- en financiële gegevens, familiegegevens of medische gegevens van een persoon, • Naam, opleiding en voorschrijfgedrag van een arts, • E-mailadres en andere identificerende gegevens die verstrekt worden door een bezoeker van een website van Amgen. <p>Bovenstaande opsomming dient slechts als voorbeeld en is niet uitputtend.</p>
<p>Gevoelige persoonsgegevens</p>	<p>Informatie over een betrokkene zoals:</p> <ul style="list-style-type: none"> • Aandoeningen of gezondheidstoestand (lichamelijk of geestelijk) • Financiële informatie • Ras of etnische afkomst • Politieke overtuiging • Geloof of filosofische visie • Lidmaatschap van een vakbond • Seksuele voorkeur • Strafrechtelijke veroordelingen of een strafblad <p>Amgen beschouwt gegevens die gebruikt kunnen worden om identiteitsdiefstal te plegen, zoals een burgerservicenummer, rijbewijsnummer, creditcard- en bankrekeninggegevens, als gevoelige gegevens.</p>
<p>Betrokkene</p>	<p>De persoon op wie de persoonsgegevens betrekking hebben. Een betrokkene kan (onder andere) zijn een:</p> <ul style="list-style-type: none"> • Patiënt/consument/deelnemer aan een klinisch onderzoek • Beroepsbeoefenaar in de gezondheidszorg (bijv. een arts) • Werknemer (huidig, voormalig of gepensioneerd) • Consultant/zzp'er/leverancier/adviseur
<p>Verwerkingsverantwoordelijke (Data Controller)</p>	<p>Elke entiteit die beslissingen neemt met betrekking tot het verzamelen en verwerken van persoonsgegevens,</p>

	inclusief beslissingen over de doeleinden waarvoor, en de manier waarop, persoonsgegevens worden verwerkt.
Gegevensverwerker	Een natuurlijke persoon of entiteit die namens een verwerkingsverantwoordelijke Persoonsgegevens verwerkt.
Verwerking	Elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet met behulp van geautomatiseerde verwerking, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Derde partij	Een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of enig ander lichaam, niet zijnde de Betrokkene, noch de verwerkingsverantwoordelijke, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke gemachtigd zijn om gegevens te verwerken. Bij Amgen wordt een Leverancier beschouwd als een Derde partij.
Leverancier	Een persoon, onderneming of organisatie die goederen en/of diensten aan Amgen levert, een contractuele relatie met Amgen heeft en/of Persoonsgegevens ontvangt van Amgen, en die verplicht is deze goederen en/of diensten te leveren.
Gegevensbeschermingsautoriteiten (Data Protection Authorities, DPA's)	Een of meer autoriteiten die in hun Lidstaat belast zijn met het toezicht op de toepassing op hun grondgebied van de uitvoering van Richtlijn 95/46 door de lidstaten vastgestelde bepalingen. Deze autoriteiten vervullen de hun opgedragen taken in volledige onafhankelijkheid.
Gereguleerd land	Een land in de Europese Economische Ruimte (EER) of een land met een passend gegevensbeschermingsniveau, als bevestigd door een besluit van de EU-Commissie, of andere landen die BCR's erkennen als legitieme methode voor het doorgeven van persoonsgegevens buiten hun rechtsgebied..Dit betreft o.a. Andorra, Argentinië; Canada; Faeröer eilanden; Guernsey;eiland Man; Israel; Jersey; Nieuw Zeeland; Zwitserland; Uruguay.
Gegevensexporteur	Een Amgen-entiteit die opereert als een in een gereguleerd land gevestigde verwerkingsverantwoordelijke die persoonsgegevens

	doorgeeft aan een andere Amgen-entiteit die niet in een gereguleerd land is gevestigd (gegevensimporteur)
Gegevensimporteur	Een niet in een gereguleerd land gevestigde Amgen-entiteit die persoonsgegevens ontvangt van een gegevensexporteur
Technische en organisatorische beveiligingsmaatregelen	Maatregelen die gericht zijn op het beveiligen van persoonsgegevens tegen onrechtmatige vernietiging of onbedoeld verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onrechtmatige verwerking.
Deelnemend bedrijf	Een entiteit binnen de Amgen-groep die gebonden is aan de BCR's.
Toestemming	Elke vrije, specifieke en op informatie berustende wilsuiting door een betrokkene waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verzameld en verwerkt.
Functionaris voor de gegevensbescherming (Data Protection Officer, DPO)	Medewerker binnen het bedrijf die door een verbonden onderneming of door het management van een BU is aangewezen als verantwoordelijke voor het toezicht op Privacy- en Gegevensbescherming op lokaal niveau en voor de tenuitvoerlegging van passende en vereiste beveiligingsmaatregelen.

Amgen interpreteert de termen in de BCR's volgens EU-Richtlijnen 95/46/EG en 2002/58/EG, hierna genoemd: de EU-Richtlijn.

3 – Beperking van de doeleinden

Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verwerkt conform Artikel 6.1(b) van Richtlijn 95/46,.

Persoonsgegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de legitieme doeleinden waarvoor de persoonsgegevens zijn verzameld. Bij het opslaan en/of verder verwerken of gebruiken van gegevens die door een ander deelnemend bedrijf aan hen zijn doorgegeven, zijn gegevensimporteurs verplicht zich aan de oorspronkelijke doeleinden te houden. Het doel van de gegevensverwerking mag slechts worden gewijzigd met toestemming van de betrokkene of voorzover toegestaan door de lokale wetgeving waaraan de gegevensexporteur die de gegevens doorgeeft, is onderworpen.

Gevoelige gegevens worden uitgerust met aanvullende waarborgen, zoals bepaald in EU-Richtlijn 95/46/EG.

4 - Kwaliteit en evenredigheid van de gegevens

De Persoonsgegevens moeten feitelijk juist zijn en waar nodig up-to-date worden gehouden. Passende maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste of onvolledige gegevens worden gecorrigeerd of gewist.

Persoonsgegevens moeten toereikend en ter zake dienend zijn, als bepaald in Artikel 6.1(c) van Richtlijn 95/46.

Gegevensverwerking, het verzamelen, verwerken en/of gebruiken van Persoonsgegevens moet worden beperkt tot het strikt noodzakelijke, oftewel zo weinig mogelijk Persoonsgegevens. Waar mogelijk moet het gebruik van anonieme of pseudonieme gegevens worden nagestreefd, met dien verstande dat de bijbehorende kosten en inspanningen in verhouding staan tot het gewenste doel.

Persoonsgegevens die niet langer nodig zijn voor het zakelijke doel waarvoor ze oorspronkelijk waren verzameld en opgeslagen, moeten in overeenstemming met het Amgen Record Retention Schedule worden verwijderd. In het geval van een wettelijke bewaartermijn- of plicht, worden de gegevens niet verwijderd maar afgeschermd. Na het verstrijken van de bewaartermijn- of plicht worden de gegevens verwijderd.

5 – Rechtsgrond voor Verwerking van Persoonsgegevens

Verwerking van persoonsgegevens is slechts toegestaan indien voldaan is aan ten minste één van de volgende voorwaarden:

- De betrokkene heeft vrijwillig en ondubbelzinnig zijn of haar toestemming verleend
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waar de betrokkene partij bij is, of voor een soortgelijke vertrouwensrelatie, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen
- De Verwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verwerkingsverantwoordelijke onderworpen is, of de verwerking is voorgeschreven of toegestaan door toepasselijke wet- en regelgeving
- De verwerking is noodzakelijk om een vitaal belang van de betrokkene, zoals diens leven, gezondheid of veiligheid, veilig te stellen
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag dat is verleend aan de verwerkingsverantwoordelijke of aan een derde partij aan wie de gegevens worden verstrekt
- De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verwerkingsverantwoordelijke of van de derde partij aan wie de gegevens worden verstrekt, mits dat belang minder zwaar weegt dan het gerechtvaardigde belang dat de betrokkene heeft bij zijn of haar fundamentele rechten en vrijheden

6 – Verwerking van gevoelige gegevens

Wanneer Amgen voor een specifiek en gerechtvaardigd doeleinde gevoelige gegevens moet verwerken, zal ze dat slechts doen indien:

- De betrokkene heeft zijn of haar uitdrukkelijke toestemming gegeven voor de verwerking van die gevoelige gegevens, behalve wanneer de toepasselijke wetgeving de verwerking verbiedt
- De verwerking is noodzakelijk met het oog op de uitvoering van de arbeidsrechtelijke verplichtingen en specifieke rechten van de verwerkingsverantwoordelijke, voorzover zulks is toegestaan bij de nationale wetgeving en deze adequate garanties biedt
- De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere persoon indien deze lichamelijk of juridisch niet bekwaam is om toestemming te geven
- De verwerking wordt verricht door een stichting, een vereniging, of enige andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van hun gerechtvaardigde activiteiten en met de nodige garanties, mits de verwerking uitsluitend betrekking heeft op de leden van de stichting, de vereniging of de instantie of op de personen die in verband met haar streefdoelen regelmatige contacten met haar onderhouden, en de gegevens niet zonder de toestemming van de betrokkenen aan derde partijen worden doorgegeven
- De verwerking heeft betrekking op gevoelige Gegevens die kennelijk door de betrokkene openbaar zijn gemaakt
- De Verwerking van gevoelige gegevens is noodzakelijk voor de vaststelling, de uitoefening of de verdediging van een juridische zaak. 1
- De Verwerking van de gevoelige gegevens is noodzakelijk voor de doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen of het beheer van gezondheidsdiensten en wanneer die gevoelige gegevens worden verwerkt door een gezondheidswerker die onderworpen is aan het in de nationale wetgeving, of in de door nationale bevoegde instanties vastgestelde regelgeving, vastgelegde beroepsgeheim of door een andere persoon voor wie een gelijkwaardige geheimhoudingsplicht geldt

7 – Transparantie en recht op informatie

Alle deelnemende bedrijven dienen persoonsgegevens op transparante wijze te verwerken. Amgen verbindt zich ertoe om de BCR's, inclusief contactgegevens, vrij beschikbaar te stellen aan iedere betrokkene en om betrokkenen te informeren over de doorgifte en verwerking van hun persoonsgegevens.

Daartoe maakt Amgen gebruik van diverse communicatiemiddelen, zoals zakelijke websites, inclusief interne websites en nieuwsbrieven, contracten en ook specifieke privacyverklaringen die daar waar nodig ter ondersteuning toegevoegd worden.

Betrokkenen van wie persoonsgegevens worden verwerkt door een deelnemend bedrijf ontvangen de volgende informatie:

- De identiteit van de verwerkingsverantwoordelijke(n) en, in voorkomend geval, van diens vertegenwoordiger;
- De doeleinden van de verwerking waarvoor de gegevens zijn bestemd;
- De herkomst van de gegevens (tenzij er sprake is van persoonsgegevens die rechtstreeks bij de betrokkene worden verzameld)
- Verdere informatie zoals:
 - i) de ontvangers of de categorieën ontvangers van de gegevens;

- ii) het bestaan van een recht op toegang tot gegevens die op hem betrekking hebben en op wijziging van deze gegevens, voorzover bedoelde aanvullende informatie noodzakelijk is en met inachtneming van de specifieke omstandigheden waaronder de verdere informatie verkregen wordt, teneinde de betrokkene een eerlijke verwerking te waarborgen.

Wanneer de gegevens niet worden ontvangen van een betrokkene, is de informatieplicht jegens de betrokkene niet van toepassing indien het verstrekken van deze informatie onmogelijk blijkt of gepaard zou gaan met disproportionele inspanningen, of indien vastlegging of onthulling uitdrukkelijk is neergelegd in de wet.

8 – Recht op toegang, wijziging, verwijderen en afscherming van gegevens

Iedere betrokkene heeft het recht om zonder beperking, met redelijke tussenpozen, de gegevens die verwerking ondergaan in begrijpelijke vorm en de beschikbare informatie over de oorsprong van de gegevens, verstrekt te krijgen. De opvolging van dit verzoek, inclusief de mogelijkheid een vergoeding in rekening te brengen en de termijn voor het reageren op een dergelijk verzoek, is onderworpen aan toepasselijke wetgeving en wordt op passende wijze aan de betrokkene meegedeeld, wanneer hij/zij zijn/haar verzoek indient.

Iedere betrokkene heeft het recht op wijziging, verwijderen of afscherming van de gegevens, met name wanneer de gegevens onvolledig of onjuist zijn.

Iedere betrokkene heeft ten allen tijde het recht zich te verzetten tegen de verwerking van zijn persoonsgegevens indien daar dwingende rechtmatige persoonlijke gronden toe bestaan, tenzij die verwerking verplicht is krachtens wet- of regelgeving. In het geval van gerechtvaardigd bezwaar moet de verwerking worden stopgezet.

Iedere betrokkene heeft het recht zich (kosteloos) te verzetten tegen verwerking van hem of haar betreffende Persoonsgegevens ten behoeve van direct-marketing.

Iedere Betrokkene heeft het recht op het verkrijgen van de kennisgeving van wijziging, verwijdering of afscherming aan derden aan wie de gegevens zijn verstrekt, als bepaald in Artikel 12(c) van Richtlijn 95/46.

Iedere betrokkene heeft het recht op het vernemen van de logica die ten grondslag ligt aan de automatische verwerking van gegevens, als bepaald in Artikel 12(a) van Richtlijn 95/46.

9 – Geautomatiseerde individuele besluiten

Geautomatiseerde procedures worden alleen gebruikt als hulpmiddel bij het besluitvormingsproces. Geen enkele evaluatie van of beslissing over een betrokkene die hem of haar in aanmerkelijke mate treft, wordt uitsluitend gebaseerd op geautomatiseerde verwerking van zijn of haar gegevens, tenzij die beslissing:

- wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst, mits aan het verzoek van de betrokkene is voldaan of passende maatregelen, zoals de mogelijkheid zijn standpunt te doen gelden, zijn genomen ter bescherming van zijn legitieme belangen; of

- zijn grondslag vindt in een wet waarin ook maatregelen zijn opgenomen die strekken tot bescherming van de legitieme belangen van de betrokkene.

10 – Beveiliging en vertrouwelijkheid

Amgen legt passende technische en organisatorische beveiligingsmaatregelen op die gericht zijn op het beveiligen van persoonsgegevens tegen - en het detecteren van - vernietiging, hetzij per ongeluk, hetzij onrechtmatig vernietiging, verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens binnen een openbaar netwerk omvat, dan wel tegen enige andere potentiële vorm van onwettige verwerking. Internationale raamwerken als ISO/IEC 27002 worden door Amgen gebruikt om deze beveiligingsmaatregelen vast te stellen.

Amgen hanteert processen om te waarborgen dat potentiële privacy-incidenten worden gemeld en gevolgd, en dat - waar nodig - passende correctie maatregelen worden genomen.

Risicobeoordelingen op het gebied van informatiebeveiliging worden gebruikt voor het opsporen van potentiële bedreigingen voor gevoelige persoonsgegevens en, in voorkomende gevallen, voor het ten uitvoer leggen van aanvullende beveiligingsmaatregelen.

Bij de tenuitvoerlegging van de maatregelen wordt rekening gehouden met de stand van de techniek, als bedoeld in Artikel 17.1 van Richtlijn 95/46.

De Chief Information Security Officer werkt samen met de Chief Privacy Officer om de beveiliging en geheimhouding van persoonsgegevens te waarborgen.

11 – Relaties met gegevensverwerkers (gegevensimporteur of leverancier van Amgen)

De verwerkingsverantwoordelijke moet een gegevensverwerker die een bedrijf van Amgen of een leverancier kan zijn, zorgvuldig uitkiezen. De verwerker moet voldoende waarborgen treffen ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerking en moet toezien op de naleving van die maatregelen.

Wanneer uitbesteding noodzakelijk wordt geacht na het beoordelen van de bedrijfsbehoeften en -risico's van een dergelijke uitbesteding, moet het selectieproces van de leverancier een evaluatie van de privacyrisicofactoren en een afweging tussen de bedrijfsbehoeften en de mogelijke risico's omvatten.

Via een schriftelijke overeenkomst en in overeenstemming met de toepasselijke wetgeving zal de verwerkingsverantwoordelijke onder andere het volgende opleggen aan de leverancier:

- i) de verwerker mag slechts handelen in opdracht van de verwerkingsverantwoordelijke, en de verwerking van gegevens voor eigen doeleinden van de verwerker of voor doeleinden van een derde is verboden; en
- ii) de regels met betrekking tot de beveiliging en geheimhouding rusten ook op de verwerker.

De verwerkingsverantwoordelijke dient ervoor te zorgen dat de verwerker de overeengekomen technische en organisatorische beveiligingsmaatregelen volledig blijft naleven.

De verwerkingsverantwoordelijke blijft verantwoordelijk voor de legitimiteit van de verwerking en blijft aansprakelijk voor de rechten van de betrokkene.

Om genoemde contractuele verplichtingen vast te leggen, wordt een contractsjabloon getiteld Data Privacy Schedule beschikbaar gesteld. Met betrekking tot de specifieke contractuele situatie kan de verwerkingsverantwoordelijke andere bepalingen op laten nemen, maar bovengenoemde verplichtingen moeten opgenomen blijven.

12 – Beperkingen op doorgifte en verdere doorgifte

Leveranciers die optreden als gegevensverwerkers zijn gebonden aan schriftelijke overeenkomsten waarin is bepaald dat de leverancier slechts in opdracht van de verwerkingsverantwoordelijke mag handelen en verantwoordelijk is voor de tenuitvoerlegging van afdoende beveiligings- en geheimhoudingsmaatregelen.

Bij de doorgifte van gegevens aan leveranciers buiten de EU worden de Europese voorschriften betreffende grensoverschrijdende gegevensstromen in acht genomen, ofwel door gebruikmaking van de EU-modelcontractbepalingen zoals goedgekeurd door de EU-Commissie, ofwel door andere gepaste contractuele middelen volgens Artikel 25 en 26 van de EU-Richtlijn.

Bij de doorgifte van gegevens aan leveranciers die optreden als gegevensverwerkers buiten de EU worden - naast de voorschriften betreffende grensoverschrijdende gegevensstromen - de bepalingen van de EU-Richtlijn met betrekking tot verwerkers gerespecteerd.

13 – Trainingsprogramma

Amgen biedt alle medewerkers passende training op het gebied van privacybeginselen en op het gebied van de BCR's. Deze training omvat ook informatie over de straf- en arbeidsrechtelijke gevolgen voor medewerkers die de BCR's schenden.

De training is verplicht en wordt jaarlijks herhaald. Succesvolle deelname aan de training wordt gedocumenteerd.

Specifieke cursussen worden per geval gegeven aan medewerkers die doorlopend of regelmatig toegang hebben tot persoonsgegevens, of die betrokken zijn bij het verzamelen van persoonsgegevens of bij het ontwikkelen van hulpmiddelen die gebruikt worden voor de verwerking van persoonsgegevens.

Daarnaast verstrekt het Privacy Office van Amgen passende informatie en middelen met betrekking tot privacy op het intranetportaal van Amgen en via andere manieren.

14 – Audit- en monitoringprogramma

Terwijl Amgen de bindende bedrijfsvoorschriften (BCR's) initieert blijven de privacyaudits bestaan en wordt het nalevingsprogramma van Amgen bijgewerkt om de BCR's op te nemen.



Daarnaast gaat Amgen door met haar reguliere privacymonitoring, die lokaal wordt uitgevoerd door de functionarissen voor de gegevensbescherming (DPO's (Data Protection Officers)) in hun hoedanigheid van Compliance Lead.

Het Auditprogramma bestrijkt alle aspecten van de BCR's, inclusief methoden om te waarborgen dat corrigerende maatregelen worden genomen.

Deze Audits worden regelmatig uitgevoerd door het interne geaccrediteerde auditteam.

Het Auditprogramma wordt in overleg ontwikkeld en overeengekomen door de Chief Audit Executive en de Chief Compliance Officer,

De Chief Privacy Officer, de Chief Compliance Officer en de Chief Information Officer kunnen te allen tijde het initiatief nemen tot ad hoc BCR-gerelateerde Audits.

Alle BCR-auditrapporten worden tijdig gecommuniceerd aan de Chief Compliance Officer en aan de Chief Privacy Officer. De BCR-gerelateerde Audit-samenvattingen en -bevindingen en andere relevante informatie, worden regelmatig gerapporteerd aan de directie via daarvoor bedoelde commissies (bijv. Corporate Responsibility & Compliance-commissie en/of Auditcommissie van de directie).

De gegevensbeschermingsautoriteiten kunnen op verzoek een exemplaar van BCR-gerelateerde auditrapporten toegezonden krijgen.

Elk deelnemend bedrijf begrijpt dat het onderworpen kan worden aan audits door de gegevensbeschermingsautoriteiten en zij dienen de adviezen van de gegevensbeschermingsautoriteiten betreffende elke kwestie die met de BCR's verband houdt, op te volgen. Elke gecontroleerde entiteit moet de Chief Privacy Officer onmiddellijk inlichten wanneer een dergelijke Audit wordt aangekondigt en plaatsvindt.

15 – Naleving en toezicht op naleving

Amgen stelt geschikte medewerkers aan, inclusief een netwerk van functionarissen voor de gegevensbescherming (Data Protection Officers), met ondersteuning van het topmanagement, om toezicht te houden op naleving van de voorschriften en om naleving te waarborgen.

Bij Amgen omvatten de verantwoordelijkheden van de Chief Privacy Officer onder meer:

- advisering van de directie,
- naleving van gegevensbescherming waarborgen op mondiaal niveau
- regelmatige rapportage inzake naleving van gegevensbescherming; en
- verlening van medewerking aan onderzoeken door gegevensbeschermingsautoriteiten

De Chief Privacy Officer heeft de leiding over het Global Privacy Office, een team dat wereldwijd deskundige ondersteuning biedt aan onderdelen van de Amgen-groep.

Op lokaal niveau zijn Data Protection Officers verantwoordelijk voor het behandelen van lokale privacyverzoeken van betrokkenen, voor het - met ondersteuning van het Privacy Office - waarborgen van naleving op lokaal niveau, en voor het melden van belangrijke privacykwesties

aan de Chief Privacy Officer. Amgen beschikt over een netwerk van functionarissen voor de gegevensbescherming (DPO's) en zorgt ervoor dat er een DPO benoemd of aangewezen wordt voor elk land waar Amgen (het Deelnemend Bedrijf) een bedrijfsentiteit heeft. Deze aanstelling vindt plaats in overleg met de lokale manager van de DPO en de lokale HR-afdeling.

Over het algemeen worden de DPO's gevormd door de lokale Healthcare Compliance Managers, die rapporteren aan de afdeling Worldwide Compliance and Business Ethics. Ook het Privacy Office rapporteert aan de afdeling Worldwide Compliance and Business Ethics. In zeldzame gevallen, door het specifieke karakter van een Amgen-entiteit of in bijzondere situaties, kan het voorkomen dat de DPO afkomstig is uit een andere functie, bijvoorbeeld Regulatory. In elk geval zorgt het Privacy Office ervoor dat de DPO's goede training ontvangen en een toereikend niveau qua leidinggeven en expertise bezitten om hun DPO-rol te vervullen. Bovendien hebben de DPO's een directe lijn met de Chief Privacy Officer en met de medewerkers van het Privacy Office voor het geval dat ze extra aansturing nodig hebben.

16 – Acties wanneer nationale wetgeving naleving van BCR's tegenhoudt

Wanneer een lid van de groep reden heeft om aan te nemen dat de op hem of haar van toepassing zijnde wetgeving het bedrijf ervan weerhoudt zijn of haar verplichtingen uit hoofde van de BCR's te vervullen en dat deze wetgeving wezenlijke gevolgen heeft voor de garanties die de BCR's bieden, dient hij of zij de Chief Privacy Officer daar onmiddellijk van in kennis te stellen (behalve wanneer dat verboden is door een wetshandhavinginstantie, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijk van een wetshandhavingsonderzoek te bewaren).

Wanneer er sprake is van strijdigheid tussen de nationale wetgeving en de verplichtingen in de BCR's, zal de Chief Privacy Officer in samenspraak met de lokale juridisch adviseur en de lokale functionaris voor gegevensbescherming bepalen welke wettelijk passende actie ondernomen moet worden. Indien noodzakelijk, zal de Chief Privacy Officer ook overleg plegen met de relevante gegevensbeschermingsautoriteiten.

17 – Interne klachtmechanismen

Amgen zal haar bestaande proces van klachtenbehandeling uitbreiden met de behandeling van eventuele BCR-gerelateerde klachten of aandachtspunten.

Elke betrokkene kan te allen tijde een klacht indienen wanneer een deelnemend Bedrijf de BCR's niet naleeft. Deze klachten worden behandeld door het Privacy Office, onder toezicht van de Chief Privacy Officer en in samenwerking met de betreffende lokale functionaris voor de gegevensbescherming.

Amgen raadt aan om dergelijke klachten schriftelijk - per post of per e-mail - rechtstreeks aan het Privacy Office of aan het verbonden bedrijf te sturen. Betrokkene kunnen ook, zover de toepasselijke wetgeving dit toestaat, gebruikmaken van de Business Conduct Hotline om een BCR-gerelateerde klacht te melden.

Indien de klacht lokaal wordt ontvangen, zal de DPO de tekst indien nodig vertalen en zonder onnodige vertraging doorsturen naar het Privacy Office.

Eerst wordt aan de Betrokkene een bericht verzonden waarin staat dat zijn/haar klacht in behandeling is genomen, en dat hij binnen maximaal twee maanden een antwoord zal ontvangen.

Indien het Privacy Office constateert dat iemand een vergrijp heeft gepleegd, worden passende disciplinaire maatregelen genomen, waar nodig met inbegrip van onmiddellijke beëindiging van het dienstverband, voorzover dit is toegestaan door de toepasselijke wetgeving.

Binnen maximaal twee maanden ontvangt de betrokkene een antwoord waarin hij/zij wordt geïnformeerd over de afhandeling van de klacht.

De Betrokkene wordt ervan in kennis gesteld dat, als hij/zij niet tevreden is over het antwoord van Amgen, hij/zij een eis kan indienen bij de betreffende rechtbank of gegevensbeschermingsautoriteit.

Dit klachtenbehandelingsproces wordt openbaar gemaakt via publicatie van de BCR's, als vermeld in hoofdstuk 7.

18 – Derde begunstigde rechten en verplichtingen

Een betrokkene wiens persoonsgegevens afkomstig zijn uit een gereguleerd land en die beweert dat een van de verplichtingen waarnaar wordt verwezen in de BCR's is geschonden, heeft het recht de BCR's af te dwingen bij derde begunstigde. Deze rechten omvatten de beschikbare rechtsmiddelen wanneer zijn gewaarborgde rechten worden geschonden en het recht op schadevergoeding. Indien van toepassing, is de aansprakelijkheid beperkt tot de feitelijke geleden schade.

Vorzover toegestaan door het toepasselijk rechtssysteem, kunnen betrokkenen ervoor kiezen hun eis in te stellen:

- in het rechtsgebied van de gegevensexporteur; indien de persoonsgegevens van de betrokkene afkomstig zijn van een gegevensexporteur in de EER, wordt de competente jurisdictie gevormd door de plaats van vestiging van de gegevensexporteur in de EER, of
- bij de bevoegde gegevensbeschermingsautoriteiten.

Elke betrokkene die schade heeft geleden ten gevolge van een schending van de in de BCR's bedoelde verplichtingen door de gegevensexporteur of de gegevensimporteur heeft het recht om van de gegevensexporteur vergoeding van de geleden schade te verkrijgen. Indien de gegevensexporteur of de gegevensimporteur aansprakelijk wordt gesteld voor een schending, zal hij, voorzover deze aansprakelijk is, de andere partij schadeloosstellen voor de door die partij opgelopen kosten, lasten, schade, onkosten en verliezen.

Elke gegevensexporteur en gegevensimporteur kan worden ontheven van aansprakelijkheid uit hoofde van de BCR's indien hij aantoont dat het lid van de groep buiten de EU geen BCR's heeft geschonden of niet verantwoordelijk is voor de schade die aan de betrokkene is berokkend. De bewijslast blijft echter rusten op de gegevensexporteur en gegevensimporteur.

De gegevensimporteur die optreedt als gegevensverwerker kan zich niet beroepen op een schending door een onderverwerker van diens verplichtingen om zijn eigen aansprakelijkheid te ontlopen. Indien een betrokkene op grond van een schending van de BCR's een eis wil instellen tegen de gegevensexporteur, maar daartoe niet in staat is omdat de gegevensexporteur feitelijk is verdwenen of in juridische zin niet meer bestaat of failliet is verklaard, kan de betrokkene zijn rechten rechtstreeks tegen de gegevensimporteur doen gelden. Indien een rechtverkrijgende entiteit contractueel of van rechtswege alle wettelijke verplichtingen van de gegevensexporteur of gegevensimporteur heeft overgenomen, kan de betrokkene zijn rechten doen gelden tegen deze entiteit. De aansprakelijkheid van de gegevensimporteur is beperkt tot zijn eigen verwerkingsactiviteiten uit hoofde van de BCR's.

19 – Onderlinge medewerking en samenwerking met gegevensbeschermingsautoriteiten

Deelnemende bedrijven zijn verplicht samen te werken en elkaar medewerking te verlenen bij de behandeling van een verzoek of klacht van een betrokkene of bij een onderzoek of aanvraag door gIn samenwerking met de Chief Privacy Officer reageren deelnemende bedrijven binnen een gepaste termijn en op een gepaste wijze op BCR-gerelateerde verzoeken van een gegevensbeschermingsautoriteit en volgen ze de adviezen en beslissingen van de bevoegde gegevensbeschermingsautoriteit op met betrekking tot de tenuitvoerlegging van de BCR's.

20 – Bijwerken en wijzigen van BCR's

Amgen behoudt zich te allen tijde het recht voor deze BCR's te wijzigen en/of bij te werken. Bijwerking van de BCR's kan met name noodzakelijk zijn in geval van gewijzigde wettelijke verplichtingen, significante wijzigingen in de structuur van de Amgen-groep of officiële eisen opgelegd door de competente (relevante) gegevensbeschermingsautoriteiten.

Amgen meldt alle significante wijzigingen in de BCR's of in de lijst met deelnemende bedrijven aan alle andere deelnemende bedrijven en aan de gegevensbeschermingsautoriteiten, waarbij rekening wordt gehouden met veranderingen in de regelgeving en bedrijfsstructuur.

Voor sommige wijzigingen kan een nieuwe autorisatie van de gegevensbeschermingsautoriteiten noodzakelijk zijn.

De Chief Privacy Officer houdt een volledig bijgewerkte lijst bij van deelnemende Bedrijven aan de BCR's en van gereguleerde landen die mogelijk bescherming genieten uit hoofde van de BCR's, volgt alle wijzigingen in de BCR's en verstrekt op verzoek de noodzakelijke informatie aan de Betrokkenen of Gegevensbeschermingsautoriteiten.

Amgen verplicht zich ertoe dat er geen doorgifte aan een nieuw deelnemend bedrijf plaatsvindt uit hoofde van de garanties van de BCR's tot het moment dat het nieuwe deelnemend bedrijf daadwerkelijk gebonden is aan de BCR's en aan de BCR's voldoet.

Wijzigingen in de BCR's of in de lijst met deelnemende bedrijven worden één maal per jaar gemeld aan de gegevensbeschermingsautoriteiten die de autorisaties verlenen, met een korte toelichting betreffende de reden(en) voor de wijziging.

Substantiële wijzigingen in de BCR's worden ook aan de betrokkenen gecommuniceerd, waarbij gebruik wordt gemaakt van een communicatiemiddel als bedoeld in Artikel 7 van de BCR's.

21 – Relatie tussen nationale wetten en de BCR's

Wanneer de lokale wetgeving een hoger beschermingsniveau voor persoonsgegevens voorschrijft, dan geniet deze wetgeving voorrang boven de BCR's. Indien de toepasselijke lokale wetgeving een lager beschermingsniveau voor persoonsgegevens voorschrijft dan de BCR's, dan worden de BCR's toegepast.

Indien verplichtingen uit hoofde van de toepasselijke lokale wetgeving strijdig zijn met de BCR's, dient het deelnemend bedrijf de Chief Privacy Officer daar onverwijld van in kennis te stellen.

In elk geval moeten persoonsgegevens in overeenstemming met het toepasselijk recht worden verwerkt, als bepaald door Artikel 4 van Richtlijn 95/46/EG en de betreffende lokale wetgeving.