EU bindende bedrijfsvoorschriften van Amgen – Verwerkingsverantwoordelijke (EU BCR's)

Laatst bijgewerkt: 12 december 2023

Inleiding

(A) Amgen is een toonaangevend biotechnologisch bedrijf dat zich toelegt op het helpen van mensen bij het bestrijden van ernstige ziekten. De EU bindende bedrijfsvoorschriften van Amgen – Verwerkingsverantwoordelijke ('**EU BCR's**') vormen de uitdrukking van Amgen's streven naar adequate privacy- en gegevensbescherming bij de overdracht en verwerking van persoonsgegevens tussen Deelnemende bedrijven.

(B) Alle deelnemende bedrijven en al het personeel streven ernaar deze EU BCR's te respecteren en zijn er wettelijk aan gebonden met betrekking tot persoonsgegevens binnen het toepassingsgebied van de EU BCR's. Niet-naleving kan leiden tot disciplinaire sancties, voorzover toegestaan door lokale wetgeving. De Chief Compliance Officer zorgt er samen met de Chief Privacy Officer voor dat naleving van de EU BCR's wordt afgedwongen. Een lijst met Deelnemende bedrijven vindt u hier: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. Voor alle vragen over deze EU BCR's kunt u contact opnemen met alle Deelnemende bedrijven via privacy@amgen.com.

(C) Deze EU BCR's zijn vastgesteld in verwijzing naar de EU-wetgeving inzake gegevensbescherming. Amgen France is ervoor verantwoordelijk dat de deelnemende bedrijven deze EU BCR's naleven. Individuen kunnen deze EU BCR's afdwingen tegen Amgen France als derde begunstigde, zoals hieronder beschreven. Deze EU BCR's zijn beschikbaar op de website van Amgen: www.amgen.com/bcr. U kunt ook contact opnemen met Amgen via privacy@amgen.com om een kopie aan te vragen.

1. Toepassingsgebied

1.1. De EU BCR's van Amgen zijn van toepassing op de overdracht en verwerking, geautomatiseerd of handmatig, van alle persoonsgegevens van betrokkenen, uitgevoerd door een Deelnemend bedrijf dat opereert als verantwoordelijke voor gegevensverwerking of als gegevensverwerker voor een ander Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking in een van de volgende gevallen:

1.1.1. het Deelnemend bedrijf dat de persoonsgegevens verwerkt, is gevestigd in de EU; of

1.1.2. het Deelnemend bedrijf dat de persoonsgegevens verwerkt, is niet gevestigd in de EER en heeft de persoonsgegevens ontvangen van een Deelnemend bedrijf gevestigd in de EER; of

1.1.3. om persoonsgegevens over te dragen van Gegevensimporteurs naar Gegevensimporteurs.

1.2. Een overzicht van de gegevensstromen op grond van deze EU BCR's is beschikbaar in Bijlage 1.

2. Definities

Termen	*Definities*
Amgen France	Amgen S.A.S., een vennootschap opgericht in Frankrijk met statutaire zetel op 25 quai du Président Paul Doumer, 92400 Courbevoie.
Toepasselijke wetten	De wetgeving van de EU en/of (indien van toepassing) de nationale of lokale wetgeving van de EER-lidstaten (inclusief maar niet beperkt tot de EU-wetgeving inzake gegevensbescherming).
Hoofd Compliance	Een persoon binnen de Healthcare Compliance-divisie van de afdeling Worldwide Compliance and Business Ethics van een Deelnemend bedrijf die de verantwoordelijkheid voor gegevensbescherming en privacy heeft gedelegeerd en, waar verschillend van de lokale functionaris voor gegevensbescherming, de lokale functionaris voor gegevensbescherming ondersteunt met zijn verantwoordelijkheden en taken.
Toestemming	Elke vrijelijk gegeven specifieke, geïnformeerde en ondubbelzinnige indicatie van de wensen van een betrokkene, waarmee de betrokkene, door een verklaring of door een duidelijke bevestigende handeling, aangeeft in te stemmen met de verwerking van persoonsgegevens die op hem/haar betrekking hebben.
Verantwoordelijke voor gegevensverwerking	Elke entiteit die beslissingen neemt met betrekking tot het verzamelen en verwerken van persoonsgegevens, inclusief beslissingen over de doeleinden waarvoor, en de manier waarop, persoonsgegevens worden verwerkt.
Gegevensexporteur	Een deelnemend bedrijf dat opereert als verantwoordelijke voor gegevensverwerking, gevestigd in de EER, en dat persoonsgegevens overdraagt aan een gegevensimporteur.
Gegevensimporteur	Een Deelnemend bedrijf dat niet in de EER is gevestigd en dat (a) persoonsgegevens ontvangt van een gegevensexporteur of (b) een verdere overdracht van persoonsgegevens ontvangt overeenkomstig artikel 1(c) van deze EU BCR's.
Gegevensverwerker	Een natuurlijke persoon of entiteit die namens een verantwoordelijke voor gegevensverwerking persoonsgegvens verwerkt.
Gegevensbeschermingsautoriteit (Data Protection Authority, DPA)	Een onafhankelijke openbare gegevensbeschermingsautoriteit, opgericht door een EER-lidstaat.

Termen	*Definities*
Functionaris voor gegevensbescherming (Data Protection Officer, DPO)	Een persoon die door de Chief Privacy Officer van Amgen is benoemd als verantwoordelijke voor het toezicht op privacy en gegevensbescherming op lokaal niveau en voor de implementatie van passende en vereiste controles.
Betrokkene	Een natuurlijke persoon die direct of indirect kan worden geïdentificeerd aan de hand van persoonsgegevens. Een betrokkene kan zijn (zonder beperking): • een patiënt/persoon uit een klinische proef (mogelijk een kind jonger dan 18 jaar) • een gezondheidszorgprofessional • een werknemer • een verkoper of leverancier
EEA	De lidstaten van de Europese Unie (Oostenrijk, België, Bulgarije, Kroatië, Republiek Cyprus, Tsjechië, Denemarken, Estland, Finland, Frankrijk, Duitsland, Griekenland, Hongarije, Ierland, Italië, Letland, Litouwen, Luxemburg, Malta, Nederland, Polen, Portugal, Roemenië, Slowakije, Slovenië, Spanje en Zweden) en IJsland, Liechtenstein en Noorwegen (allemaal '**EER-lidstaten**').
EU-wetgeving inzake gegevensbescherming	De AVG en (indien van toepassing) de lokale of nationale wetgeving met betrekking tot gegevensbescherming en de verwerking van persoonsgegevens en de implementatie van de AVG van een relevante EER-lidstaat.
AVG	De Algemene Verordening Gegevensbescherming ((EU) 2016/679).
Deelnemend bedrijf	Een entiteit binnen de Amgen-groep die gebonden is aan de EU BCR's.

Termen	*Definities*
Persoonsgegevens	Alle informatie met betrekking tot een Betrokkene, zoals een naam, een identificatienummer, locatiegegevens, een online identificator betreffende een of meer factoren die specifiek zijn voor of informatie met betrekking tot de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van die natuurlijke persoon. Voorbeelden van persoonsgegevens kunnen het volgende zijn: • De naam, het adres, het burgerservicenummer, het nummer van het rijbewijs, informatie over bankrekeningen, over de gezinssamenstelling of medische gegevens van een betrokkene, • De naam, opleiding en het voorschrijfgedrag van een gezondheidszorgprofessional, • E-mailadres en andere identificerende gegevens die verstrekt worden door een bezoeker van een website van Amgen. Bovenstaande opsomming is slechts indicatief en is niet uitputtend.
Inbreuk op persoonsgegevens	Elke inbreuk op de beveiliging die leidt tot de accidentele of onrechtmatige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot verzonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Personeel	Alle personeelsleden en tijdelijke werknemers (inclusief consultants, uitzendkrachten en contractarbeiders) van elk Deelnemend bedrijf.
Verwerking	Elke handeling of reeks handelingen die wordt uitgevoerd op persoonsgegevens (of reeksen van Persoonsgegevens), al dan niet via geautomatiseerde middelen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, aanpassen of wijzigen, opvragen, raadplegen, gebruiken, openbaar maken door verzending, verspreiding of anderszins beschikbaar stellen, uitlijnen of combineren, beperken, wissen of vernietigen.
Gevoelige persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen of lidmaatschap van een vakbond blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over de gezondheid of gegevens over de seksualiteit of seksuele geaardheid van een natuurlijke persoon. Los van de EU-wetgeving inzake gegevensbescherming beschouwt Amgen ook financiële informatie en informatie die kan worden gebruikt om identiteitsdiefstal te plegen (bijv.

Termen	*Definities*
	burgerservicenummer, rijbewijsnummer, creditcard- of andere bankrekeninginformatie) als gevoelige persoonsgegevens.
Technische en organisatorische beveiligingsmaatregelen	Technologische en organisatorische maatregelen gericht 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.
Derde partij	Een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of enig ander lichaam anders dan de Betrokkene, waarbij het Deelnemend bedrijf optreedt als verantwoordelijke voor gegevensverwerking en een Deelnemend bedrijf optreedt als Gegevensverwerker. Bij Amgen wordt een leverancier beschouwd als een Derde partij. Afhankelijk van de omstandigheden kan een Derde partij optreden als verantwoordelijke voor gegevensverwerking of gegevensverwerker met betrekking tot de verwerking van persoonsgegevens.
Leverancier	Elke natuurlijke of rechtspersoon, bedrijf of organisatie die goederen en/of diensten levert aan een Deelnemend bedrijf op grond van een contractuele relatie en/of een ontvanger is van persoonsgegevens van een dergelijk Deelnemend bedrijf om die goederen en/of diensten te leveren.

Amgen zal de voorwaarden in deze EU BCR's interpreteren in overeenstemming met de EU-wetgeving inzake gegevensbescherming.

3. Beperking van de doeleinden

3.1. Persoonsgegevens worden verwerkt voor expliciete, gespecificeerde en legitieme doeleinden overeenkomstig Artikel 5(1)(b) van de AVG.

3.2. Persoonsgegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met de legitieme doeleinden waarvoor de Persoonsgegevens zijn verzameld met de toepasselijke wetgeving. Gegevensimporteurs zijn verplicht zich te houden aan de oorspronkelijke doeleinden bij het opslaan en/of verder verwerken van persoonsgegevens of het verwerken van persoonsgegevens die door een ander Deelnemend bedrijf aan hen zijn overgedragen. Het doel van de verwerking van persoonsgegevens mag alleen worden gewijzigd met toestemming van de Betrokkene of voor zover toegestaan door de toepasselijke wetgeving.

3.3. Gevoelige persoonsgegevens zullen worden voorzien van aanvullende waarborgen, zoals voorzien door de EU-wetgeving inzake gegevensbescherming.

4. Kwaliteit en evenredigheid van de gegevens

4.1. Persoonsgegevens moeten accuraat zijn en waar nodig actueel worden gehouden; alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat persoonsgegevens die onjuist zijn, gelet op de doeleinden waarvoor ze worden verwerkt, onverwijld worden gewist of gecorrigeerd.

4.2. Persoonsgegevens zijn adequaat, relevant en beperkt tot het strikt noodzakelijke met betrekking tot de doeleinden waarvoor ze worden verwerkt, overeenkomstig artikel 5(1)(c) van de AVG.

4.3. Verwerking van persoonsgegevens moet worden geleid door de doelstelling dat het verzamelen, verwerken en/of gebruiken van persoonsgegevens dient te 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.

4.4. 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

5.1. Verwerking van persoonsgegevens is slechts toegestaan indien voldaan is aan ten minste <u>één</u> van de volgende voorwaarden:

5.1.1. De Betrokkene heeft toestemming gegeven voor de verwerking van zijn of haar persoonsgegevens voor een of meer specifieke doeleinden.

5.1.2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waar de Betrokkene partij bij is of om op verzoek van de Betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

5.1.3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting waaraan de verantwoordelijke voor gegevensverwerking onderworpen is onder de toepasselijke wetgeving.

5.1.4. De verwerking is noodzakelijk om een vitaal belang van de Betrokkene of een andere natuurlijke persoon, zoals diens leven, gezondheid of veiligheid, veilig te stellen.

5.1.5. 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 verantwoordelijke voor gegevensverwerking.

5.1.6. De verwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke voor gegevensverwerking of van de Derde partij, mits dat belang minder zwaar weegt dan het gerechtvaardigde belang dat de Betrokkene heeft bij zijn of haar fundamentele rechten en vrijheden.

5.2. Verwerking van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten mag alleen worden uitgevoerd wanneer de verwerking is toegestaan door de toepasselijke wetgeving die voorziet in passende waarborgen voor de rechten en vrijheden van Betrokkenen.

6. Verwerking van gevoelige persoonsgegevens

6.1. Indien het Deelnemend bedrijf op grond van een specifiek en legitiem doel Gevoelige persoonsgegevens moet verwerken, zal het Deelnemend bedrijf dit alleen doen als:

6.1.1. De Betrokkene expliciete toestemming heeft gegeven voor de verwerking van die Gevoelige persoonsgegevens voor een of meer specifieke doeleinden, behalve wanneer de toepasselijke wetgeving bepaalt dat het verbod van Artikel 9(1) van de AVG niet door de Betrokkene mag worden opgeheven.

6.1.2. De verwerking is noodzakelijk voor het uitvoeren van de verplichtingen en specifieke rechten van de verantwoordelijke voor gegevensverwerking op het gebied van werkgelegenheid, sociale zekerheid en sociale bescherming, voor zover dit is toegestaan door de toepasselijke wetgeving of door een collectieve overeenkomst op grond van de toepasselijke wetgeving die passende waarborgen biedt voor de grondrechten en de belangen van de Betrokkene.

6.1.3. De verwerking is noodzakelijk ter bescherming van de vitale belangen van de Betrokkene of van een andere natuurlijke persoon indien deze lichamelijk of juridisch niet bekwaam is om toestemming te geven.

6.1.4. 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 buiten die instantie worden doorgegeven.

6.1.5. De verwerking heeft betrekking op gevoelige persoonsgegevens die kennelijk door de Betrokkene openbaar zijn gemaakt.

6.1.6. De verwerking van gevoelige persoonsgegevens is noodzakelijk voor de vaststelling, de uitoefening of de verdediging van rechtsvorderingen.

6.1.7. De verwerking is noodzakelijk om redenen van zwaarwegend openbaar belang, op basis van de toepasselijke wetgeving die in verhouding moet staan tot het nagestreefde doel, de essentie van het recht op gegevensbescherming moet respecteren en moet voorzien in passende en specifieke maatregelen om de grondrechten en de belangen te beschermen van de Betrokkene.

6.1.8. De verwerking van de gevoelige persoonsgegevens is vereist voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidscapaciteit van de werknemer, medische diagnose, het verlenen van gezondheidszorg of sociale zorg of behandeling of het beheer van gezondheidszorg- of sociale zorgstelsels en diensten op basis van de toepasselijke wetgeving of krachtens een

contract met een gezondheidszorgprofessional, en wanneer deze gevoelige persoonsgegevens worden verwerkt door of onder de verantwoordelijkheid van een gezondheidszorgprofessional moet deze professional onderworpen zijn aan de verplichting tot beroepsgeheim onder de toepasselijke wetgeving of toepasselijke regels vastgesteld door bevoegde instanties in een EER-lidstaat of door een andere persoon die ook onderworpen is aan een geheimhoudingsplicht krachtens het toepasselijke recht of regels vastgesteld door bevoegde instanties in een EER-lidstaat.

6.1.9. De verwerking van gevoelige persoonsgegevens is noodzakelijk om redenen van openbaar belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gezondheidsbedreigingen of het waarborgen van hoge normen voor de kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op basis van de toepasselijke wetgeving die voorziet in passende en specifieke maatregelen om de rechten en vrijheden van de Betrokkene te beschermen, in het bijzonder het beroepsgeheim.

6.1.10. De verwerking van gevoelige persoonsgegevens is noodzakelijk voor archiveringsdoeleinden in het algemeen belang, wetenschappelijke of historische onderzoeksdoeleinden of statistische doeleinden in overeenstemming met artikel 89(1) van de AVG op basis van de toepasselijke wetgeving, die evenredig is aan het nagestreefde doel en de essentie van het recht op gegevensbescherming en voorzien in passende en specifieke maatregelen om de grondrechten en de belangen van de Betrokkene te beschermen.

7. Transparantie en recht op informatie

7.1. Alle Deelnemende bedrijven dienen persoonsgegevens op transparante wijze te verwerken. Amgen verbindt zich ertoe om de EU BCR's, inclusief contactgegevens, vrij beschikbaar en gemakkelijk toegankelijk te stellen aan iedere Betrokkene en om Betrokkenen te informeren over de overdracht en verwerking van hun persoonsgegevens. Deze EU BCR's zijn beschikbaar op de website van Amgen: www.amgen.com/bcr. U kunt ook contact opnemen met Amgen via privacy@amgen.com om een kopie aan te vragen. Amgen zal ook verschillende communicatiemiddelen gebruiken, zoals bedrijfswebsites, inclusief interne websites en nieuwsbrieven, contracten en specifieke privacyverklaringen, om aan deze toegankelijkheidsvereiste te voldoen. Bovendien zal Amgen Betrokkenen, met behulp van deze communicatiemiddelen, zonder onnodige vertraging op de hoogte stellen van eventuele updates of wijzigingen in de EU BCR's of in de lijst van Deelnemende bedrijven.

7.2. Betrokkenen van wie de persoonsgegevens door een Deelnemend bedrijf worden Verwerkt, ontvangen de informatie zoals uiteengezet in Artikelen 13 en 14 van de AVG.

7.3. Wanneer de persoonsgegevens 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, rectificatie, uitwissing en beperking van gegevens

8.1. Elke Betrokkene heeft het recht om van het Deelnemend bedrijf bevestiging te krijgen over de vraag of persoonsgegevens die hem of haar betreffen al dan niet worden verwerkt, en, indien dat het geval is, toegang tot de persoonsgegevens en de informatie die moet worden

verstrekt op grond van artikel 15(1) van de AVG. 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.

8.2. Iedere Betrokkene heeft het recht op rectificatie, uitwissing of beperking van de persoonsgegevens, met name wanneer de gegevens onvolledig of onjuist zijn.

8.3. Elke Betrokkene heeft het recht om op elk moment, om redenen die verband houden met zijn of haar specifieke situatie, bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens op basis van de uitvoering van een taak die wordt uitgevoerd in het openbaar belang of de legitieme belangen van het Deelnemend bedrijf of een Derde partij (inclusief profilering op basis van die gronden). Het Deelnemend bedrijf zal de persoonsgegevens niet langer verwerken, tenzij het dwingende legitieme redenen voor de Verwerking aantoont die zwaarder wegen dan de belangen, rechten en vrijheden van de Betrokkene of voor het instellen, uitoefenen of verdedigen van rechtsvorderingen.

8.4. Elke Betrokkene heeft het recht om (kosteloos) bezwaar te maken tegen de verwerking van persoonsgegevens die op hem of haar betrekking hebben met het oog op direct marketing, inclusief profilering voor zover deze verband houdt met dergelijke direct marketing. Wanneer de Betrokkene zijn of haar recht uitoefent om bezwaar te maken tegen de verwerking van persoonsgegevens die hem of haar betreffen met het oog op direct marketing, moet het Deelnemend bedrijf de verwerking van de persoonsgegevens voor dat doeleinde staken.

8.5. Iedere Betrokkene heeft het recht op het verkrijgen van de kennisgeving van rectificatie, uitwissing of beperking aan Derden aan wie de gegevens zijn verstrekt, als bepaald in Artikel 19 van de AVG.

8.6. 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 13(2)(f) van de AVG.

8.7. Wanneer de verwerking gebaseerd is op toestemming, heeft iedere Betrokkene het recht om zijn of haar toestemming op elk moment in te trekken. Het intrekken van de toestemming heeft geen invloed op de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking ervan.

8.8. Elke Betrokkene heeft het recht om bij het Deelnemend bedrijf een klacht in te dienen over de verwerking van persoonsgegevens via het interne klachtenmechanisme dat is voorzien krachtens Artikel 17.

8.9. Alle verzoeken op grond van dit artikel 8 (of artikel 9 hieronder) moeten worden verzonden naar het Deelnemend bedrijf op: privacy@amgen.com. Hoewel het indienen van verzoeken per e-mail sterk wordt aangemoedigd, sluit dit niet uit dat een betrokkene een mondeling verzoek indient. Het Deelnemend bedrijf stelt de Betrokkene onverwijld op de hoogte van de uitkomst van zijn verzoek en uiterlijk binnen één maand na ontvangst van het verzoek (inclusief, indien van toepassing, de redenen om geen actie te ondernemen en de mogelijkheid om een klacht in te dienen bij de bevoegde gegevensbeschermingsautoriteit en/of het zoeken naar een rechtsmiddel). Deze periode van één maand kan indien nodig met twee maanden worden verlengd, rekening houdend met de complexiteit en het aantal verzoeken. Het Deelnemend bedrijf zal de betrokkene binnen een maand na ontvangst van het verzoek op de hoogte stellen van een dergelijke verlenging, samen met de redenen voor de vertraging. Elke communicatie, actie en/of informatie die wordt verstrekt met betrekking

tot een verzoek op grond van dit Artikel 8 (of Artikel 9 hieronder) wordt kosteloos aan de Betrokkene verstrekt. Wanneer verzoeken van een Betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, kan het Deelnemend bedrijf het volgende doen: (a) een redelijke vergoeding in rekening brengen, rekening houdend met de administratieve kosten voor het verstrekken van de informatie of communicatie of het ondernemen van de gevraagde actie; of (b) weigeren gevolg te geven aan het verzoek. Het Deelnemend bedrijf draagt de last om het kennelijk ongegronde of buitensporige karakter van het verzoek aan te tonen.

9. Geautomatiseerde individuele besluiten

9.1. De Betrokkene heeft het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, met inbegrip van profilering, gebaseerd besluit waaraan voor hem of haar rechtsgevolgen zijn verbonden of die hem of haar op soortgelijke wijze aanzienlijk treffen, tenzij dat besluit:

9.1.1. noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst tussen de Betrokkene en het Deelnemend bedrijf;

9.1.2. is vereist of geautoriseerd door de toepasselijke wetgeving, die ook passende maatregelen vastlegt om de rechten en vrijheden en legitieme belangen van de Betrokkene te beschermen (inclusief ten minste het recht op menselijke tussenkomst van de kant van het Deelnemend bedrijf, om zijn of haar standpunt kenbaar te maken en om de beslissing aan te vechten); of

9.1.3. is gebaseerd op de uitdrukkelijke toestemming van de Betrokkene.

10. Beveiliging en vertrouwelijkheid

10.1. Amgen implementeert passende technische en organisatorische beveiligingsmaatregelen om inbreuken op persoonsgegevens te voorkomen en te detecteren. Internationale raamwerken als ISO/IEC 27002 worden door Amgen gebruikt om deze beveiligingsmaatregelen vast te stellen.

10.2. Amgen hanteert processen om ervoor te zorgen dat inbreuken op persoonsgegevens onderworpen zijn aan rapportage, tracking en passende corrigerende maatregelen, indien nodig. Elke inbreuk op persoonsgegevens zal worden gedocumenteerd (inclusief de feiten met betrekking tot de inbreuk op persoonsgegevens, de gevolgen ervan en de ondernomen herstelmaatregelen) en de documentatie zal op verzoek ter beschikking worden gesteld aan de bevoegde gegevensbeschermingsautoriteit. Deelnemende bedrijven zullen elke inbreuk op persoonsgegevens zonder onnodige vertraging melden aan Amgen France, de Chief Privacy Officer en de overige relevante privacyfunctionaris/functie, en (indien het Deelnemend bedrijf dat te maken heeft met een inbreuk op persoonsgegevens optreedt als gegevensverwerker) aan het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking. Inbreuken op persoonsgegevens zullen, in samenwerking met de Chief Privacy Officer, zonder onnodige vertraging (en waar mogelijk uiterlijk 72 uur nadat zij zich bewust zijn geworden van de inbreuk op persoonsgegevens) worden gemeld aan de bevoegde gegevensbeschermingsautoriteit, tenzij het onwaarschijnlijk is dat deze inbreuk zal resulteren in een risico voor de rechten en vrijheden van betrokkenen. Wanneer de inbreuk op persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van Betrokkenen, wordt deze ook zonder onnodige vertraging aan de Betrokkenen gemeld.

10.3. 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.

10.4. Bij de tenuitvoerlegging van de maatregelen wordt rekening gehouden met de stand van de techniek, als bedoeld in Artikel 32 van de AVG.

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

10.6. De technische en organisatorische beveiligingsmaatregelen zullen worden ontworpen om de gegevensbeschermingsbeginselen uit hoofde van artikel 5 van de AVG, de gegevensbescherming en de standaardbeginselen overeenkomstig artikel 25 van de AVG te implementeren en om de naleving van de vereisten van deze EU BCR's in de praktijk te vergemakkelijken.

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

11.1. Het Deelnemend bedrijf (dat optreedt als verantwoordelijke voor gegevensverwerking) zal zorgvuldig een gegevensverwerker kiezen die een ander Deelnemend bedrijf of een leverancier kan zijn. De gegevensverwerker dient voldoende waarborgen te bieden ten aanzien van zijn technische en organisatorische beveiligingsmaatregelen met betrekking tot de uit te voeren verwerking en zorg te dragen voor de naleving van die maatregelen.

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

11.3. Het Deelnemend bedrijf dat als verantwoordelijke voor gegevensverwerking optreedt, zal, met gebruikmaking van schriftelijke contractuele middelen, in overeenstemming met de toepasselijke wetgeving (en in het bijzonder de vereisten van artikel 28(3) van de AVG) de gegevensverwerker onder meer de volgende instructies geven:

11.3.1. de gegevensverwerker zal alleen handelen op instructie van het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking en de verwerking van persoonsgegevens is verboden voor de eigen doeleinden van de gegevensverwerker of voor de doeleinden van een Derde;

11.3.2. over de regels met betrekking tot de veiligheid en vertrouwelijkheid die op de gegevensverwerker moeten rusten en om passende technische en organisatorische maatregelen te implementeren om een beveiligingsniveau te garanderen dat passend is voor het risico van de verwerking;

11.3.3. personen die bevoegd zijn om de persoonsgegevens te verwerken, hebben zich tot geheimhouding verplicht of vallen onder een passende wettelijke geheimhoudingsplicht;

11.3.4. de gegevensverwerker zal geen andere gegevensverwerker inhuren zonder de voorafgaande specifieke of algemene schriftelijke toestemming van het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking

en, indien een dergelijke toestemming wordt gegeven, zullen dezelfde gegevensbeschermingsverplichtingen als uiteengezet in het contract of een andere rechtshandeling tussen het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking en de gegevensverwerker worden opgelegd aan die andere gegevensverwerker;

11.3.5. rekening houdend met de aard van de verwerking moet deze, voor zover mogelijk, het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking bijstaan door middel van passende technische en organisatorische maatregelen om te voldoen aan de verplichting van het Deelnemend bedrijf om te reageren op verzoeken om de rechten van de Betrokkene uit te oefenen;

11.3.6. deze moet het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking assisteren bij het waarborgen van de naleving van de verplichtingen met betrekking tot de veiligheid van de verwerking, het melden van een inbreuk op persoonsgegevens aan de bevoegde DPA, het communiceren van een inbreuk op persoonsgegevens aan de betrokkene, beoordelingen van de impact op gegevensbescherming en voorafgaande overleg met de bevoegde gegevensbeschermingsautoriteit, rekening houdend met de aard van de verwerking en de informatie waarover de gegevensverwerker beschikt;

11.3.7. naar keuze van het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking, moet het alle persoonsgegevens verwijderen of terugsturen naar het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking na het einde van de dienstverlening met betrekking tot de verwerking, en bestaande kopieën verwijderen, tenzij de EU-wetgeving inzake gegevensbescherming opslag vereist van de persoonsgegevens;

11.3.8. deze moet het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking alle informatie ter beschikking stellen die nodig is om de naleving van de verplichtingen vastgelegd in dit Artikel 11 aan te tonen, en moet ervoor zorgen dat audits, inclusief inspecties, die worden uitgevoerd door het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking of een andere door haar gemachtigde auditor mogelijk worden gemaakt en moet hieraan een bijdrage leveren.

11.4. Het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking zorgt ervoor dat de gegevensverwerker volledig blijft voldoen aan de overeengekomen technische en organisatorische beveiligingsmaatregelen.

11.5. Het Deelnemend bedrijf dat als verantwoordelijke voor gegevensverwerking optreedt, behoudt de verantwoordelijkheid voor de legitimiteit van de verwerking en is nog steeds aansprakelijk voor de rechten van de Betrokkene. Voor zover de gegevensverwerker onderworpen is aan de EU-wetgeving inzake gegevensbescherming, is hij ook aansprakelijk voor zijn verplichtingen en verantwoordelijkheden als gegevensverwerker onder dergelijke wetten.

11.6. Om te voldoen aan de contractuele verplichtingen uiteengezet in dit artikel over gegevensverwerkers, wordt een contractueel model met de naam Gegevensprivacyschema verstrekt voor gebruik door Deelnemende bedrijven die optreden als verantwoordelijke voor

gegevensverwerking. Het Deelnemend bedrijf dat als verantwoordelijke voor gegevensverwerking optreedt, kan, afhankelijk van de specifieke omstandigheden van elke contractuele regeling, onderhandelen over andere bepalingen dan die uiteengezet in het Gegevensprivacyschema, maar de contractuele bepalingen moeten nog steeds minimaal de verplichtingen dekken die hierboven zijn uiteengezet in dit Artikel 11.

11.7. Elk Deelnemend bedrijf dat optreedt als gegevensverwerker en onderworpen is aan de EU-wetgeving inzake gegevensbescherming moet een register bijhouden van alle categorieën van verwerkingsactiviteiten die worden uitgevoerd namens een Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking. Dit dossier moet schriftelijk en in elektronische vorm worden bijgehouden, moet op verzoek beschikbaar worden gesteld aan de Chief Privacy Officer en de bevoegde gegevensbeschermingsautoriteit en moet de volgende informatie bevatten: (a) de naam en contactgegevens van het Deelnemend bedrijf dat optreedt als gegevensverwerker en van elk Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking namens wie het optreedt, en, indien van toepassing, zijn vertegenwoordiger en DPO; (b) de categorieën van verwerkingen die worden uitgevoerd namens elk Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking; en (c) indien van toepassing, overdrachten van persoonsgegevens aan een derde land of een internationale organisatie, inclusief de identificatie van dat derde land of die internationale organisatie en, in het geval van overdrachten die afhankelijk zijn van een afwijking op grond van artikel 49 van de AVG, documentatie van de passende waarborgen; en (d) waar mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

12. Beperkingen op overdracht en verdere overdracht

12.1. Bij alle overdrachten van persoonsgegevens die onderworpen zijn aan deze EU BCR's aan Derde partijen die zich buiten de EER bevinden, zullen de EU-wetgeving inzake gegevensbescherming inzake overdracht en verdere overdracht van persoonsgegevens worden gerespecteerd, hetzij door gebruik te maken van de standaardcontractbepalingen die zijn toegestaan onder het Uitvoeringsbesluit (EU) van de Commissie van 4 juni 2021 betreffende modelcontractbepalingen voor de overdracht van persoonsgegevens naar derde landen overeenkomstig de AVG of op een andere adequate manier overeenkomstig hoofdstuk V van de AVG (inclusief, bij wijze van uitzondering, als een afwijking van toepassing is op een specifieke situatie in overeenstemming met artikel 49 van de AVG).

12.2. Bij alle overdrachten van persoonsgegevens waarop deze EU BCR's van toepassing zijn naar gegevensverwerkers die zich buiten de EER bevinden, wordt de EU-wetgeving inzake gegevensbescherming met betrekking tot gegevensverwerkers gerespecteerd (en de vereisten uiteengezet in Artikel 11 hierboven), naast de regels over overdrachten en verdere overdrachten van persoonsgegevens zoals uiteengezet in dit Artikel 12 en in de EU-wetgeving inzake gegevensbescherming.

12.3. Voordat persoonsgegevens worden overgedragen aan een gegevensimporteur of (met betrekking tot verdere overdrachten) voordat een bijgewerkte lokale nationale wet van kracht wordt, zal de Gegevensexporteur, in samenwerking met de Chief Privacy Officer en Amgen France, met de hulp van de Gegevensimporteur en rekening houdend met de omstandigheden van de overdracht, evalueren of de lokale nationale wetgeving de gegevensimporteur ervan zal weerhouden zijn verplichtingen onder de EU BCR's na te komen en bepalen of eventuele vereiste aanvullende maatregelen moeten worden geïmplementeerd. Bij een dergelijke beoordeling wordt rekening gehouden met:

12.3.1. de specifieke omstandigheden van de overdracht (inclusief de doeleinden waarvoor de persoonsgegevens worden overgedragen en verwerkt, de soorten entiteiten die betrokken zijn bij de verwerking, de economische sector waarin de overdracht plaatsvindt, de categorieën en het formaat van de overgedragen persoonsgegevens, de locatie van de verwerking (inclusief opslag) en de gebruikte transmissiekanalen);

12.3.2. de wetten en praktijken van het derde land van bestemming die relevant zijn in het licht van de specifieke omstandigheden van de overdracht (inclusief de wetten en praktijken die de openbaarmaking van gegevens aan overheidsinstanties vereisen of toegang verlenen aan dergelijke autoriteiten) en de toepasselijke beperkingen en waarborgen; en

12.3.3. alle relevante contractuele, technische of organisatorische waarborgen die zijn getroffen met betrekking tot de overdracht, inclusief maatregelen die worden toegepast tijdens de overdracht en op de verwerking van de persoonsgegevens in het land van bestemming.

Bovendien moet een dergelijke beoordeling gebaseerd zijn op het inzicht dat de wetten en praktijken van het derde land van bestemming de fundamentele rechten en vrijheden van de Betrokkene respecteren en niet verder gaan dan wat in een democratische samenleving noodzakelijk en proportioneel is voor het waarborgen van een van de volgende doelstellingen: (a) nationale veiligheid; (b) defensie; (c) openbare veiligheid; (d) het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten of het uitvoeren van strafrechtelijke sancties, met inbegrip van de bescherming tegen en het voorkomen van bedreigingen voor de openbare veiligheid; e) andere belangrijke doelstellingen van algemeen openbaar belang, in het bijzonder belangrijke economische of financiële belangen, waaronder monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid; f) de bescherming van de rechterlijke onafhankelijkheid en gerechtelijke procedures; (g) het voorkomen, onderzoeken, opsporen en vervolgen van schendingen van de ethiek voor gereglementeerde beroepen; h) monitoring-, inspectie- of regelgevende functies die verband houden met de uitoefening van het openbaar gezag in de gevallen bedoeld in de voorgaande doelstellingen; (i) de bescherming van de Betrokkene of de rechten en vrijheden van anderen; en/of (j) het afdwingen van civielrechtelijke claims.

De Chief Privacy Officer zal de gedocumenteerde beoordeling en eventuele voorgestelde aanvullende maatregelen beoordelen en goedkeuren. Indien uit de uitkomst van de beoordeling blijkt dat er aanvullende maatregelen moeten worden genomen, zal de Gegevensexporteur deze maatregelen implementeren. Indien er geen aanvullende maatregelen kunnen worden genomen (of indien geïnstrueerd door de Chief Privacy Officer of een bevoegde DPA), zal de Gegevensexporteur de overdracht opschorten. Het resultaat van de beoordeling en de voorgestelde aanvullende maatregelen worden geregistreerd en indien nodig aan de bevoegde gegevensbeschermingsautoriteit verstrekt.

De Chief Privacy Officer en Amgen France zullen alle deelnemende bedrijven op de hoogte stellen van de uitgevoerde beoordeling en van de resultaten ervan, zodat de geïdentificeerde aanvullende maatregelen kunnen worden toegepast wanneer hetzelfde soort overdrachten worden uitgevoerd door andere Deelnemende bedrijven of, wanneer effectieve aanvullende maatregelen niet kunnen worden ingevoerd, dergelijke overdrachten opgeschort of beëindigd worden.

12.4. De gegevensimporteur zal de gegevensexporteur, Amgen France en de Chief Privacy Officer onmiddellijk op de hoogte stellen als hij redenen heeft om aan te nemen dat hij onderworpen is of is geworden aan wetten of praktijken die hem ervan zouden weerhouden zijn verplichtingen onder deze EU BCR's na te komen, inclusief na een wijziging in de nationale wetgeving in het derde land zoals beschreven in artikel 12.3 of een maatregel zoals een verzoek tot openbaarmaking zoals beschreven in artikel 16.3. Bovendien zullen de gegevensexporteurs (in samenwerking met de Chief Privacy Officer) voortdurend en waar nodig met de hulp van de gegevensimporteurs toezicht houden op de ontwikkelingen in de derde landen waarnaar de gegevensexporteurs persoonsgegevens hebben overgedragen die mogelijk een negatieve invloed hebben op de initiële beoordeling van het beschermingsniveau van persoonsgegevens en de beslissingen die met betrekking tot dergelijke overdrachten worden genomen.

12.5. Na een opschorting van een overdracht moet de gegevensexporteur de overdracht of een reeks overdrachten beëindigen als de gegevensimporteur niet in staat is te voldoen aan de EU BCR's en/of de naleving niet binnen één maand na de opschorting is hersteld. In dat geval moet de gegevensimporteur, naar keuze van de gegevensexporteur, alle persoonsgegevens die vóór de opschorting zijn overgedragen, en eventuele kopieën daarvan, retourneren of vernietigen.

12.6. Stromen van persoonsgegevens die niet onder deze EU BCR's vallen en/of niet afkomstig zijn van een Deelnemend bedrijf gevestigd in een EER-lidstaat, worden niet beschouwd als een overdracht van persoonsgegevens onder deze EU BCR's en zijn dienovereenkomstig niet onderworpen aan de vereisten van deze EU BCR's.

13. Trainingsprogramma

13.1. Zoals beschreven in Bijlage 2 biedt Amgen passende en actuele training over privacybeginselen en meer specifiek over de EU BCR's aan al het personeel. Deze training omvat ook informatie over de gevolgen op grond van het strafrecht en het arbeidsrecht en/of hun dienstverleningsovereenkomst voor personeel dat de EU BCR's overtreedt.

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

13.3. Specifieke cursussen worden per geval gegeven aan personeel dat doorlopend of regelmatig toegang heeft tot persoonsgegevens, of dat betrokken is bij het verzamelen van persoonsgegevens of bij het ontwikkelen van hulpmiddelen die gebruikt worden voor de verwerking van persoonsgegevens.

13.4. Daarnaast biedt het Global Privacy Compliance Team van Amgen passende informatie en bronnen met betrekking tot privacy, onder meer op het intranetportaal van Amgen.

14. Audit- en monitoringprogramma

14.1. De Chief Privacy Officer zorgt ervoor dat alle Deelnemende bedrijven (en hun naleving van deze EU BCR's) worden opgenomen in het audit- en monitoringprogramma vanuit het perspectief van privacy en gegevensbescherming. Er worden regelmatig uitgebreide audits uitgevoerd, niet minder vaak dan elke 2 tot 3 jaar (voor Deelnemende bedrijven met een gemiddeld tot hoog risicoprofiel op basis van de risicobeoordelingsmethodologie van de auditafdeling) en elke 4 tot 5 jaar (voor Deelnemende bedrijven met een laag risicoprofiel op basis van de risicobeoordelingsmethodologie van de auditafdeling), door het interne

auditteam of onafhankelijke, extern gecertificeerde auditors. Uitgebreide audits omvatten gegevensbescherming en privacyzaken die binnen hun toepassingsgebied vallen (inclusief de naleving van deze EU BCR's, indien van toepassing op en gebruikt door een Deelnemend bedrijf). Naast de uitgebreide audits, en zonder afbreuk te doen aan de hierboven uiteengezette tijdsbestekken, worden er ook andere audits uitgevoerd, waaronder cross-functionele of probleemspecifieke audits (bijv. de naleving van de EU BCR's), een beperkte audit van één of meer systemen voor de verwerking van persoonsgegevens en/of een beperkte audit van een of meer functionele afdelingen (bijv. het Global Privacy Compliance Team). Het auditprogramma wordt in overleg ontwikkeld en overeengekomen door de Chief Audit Executive en de Chief Compliance Officer, die een Senior Vice-President is. De Chief Privacy Officer, de Chief Compliance Officer en de Chief Information Officer kunnen te allen tijde het initiatief nemen tot ad hoc EU-gerelateerde audits. Bijvoorbeeld als reactie op een vastgesteld nalevingsprobleem of een melding van inhoudelijke niet-naleving, een inbreuk op persoonsgegevens en/of een inhoudelijke wijziging in de EU-wetgeving inzake gegevensbescherming. Het auditprogramma bestrijkt alle aspecten van de EU BCR's, inclusief methoden om te waarborgen dat corrigerende maatregelen worden genomen..

14.2. Alle EU BCR-auditrapporten worden tijdig gecommuniceerd aan de Chief Compliance Officer en aan de Chief Privacy Officer. De auditsamenvattingen en bevindingen van de EU BCR's, evenals andere relevante informatie, worden ook regelmatig gerapporteerd aan de Raad van Bestuur van Amgen Inc. via geschikte commissies (bijv. de Corporate Responsibility and Compliance Committee en/of de Audit Committee of the Board), aan de raad van bestuur van Amgen France en (indien van toepassing, bijvoorbeeld in verband met een bevinding die een oplossing vereist) aan het relevante Deelnemende bedrijf. Het Corporate Responsibility and Compliance Committee van de Raad van Bestuur van Amgen, Inc. komt vijf keer per jaar samen. Privacy- en gegevensbescherming wordt jaarlijks besproken, meestal tijdens de vergadering in oktober.

14.3. De bevoegde DPA kan op verzoek een kopie ontvangen van de EU BCR-gerelateerde auditrapporten.

14.4. Elk Deelnemend bedrijf zal samenwerken met en zal aanvaarden om, zonder beperkingen, te worden gecontroleerd door de bevoegde DPA. Elke gecontroleerde entiteit moet de Chief Privacy Officer onmiddellijk op de hoogte stellen als zij op de hoogte wordt gesteld van een dergelijke audit of als er een dergelijke audit plaatsvindt.

15. Naleving en toezicht op naleving

15.1. Amgen benoemt het juiste personeel, inclusief waar van toepassing een netwerk van functionarissen voor gegevensbescherming, met ondersteuning van het topmanagement om toezicht te houden op de naleving van de regels voor gegevensbescherming en deze naleving te garanderen. De Chief Privacy Officer heeft de leiding over het Global Privacy Compliance Team, een mondiaal team dat wereldwijd deskundige ondersteuning biedt aan Amgen-entiteiten (inclusief Deelnemende bedrijven).

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

15.2.1. advisering van de directie;

15.2.2. het waarborgen van de naleving van de gegevensbescherming op mondiaal niveau (inclusief het dragen van de algehele verantwoordelijkheid voor de EU BCR's);

15.2.3. het regelmatig rapporteren over de naleving van gegevensbescherming (inclusief aan de Chief Compliance Officer); en

15.2.4. het meewerken aan de onderzoeken van de bevoegde DPA.

15.3. Het Global Privacy Compliance Team bestaat uit de Chief Privacy Officer (die, naast de hierboven genoemde verantwoordelijkheden, toezicht houdt op het wereldwijde netwerk van functionarissen voor gegevensbescherming), de Europese functionaris voor gegevensbescherming en andere lokale functionarissen voor gegevensbescherming. Het Global Privacy Compliance Team heeft bij Amgen de algehele verantwoordelijkheid voor gegevensbescherming en privacynaleving wereldwijd.

15.4. De Europese functionaris voor gegevensbescherming is door Amgen aangesteld als functionaris voor gegevensbescherming voor de EER, het Verenigd Koninkrijk en Zwitserland. De Europese functionaris voor gegevensbescherming voert de taken uit die zijn vastgelegd in Artikel 39 van de AVG. Amgen zal ervoor zorgen dat de taken en plichten van de Europese functionaris voor gegevensbescherming niet resulteren in een belangenconflict bij dergelijke taken. De Europese functionaris voor gegevensbescherming heeft een directe rapportagelijn met de Chief Privacy Officer (die deel uitmaakt van het hoogste managementniveau voor Amgen) en wordt ondersteund door het lokale Hoofd Compliance in Frankrijk. De Europese functionaris voor gegevensbescherming kan contact opnemen met de Chief Privacy Officer als er vragen of problemen rijzen tijdens de uitvoering van zijn taken. U kunt contact opnemen met de Europese functionaris voor gegevensbescherming op: privacy@amgen.com

15.5. Op lokaal niveau zijn functionarissen voor gegevensbescherming verantwoordelijk voor het behandelen van lokale privacyverzoeken van Betrokkenen, voor het waarborgen van naleving op lokaal niveau met ondersteuning van de Global Privacy Compliance Team, en voor het melden van belangrijke privacykwesties aan de Chief Privacy Officer. Amgen onderhoudt een netwerk van functionarissen voor gegevensbescherming en zorgt ervoor dat er een DPO wordt aangesteld of toegewezen voor elk land waar Amgen een bedrijfsentiteit heeft (het Deelnemend bedrijf) en de toepasselijke wetgeving van het rechtsgebied van een dergelijk Deelnemend bedrijf een dergelijke benoeming vereist.

15.6. Normaal gesproken zijn de functionarissen voor gegevensbescherming de lokale Hoofden Compliance, die rapporteren aan de afdeling Worldwide Compliance and Business Ethics, of worden ze erdoor ondersteund. Het Global Privacy Compliance Team maakt deel uit van en rapporteert aan de afdeling Worldwide Compliance and Business Ethics, die wordt geleid door de Chief Compliance Officer. De Chief Compliance Officer heeft de algehele verantwoordelijkheid voor de naleving van de wet- en regelgeving door de Amgen-groep wereldwijd. In zeldzame gevallen kan de functionaris voor gegevensbescherming, vanwege de specifieke omstandigheden van een Deelnemend bedrijf of andere bijzondere omstandigheden, afkomstig zijn uit een andere functie, bijvoorbeeld Regulatory. In ieder geval zorgt het Global Privacy Compliance Team ervoor dat de functionarissen voor gegevensbescherming en Hoofden Compliance op de juiste manier zijn opgeleid en over voldoende management en expertise beschikken om hun rol te vervullen. Bovendien hebben de functionarissen voor gegevensbescherming een directe rapportagelijn naar de Chief Privacy Officer en worden ze ondersteund door het Global Privacy Compliance Team Personnel voor het geval ze aanvullende begeleiding nodig hebben.

15.7. Elk Deelnemend bedrijf dat als verantwoordelijke voor gegevensverwerking optreedt, is verantwoordelijk voor en kan de naleving van de EU BCR's aantonen. Als onderdeel van deze vereiste moeten alle Deelnemende bedrijven:

15.7.1. een register bijhouden van alle categorieën van verwerkingsactiviteiten die zijn uitgevoerd in overeenstemming met de vereisten zoals uiteengezet in artikel 30(1) van de AVG. Dit dossier moet schriftelijk en in elektronische vorm worden bijgehouden, moet op verzoek beschikbaar worden gesteld aan de Chief Privacy Officer en de bevoegde gegevensbeschermingsautoriteit en moet de volgende informatie bevatten: (a) de naam en contactgegevens van het Deelnemend bedrijf dat optreedt als verantwoordelijke voor gegevensverwerking, zijn vertegenwoordiger en DPO; (b) de doeleinden van de verwerking; (c) een beschrijving van de categorieën Betrokkenen en van de categorieën persoonsgegevens; (d) de categorieën ontvangers aan wie de persoonsgegevens zijn of zullen worden bekendgemaakt, inclusief ontvangers in derde landen of internationale organisaties; (e) indien van toepassing, overdrachten van persoonsgegevens aan een derde land of een internationale organisatie, inclusief de identificatie van dat derde land of die internationale organisatie en, in het geval van overdrachten die afhankelijk zijn van een afwijking, documentatie van de passende waarborgen; (f) waar mogelijk, de beoogde termijnen voor het wissen van de verschillende categorieën persoonsgegevens; en (g) waar mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

15.7.2. privacyeffectbeoordelingen uitvoeren voor verwerkingsactiviteiten die waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengen, in overeenstemming met Artikel 35 van de AVG. Wanneer uit een privacyeffectbeoordeling op grond van Artikel 35 blijkt dat de verwerking een hoog risico met zich mee zou brengen bij gebrek aan maatregelen die door het Deelnemend bedrijf zijn genomen om het risico te beperken, moet vóór de verwerking de Chief Privacy Officer worden geraadpleegd, die vervolgens zal overleggen met de bevoegde DPA overeenkomstig Artikel 36 van de AVG.

16. Acties wanneer nationale wetgeving naleving van EU BCR's tegenhoudt

16.1. Wanneer een Deelnemend bedrijf reden heeft om aan te nemen dat de op hem van toepassing zijnde wetten het Deelnemend bedrijf beletten zijn verplichtingen onder de EU BCR's na te komen of een substantieel effect hebben op de garanties die door de regels worden geboden, zal het de Chief Privacy Officer (behalve wanneer verboden door een wetshandhavingsinstantie, zoals een strafrechtelijk verbod om de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren) en Amgen France hiervan onmiddellijk op de hoogte stellen.

16.2. Wanneer er sprake is van strijdigheid tussen de nationale wetgeving en de verplichtingen in de EU 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 nodig overlegt de Chief Privacy Officer ook met de bevoegde DPA.

16.3. Wanneer een wettelijke vereiste waaraan een Deelnemend bedrijf in een derde land onderworpen is waarschijnlijk een substantieel nadelig effect zal hebben op de garanties die worden geboden door de EU BCR's, zullen de Chief Privacy Officer, Amgen France, en de gegevensexporteur onmiddellijk op de hoogte worden gesteld door de gegevensimporteur, en de Chief Privacy Officer zal de bevoegde gegevensbeschermingsautoriteit en (waar mogelijk) de Betrokkenen hiervan op de hoogte stellen. Dit omvat (a) elk juridisch bindend

verzoek om openbaarmaking van de persoonsgegevens door een wetshandhavingsautoriteit of staatsveiligheidsinstantie, en in een dergelijk geval moet de bevoegde gegevensbeschermingsautoriteit duidelijk worden geïnformeerd over het verzoek, inclusief informatie over de gevraagde gegevens, de verzoekende instantie, en de wettelijke basis voor de openbaarmaking en het gegeven antwoord (tenzij anderszins verboden, zoals een strafrechtelijk verbod om de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren), en (b) eventuele directe toegang van overheidsinstanties tot persoonsgegevens overgedragen op grond van deze EU BCR's in overeenstemming met de wetten van het land van bestemming, en in dat geval zal een dergelijke kennisgeving alle informatie bevatten waarover het Deelnemend bedrijf beschikt (tenzij anderszins verboden, zoals een strafrechtelijk verbod om de vertrouwelijkheid van een politieonderzoek).

16.4. Indien in specifieke gevallen de opschorting en/of kennisgeving verboden is, zal het Deelnemende bedrijf dat het verzoek ontvangt zijn uiterste best doen om het recht te verkrijgen om van dit verbod af te zien, teneinde zo veel mogelijk informatie zo snel mogelijk te communiceren en te kunnen communiceren om aan te tonen (op verzoek van de gegevensexporteur) dat hij dit heeft gedaan.

16.5. De gegevensimporteur zal de gegevensexporteur op gezette tijden voorzien van zoveel mogelijk relevante informatie over de ontvangen verzoeken (in het bijzonder het aantal verzoeken, het soort gevraagde persoonsgegevens, de identiteit van de verzoekende autoriteiten, of verzoeken al dan niet zijn aangevochten en de uitkomst van dergelijke aangevochten verzoeken). De gegevensimporteur bewaart dergelijke informatie zolang de persoonsgegevens onderworpen zijn aan de waarborgen geboden door de EU BCR's en zal deze op verzoek beschikbaar stellen aan de bevoegde DPA. Als het de gegevensimporteur geheel of gedeeltelijk verboden is de bovengenoemde informatie aan de gegevensexporteur te verstrekken, zal de gegevensimporteur de gegevensexporteur daarvan zonder onnodige vertraging op de hoogte stellen.

16.6. De gegevensimporteur zal, in samenwerking met de Chief Privacy Officer, de wettigheid van een verzoek om openbaarmaking door een overheidsinstantie beoordelen om te bepalen of dit binnen de bevoegdheden valt die aan de verzoekende overheidsinstantie zijn verleend. De gegevensimporteur zal het verzoek betwisten als hij na een dergelijke beoordeling tot de conclusie komt (in samenwerking met de Chief Privacy Officer) dat er redelijke gronden zijn om aan te nemen dat het verzoek onwettig is volgens de wetten van het land van bestemming, toepasselijke verplichtingen onder internationaal recht en/of principes van internationale gastvrijheid. Als de gegevensimporteur van mening is dat er redelijke gronden zijn om het verzoek als onwettig te beschouwen, zal hij de mogelijkheden tot beroep nastreven. Wanneer de gegevensimporteur een verzoek betwist, zal hij om voorlopige maatregelen verzoeken om de gevolgen van het verzoek op te schorten totdat de bevoegde rechterlijke instantie over de gegrondheid ervan heeft beslist. De gegevensimporteur zal de gevraagde persoonsgegevens niet openbaar maken totdat hij daartoe verplicht is op grond van de toepasselijke wetgeving en procedureregels van het land van bestemming. De gegevensimporteur zal zijn juridische beoordeling en eventuele betwisting van het verzoek om openbaarmaking documenteren en, voor zover toegestaan volgens de wetten van het land van bestemming, de documentatie beschikbaar stellen aan de gegevensexporteur en, op verzoek, aan de bevoegde DPA.

16.7. De gegevensimporteur zal de minimaal toegestane hoeveelheid informatie verstrekken bij het reageren op een verzoek om openbaarmaking, op basis van een redelijke interpretatie van het verzoek.

16.8. In ieder geval zullen de overdrachten van persoonsgegevens door een Deelnemend bedrijf aan een overheidsinstantie niet massaal, onevenredig en willekeurig zijn op een manier die verder gaat dan wat noodzakelijk is in een democratische samenleving.

16.9. Voor Deelnemende bedrijven in de EER kan elk vonnis van een rechtbank of tribunaal en elk besluit van een administratieve autoriteit van een derde land dat een verantwoordelijke voor gegevensverwerking of gegevensverwerker verplicht om persoonsgegevens over te dragen of openbaar te maken, enkel worden erkend of afgedwongen als dit is gebaseerd op een internationale overeenkomst, zoals een verdrag voor wederzijdse rechtshulp, die van kracht is tussen het verzoekende derde land en de EU of een EER-lidstaat, onverminderd andere gronden voor overdracht op grond van Hoofdstuk V van de AVG.

17. Interne klachtmechanismen

17.1. Amgen zal haar bestaande klachtenbehandelingsproces gebruiken om de behandeling van eventuele klachten of zorgen in verband met de EU BCR's op te nemen.

17.2. Elke Betrokkene kan te allen tijde een klacht indienen wanneer een Deelnemend bedrijf de EU BCR's niet naleeft. Deze klachten worden behandeld door het Global Privacy Compliance Team, onder toezicht van de Chief Privacy Officer en in samenwerking met de betreffende lokale functionaris voor gegevensbescherming.

17.3. Amgen raadt aan dergelijke klachten schriftelijk per post of rechtstreeks per e-mail aan het Global Privacy Compliance Team of aan het Deelnemend bedrijf te melden. U kunt contact opnemen met het Global Privacy Compliance Team via de onderstaande contactgegevens:

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

E-mail: privacy@amgen.com

17.4. Het personeel van Amgen kan, indien aanvaardbaar volgens de wetten die van toepassing zijn op het Deelnemend bedrijf, de Business Conduct Hotline gebruiken om een EU BCR-klacht te melden.

17.5. Als de klacht lokaal door het Deelnemende bedrijf wordt ontvangen, zal de DPO indien nodig een vertaling maken en deze zonder onnodige vertraging doorsturen naar het Global Privacy Compliance Team.

17.6. Er zal binnen tien (10) werkdagen een eerste reactie aan de Betrokkene worden verstrekt, waarin deze wordt geïnformeerd dat zijn of haar klacht in behandeling is en dat hij of zij zonder onnodige vertraging een inhoudelijk antwoord zal ontvangen, en in ieder geval binnen één maand na ontvangst van het verzoek. Rekening houdend met de complexiteit en het aantal verzoeken, kan de termijn van één maand met maximaal twee maanden worden verlengd, in welk geval de Betrokkene hiervan op de hoogte wordt gesteld. Het inhoudelijke antwoord omvat details over onze bevindingen en eventuele maatregelen die Amgen heeft of voorstelt om te nemen. Als Amgen bepaalt dat er geen actie moet worden ondernomen, zal dit aan de Betrokkene worden uitgelegd, samen met de redenen voor deze vaststelling.

17.7. Als de klacht door Amgen wordt aanvaard, zal Amgen passende herstelmaatregelen treffen. Deze maatregelen zullen geval per geval worden beslist door de Chief Privacy Officer en het Global Privacy Compliance Team, de lokale DPO en, indien van toepassing, elke andere relevante afdeling. Bovendien zullen, als het Global Privacy Compliance Team individueel

wangedrag ontdekt, passende disciplinaire maatregelen worden genomen, tot en met beëindiging van het dienstverband of de opdracht, voor zover toegestaan door de toepasselijke wetgeving.

17.8. De Betrokkene ontvangt een antwoord waarin hij/zij wordt geïnformeerd over de uitkomst van zijn/haar klacht. Dit zal zonder onnodige vertraging gebeuren en in ieder geval binnen één maand na ontvangst van de klacht (met voldoende details zodat Amgen de aard van de klacht kan identificeren en, alleen indien redelijkerwijs noodzakelijk, met alle gevraagde informatie om de identiteit van de klager te bevestigen). Rekening houdend met de complexiteit en het aantal verzoeken, kan de termijn van één maand met maximaal twee maanden worden verlengd, in welk geval de Betrokkene hiervan op de hoogte wordt gesteld.

17.9. De Betrokkene wordt geïnformeerd dat als hij/zij niet tevreden is met het antwoord van Amgen, hij/zij een claim kan indienen bij de rechtbanken van een EER-lidstaat of bij de bevoegde gegevensbeschermingsautoriteit. Het is echter geen vereiste dat een Betrokkene eerst het klachtenbehandelingsproces van Amgen doorloopt voordat hij of zij een klacht kan indienen bij de bevoegde gegevensbeschermingsautoriteit of een claim kan indienen bij de rechtbanken van een EER-lidstaat.

17.10. Dit klachtenbehandelingsproces zal openbaar worden gemaakt door de publicatie van de EU BCR's zoals vermeld in artikel 7 hierboven.

18. Rechten van derde-begunstigden en aansprakelijkheid

18.1. Een Betrokkene wiens persoonsgegevens afkomstig zijn uit de EER of worden beschermd door de EU-wetgeving inzake gegevensbescherming en worden overgedragen aan Deelnemende bedrijven buiten de EER heeft het recht om de EU BCR's af te dwingen als derde-begunstigde en heeft het recht tot het verzoeken van gerechtelijk verhaal, het verkrijgen van rechtsmiddelen en, indien van toepassing, compensatie voor daadwerkelijke schade die is geleden als gevolg van de schending van deze EU BCR's. Dergelijke claims kunnen door de Betrokkene worden ingediend bij een bevoegde DPA (dit kan de DPA zijn in de EER-lidstaat waar de Betrokkene gewoonlijk verblijft, of de DPA van zijn/haar werkplek of de DPA van de plaats van de vermeende inbreuk). Betrokkenen kunnen ook een claim instellen bij een bevoegde rechtbank in een EER-lidstaat (dit kunnen de rechtbanken zijn van de EER-lidstaat waar het betreffende Deelnemend bedrijf een vestiging heeft of de rechtbanken van de EER-lidstaat waar de Betrokkene zijn/haar gewone verblijfplaats heeft). Een Betrokkene kan bij de uitoefening van zijn recht op een effectief rechtsmiddel tegen een Deelnemend bedrijf worden vertegenwoordigd door een non-profitorganisatie, organisatie of vereniging, op voorwaarde dat deze instantie, organisatie of vereniging op de juiste manier is opgericht in overeenstemming met de toepasselijke wetgeving, wettelijke doelstellingen heeft die van algemeen belang zijn en actief is op het gebied van de bescherming van de rechten en vrijheden van Betrokkenen met betrekking tot de bescherming van zijn persoonsgegevens. De Betrokkene kan als derde-begunstigde de volgende Artikelen afdwingen:

18.1.1. Artikelen 1 (Toepassingsgebied), 2 (Definities), 3 (Doelbeperking), 4 (Gegevenskwaliteit en evenredigheid), 5 (Rechtsgrondslag voor de verwerking van persoonsgegevens) en 6 (Verwerking van gevoelige persoonsgegevens);

18.1.2. Artikel 7 (Transparantie en informatierechten);

18.1.3. Artikelen 8 (Rechten op toegang, rectificatie, verwijdering en beperking van gegevens) en 9 (Geautomatiseerde individuele beslissingen);

18.1.4. Artikel 10 (Veiligheid en vertrouwelijkheid), 11 (Relaties met gegevensverwerkers (gegevensimporteur of leverancier van Amgen) en 12 (Beperking van overdrachten en verdere overdrachten);

18.1.5. Artikelen 16 (Acties in geval van nationale wetgeving die de naleving van de EU BCR's verhindert) en 21 (Relatie tussen nationale wetten en de EU BCR's);

18.1.6. Artikel 18 (Rechten van derde-begunstigden en aansprakelijkheid); en

18.1.7. Artikel 19 (Wederzijdse bijstand en samenwerking met de gegevensbeschermingsautoriteiten).

18.2. Om twijfel te voorkomen: de rechten van derde begunstigden strekken zich niet uit tot de Artikelen en elementen van deze EU BCR's die betrekking hebben op interne mechanismen die zijn geïmplementeerd binnen Deelnemende bedrijven of de Amgen-groep, zoals details met betrekking tot training (inclusief Bijlage 2), auditprogramma's, interne nalevingsnetwerken en -structuur en het mechanisme voor het bijwerken van de EU BCR's.

18.3. Amgen France aanvaardt de verantwoordelijkheid voor en stemt ermee in om de maatregelen te nemen die redelijkerwijs noodzakelijk zijn om de daden van Deelnemende bedrijven die buiten de EER gevestigd zijn te verhelpen. Amgen France zal compensatie betalen voor alle materiële of immateriële schade die voortvloeit uit de overtreding van deze EU BCR's, tenzij zij kan aantonen dat het Deelnemend bedrijf dat buiten de EER is gevestigd niet verantwoordelijk is voor de gebeurtenis die aanleiding geeft tot de schade. Amgen France beschikt over voldoende financiële middelen en verzekeringsdekking om schade te dekken onder de EU BCR's.

18.4. Elke Betrokkene die schade heeft geleden als gevolg van een schending van deze EU BCR's door een Deelnemend bedrijf dat niet in de EER is gevestigd, heeft, indien van toepassing, recht op compensatie van Amgen France, de rechtbanken of andere bevoegde autoriteiten in de EER voor de geleden schade. De Betrokkene heeft de rechten en rechtsmiddelen tegen Amgen France alsof de overtreding is veroorzaakt door Amgen France in de EU in plaats van door het Deelnemende bedrijf dat niet in de EER is gevestigd. Als het Deelnemende bedrijf dat niet in de EER is gevestigd verantwoordelijk of aansprakelijk wordt gehouden voor een dergelijke schending, zal het, voor zover het verantwoordelijk of aansprakelijk is, Amgen France schadeloos stellen voor alle kosten, heffingen, schade, uitgaven of verliezen die Amgen France oploopt in verband met een dergelijke schending.

18.5. In het geval van een claim van een Betrokkene dat hij/zij schade heeft geleden en heeft vastgesteld dat het waarschijnlijk is dat dergelijke schade is ontstaan als gevolg van een schending van deze EU BCR's, zal de bewijslast bij Amgen France berusten om aan te tonen dat de door de Betrokkene geleden schade als gevolg van een schending van deze EU BCR's niet kan worden toegeschreven aan het betreffende Deelnemende bedrijf. Als Amgen France kan aantonen dat het Deelnemende bedrijf dat buiten de EER is gevestigd, niet verantwoordelijk is voor de gebeurtenis die de schade veroorzaakt, is het niet aansprakelijk of verantwoordelijk voor de schade.

19. Wederzijdse bijstand en samenwerking met de gegevensbeschermingsautoriteiten

19.1. Deelnemende bedrijven zullen samenwerken en elkaar bijstaan bij het afhandelen van een verzoek of klacht van een Betrokkene of een onderzoek of aanvraag door de bevoegde DPA.

19.2. Deelnemende bedrijven zullen, in samenwerking met de Chief Privacy Officer, EU BCR-gerelateerde verzoeken van de bevoegde DPA binnen een passend tijdsbestek beantwoorden, rekening houdend met de omstandigheden van het verzoek (en in ieder geval niet later dan de door de bevoegde DPA opgelegde termijn) en met de nodige details op basis van de informatie die redelijkerwijs beschikbaar is voor het Deelnemende bedrijf. Met betrekking tot de implementatie en voortdurende toepassing van de EU BCR's zullen Deelnemende bedrijven de nodige aandacht besteden aan de mededelingen en aanbevelingen van de bevoegde DPA en zullen zij voldoen aan alle formele beslissingen of kennisgevingen van de bevoegde DPA.

19.3. Elk geschil dat verband houdt met de uitoefening door een bevoegde DPA van toezicht op de naleving van deze EU BCR's zal worden beslecht door de rechtbanken van de lidstaat van die DPA, in overeenstemming met de toepasselijke wetgeving van die lidstaat.

20. Bijwerken en wijzigen van EU BCR's

20.1. Amgen behoudt zich te allen tijde het recht voor deze EU BCR's te wijzigen en/of bij te werken. Bijwerking van de EU 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 DPA.

20.2. Amgen zal eventuele significante wijzigingen in de EU BCR's of in de lijst van Deelnemende bedrijven onmiddellijk en zonder onnodige vertraging melden aan alle andere Deelnemende bedrijven en aan de bevoegde gegevensbeschermingsautoriteit om rekening te houden met wijzigingen in de toepasselijke wetgeving, het regelgevingsklimaat en/of de structuur van de Amgen-groep. In het bijzonder wanneer een wijziging van invloed zou zijn op het beschermingsniveau dat wordt geboden door de EU BCR's, zal de Chief Privacy Officer een dergelijke wijziging onmiddellijk vooraf aan de bevoegde gegevensbeschermingsautoriteit doorgeven, met een korte uitleg van de redenen voor de wijziging. Voor sommige wijzigingen is mogelijk een nieuwe goedkeuring van de bevoegde DPA vereist.

20.3. De Chief Privacy Officer zal een volledig bijgewerkte lijst bijhouden van de Deelnemende bedrijven aan de EU BCR's, eventuele updates van de regels volgen en op verzoek de nodige informatie verstrekken aan de betrokkenen of de bevoegde gegevensbeschermingsautoriteit. Eventuele administratieve wijzigingen in de EU BCR's zullen regelmatig aan de Deelnemende bedrijven worden gerapporteerd.

20.4. Er vindt geen overdracht van persoonsgegevens plaats aan een nieuw Deelnemend bedrijf onder de garanties van de EU BCR's totdat het nieuwe Deelnemende bedrijf effectief gebonden is aan de EU BCR's en in overeenstemming is met de EU BCR's.

20.5. Eventuele administratieve wijzigingen aan de EU BCR’s of aan de lijst van Deelnemende bedrijven zullen op regelmatige basis worden gerapporteerd aan de Deelnemende bedrijven en minstens één keer per jaar aan de bevoegde gegevensbeschermingsautoriteit, met een korte uitleg over de redenen voor de update.

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

21. Relatie tussen nationale wetten en de EU BCR's

21.1. Wanneer de lokale nationale wetgeving die van toepassing is op een Deelnemend bedrijf een hoger beschermingsniveau voor Persoonsgegevens vereist, heeft dit voorrang op de EU BCR's. Als de lokale nationale wetten die van toepassing zijn op een Deelnemend bedrijf een lager beschermingsniveau voor persoonsgegevens bieden dan de EU BCR's, zullen de EU BCR's worden toegepast.

21.2. In het geval dat verplichtingen die voortkomen uit de lokale nationale wetgeving die van toepassing is op een Deelnemend bedrijf in strijd zijn met de EU BCR's, zal het Deelnemende bedrijf de Chief Privacy Officer hiervan zonder onnodige vertraging op de hoogte stellen en voldoen aan de aanvullende vereisten zoals uiteengezet in Artikel 16 hierboven.

21.3. In ieder geval zullen persoonsgegevens worden verwerkt in overeenstemming met Artikel 5 van de AVG en de relevante lokale wetgeving.

22. Slotbepalingen

22.1. De EU BCR's worden van kracht na goedkeuring door de bevoegde DPA en zijn van toepassing op de Deelnemende bedrijven bij ondertekening van de Adoptieovereenkomst van de EU BCR's.

22.2. Er zal geen overdracht plaatsvinden aan een Deelnemend bedrijf, tenzij het gebonden is aan deze EU BCR's. Wanneer een gegevensimporteur niet langer gebonden is aan de EU BCR's, moet hij alle persoonsgegevens (inclusief kopieën daarvan) die zijn overgedragen onder deze EU BCR's onmiddellijk teruggeven of verwijderen, behalve op voorwaarde dat de gegevensimporteur wettelijk bindende verplichtingen biedt om de bescherming van de Persoonsgegevens te behouden in overeenstemming met Hoofdstuk V van de AVG, waarbij deze Persoonsgegevens kan bewaren die zijn overgedragen onder deze EU BCR's.

22.3. De gegevensimporteur moet de gegevensexporteur, Amgen France en de Chief Privacy Officer onmiddellijk op de hoogte stellen als hij om welke reden dan ook niet in staat is om aan deze EU BCR's te voldoen (inclusief de situaties beschreven in Artikel 12.3 hierboven). Wanneer de Gegevensimporteur deze EU BCR's schendt, of niet in staat is deze na te leven, moet de Gegevensexporteur de Chief Privacy Officer hiervan op de hoogte stellen en de overdracht van persoonsgegevens opschorten.

22.4. Naar keuze van de gegevensexporteur moet de gegevensimporteur alle persoonsgegevens (inclusief kopieën daarvan) die zijn overgedragen onder deze EU BCR's onmiddellijk teruggeven of verwijderen, en dit aan de gegevensexporteur certificeren, waarbij:

22.4.1. de Gegevensexporteur de overdracht van persoonsgegevens heeft opgeschort en de naleving van deze EU BCR's niet binnen een redelijke termijn, en in ieder geval binnen één maand na de opschorting, wordt hersteld; of

22.4.2. de gegevensimporteur een wezenlijke inbreuk pleegt op deze EU BCR's; of

22.4.3. de gegevensimporteur verzuimt te voldoen aan een bindende beslissing van een bevoegde rechtbank of bevoegde gegevensbeschermingsautoriteit met betrekking tot zijn verplichtingen onder deze EU BCR's.

Totdat de persoonsgegevens zijn verwijderd of geretourneerd, moet de gegevensimporteur de naleving van deze EU BCR's blijven garanderen. Als de lokale nationale wetgeving die van toepassing is op de gegevensimporteur de teruggave of verwijdering verbiedt van de persoonsgegevens die zijn overgedragen onder deze EU BCR's, moet de gegevensimporteur de naleving van deze EU BCR's blijven garanderen en de persoonsgegevens alleen verwerken voor zover en zolang als vereist onder dergelijke lokale nationale wetten.

23. Bijlagen

De bijgevoegde bijlagen maken integraal deel uit van de EU BCR's.

Bijlage 1: Overzicht van Amgen-gegevensstromen

Bijlage 2: Overzicht van het Amgen-trainingsprogramma

Bijlage 1: Overzicht van Amgen-gegevensstromen

Betrokkenen	Gegevenscategorieën	Doelen	Overdracht
Werknemer	Identificatiegegevens zoals naam, adres, geboortedatum en -plaats, wervingsdatum, burgerservicenummers, creditcardnummers, bankrekening- en financiële informatie, en rijbewijs- en door de overheid uitgegeven identiteitskaartnummers Vakanties en voordelen, klachten, bonussen, promoties, beoordelingen en evaluaties, werkgegevens, informatie met betrekking tot gezondheids- en welzijnsdekking, pensioenplannen en details over aandelenopties Fiscale en financiële persoonsgegevens Gevoelige gegevens zoals nationale afkomst, indien toegestaan door de lokale wetgeving	Personeelsbeheer, informatietechnologieondersteuning en administratieve doeleinden in verband met de arbeidsrelatie en arbeidsvoorwaarden, of het beheer van vergoedingen na uitdiensttreding, en om te voldoen aan de wettelijke, administratieve en zakelijke verplichtingen van Amgen	De wereldwijde databases van Amgen bevinden zich in de VS, waar het hoofdkantoor van Amgen Inc. is gevestigd. Gegevensstromen worden overgedragen van Amgen France (of de relevante gegevensexporteur) naar Amgen Inc. in de Verenigde Staten of naar Deelnemende bedrijven in Zwitserland. Vervolgens kunnen de gegevens: - daar eenvoudigweg worden opgeslagen en onderhouden - worden geanalyseerd om mondiale statistieken en rapporten te verkrijgen - binnen de Amgen-groep verder worden gedeeld met andere Deelnemende bedrijven waar er een zakelijke behoefte bestaat aan dergelijke toegang door specifiek personeel of zakelijke functies bij die Deelnemende bedrijven (bijv.: een werknemer die solliciteert naar een baan buiten zijn land of die
Gezondheidszorgprofessionals	Naam, zakelijke contactgegevens inclusief telefoonnummer en e-mailadres, vakgebied Professionele achtergrond (cv) Deelname aan ander onderzoek Financiële informatie (facturerings- en betalingsinformatie)	Administratie en beheer van de professionele en wetenschappelijke activiteiten van Amgen – Onderzoek en ontwikkeling (bijvoorbeeld deelname aan medisch onderzoek, klinische onderzoeken, professionele bijeenkomsten of congressen) Promotie van de producten en diensten van Amgen Openbaarmaking van financiële informatie wanneer dit vereist is door de toepasselijke wetgeving of het naleven van de branchecode Naleving van de regelgeving, zoals veiligheidsmonitoring en rapportage van	

		bijwerkingen	moet rapporteren aan een manager buiten zijn land). In de meeste gevallen zullen dergelijke Deelnemende bedrijven optreden als verantwoordelijken voor gegevensverwerking, maar afhankelijk van de zakelijke behoefte kunnen deelnemende bedrijven ook optreden als gegevensverwerkers (bijv. bij het bieden van IT-helpdeskondersteuning of het bieden van ondersteuning met betrekking tot het HR Connect-servicecentrum).
Verkopers/leveranciers	Individuele naam, naam van de organisatie, zakelijke contactgegevens Facturerings- en betalingsinformatie	Verwerken van betalingen aan verkopers en leveranciers Naleving van regelgeving, zoals de belastingwetgeving	
Betrokkenen bij klinische onderzoeken (waaronder mogelijk kinderen jonger dan 18 jaar waarbij een pediatrische patiënt betrokken is bij een door Amgen gesponsord klinisch onderzoek).	Gecodeerde gegevens – de naam en contactgegevens van de patiënt worden vervangen door een intern gegenereerd identificatienummer. Alleen de klinische onderzoekslocatie (ziekenhuis/onderzoekslocatie) houdt de lijst bij om het identificatienummer aan de naam van de patiënt te koppelen. Indirecte identificatiegegevens zoals geboortejaar of -datum (de volledige geboortedatum wordt alleen verzameld voor onderzoeken bij kinderen), geslacht, gewicht en lengte. Gezondheidsgegevens die noodzakelijk zijn zoals beschreven in het onderzoeksprotocol. Andere gegevens met betrekking tot de patiënt die nodig zijn voor de uitvoering van het onderzoek, waaronder etniciteit, gezinssituatie (zoals aantal kinderen), gebruik van drugs, alcohol, middelen, algemene gewoonten of gedragingen, professionele situatie zoals werk,	Administratie en beheer van biomedisch onderzoek (klinische proeven, observatoriumstudies)	

	werkloosheid, deelname aan ander onderzoek.		
Patiënten (waaronder mogelijk kinderen jonger dan 18 jaar waarbij er een bijwerking optreedt bij het gebruik van een Amgen-product met een pediatrische indicatie).	Indirecte identificatiegegevens van de patiënt, zoals leeftijd, geboortejaar of geboortedatum, initialen van de patiënt (zoals toegestaan door de lokale wetgeving), geslacht, gewicht/lengte of identificatienummer van de patiënt (exclusief nationale gezondheidsidentificatiegegevens). Gegevens met betrekking tot de identificatie van het Amgen-product, zoals het gebruikte product of apparaat, serienummers van apparaten, leveringsmethode of dosering van het product, lot-/batchnummers van het product. Gezondheidsgegevens, waaronder toegediende behandelingen, resultaten van onderzoeken, aard van eventuele bijwerkingen, persoonlijke of familiale medische geschiedenis, daarmee samenhangende ziekten of gebeurtenissen, risicofactoren, informatie met betrekking tot het voorschrijven en gebruiken van medicijnen en het therapeutische gedrag van de gezondheidsprofessionals die betrokken zijn bij de behandeling van de ziekte van de patiënt. Andere gegevens met betrekking tot de patiënt die nodig zijn voor de beoordeling van de nadelige gezondheidsgebeurtenis in overeenstemming met wettelijke nalevingsverplichtingen zoals etniciteit, beroepsleven, consumptie van drugs, alcohol, middelen en/of algemene gewoonten of gedragingen.	Naleving van regelgeving en geneesmiddelenbewaking, zoals veiligheidsmonitoring en rapportage van bijwerkingen (indien toegestaan door de lokale wetgeving)	

Bijlage 2: Overzicht van het Amgen-trainingsprogramma

Privacy- en gegevensbeschermingstrainingsprogramma

Het Privacy- en gegevensbeschermingstrainingsprogramma streeft ernaar ervoor te zorgen dat al het Amgen-personeel goed is opgeleid met betrekking tot de EU BCR's van Amgen en alle wettelijke verplichtingen die van invloed zijn op de verwerking van persoonsgegevens. Dit programma bevat verschillende elementen.

Algemene training voor al het Amgen-personeel

Al het Amgen-personeel moet jaarlijks een online training over gegevensbescherming uitvoeren als onderdeel van de gedragscodetraining. Deze training is verplicht, wordt gecontroleerd en duurt doorgaans ongeveer 75 minuten. Deze training omvat de EU BCR's en informatie over de gevolgen op grond van het strafrecht en arbeidsrecht en/of hun dienstverleningsovereenkomst voor personeel dat de EU BCR's overtreedt.

Specifieke training voor DPO's

Alle DPO's van Amgen worden regelmatig getraind in nieuwe processen via regelmatige DPO-oproepen door het Global Privacy Compliance Team en privacyworkshops ter plaatse en/of online op een 'need-to-know'-basis. Alle DPO's hebben toegang tot een wikipagina die de meest gestelde vragen beantwoordt en begeleiding biedt, evenals links naar externe bronnen.

Specifieke opleiding voor personeel

Specifieke training kan worden gegeven op een 'need-to-know'-basis, online of op locatie, of door informatie op het Amgen-intranet te plaatsen. Deze training kan gericht zijn op specifieke groepen die dagelijks persoonsgegevens verwerken of andere groepen ondersteunen die persoonsgegevens verwerken. Zo worden de auditgroep, R&D-functies en de juridische afdeling regelmatig getraind. Dit omvat informatie over procedures voor het beheren van verzoeken om toegang tot persoonsgegevens door overheidsinstanties, indien relevant voor specifiek personeel. Deze training kan zowel op regionaal niveau als op landelijk niveau plaatsvinden. Er kunnen verdere specifieke EU BCR-trainingen worden ontwikkeld op een 'need-to-know'-basis.

Bewustzijn

Amgen heeft een speciale pagina op haar intranet over privacy en gegevensbescherming met links naar andere bronnen, zowel intern als extern.

Het Global Privacy Compliance Team van Amgen werkt samen met de afdeling Informatiebeveiliging aan het Sentinel-programma, een wereldwijd programma om het bewustzijn van Amgen-personeel op het gebied van informatiebeveiliging te vergroten.

Ondersteuning van trainingen

Alle privacygerelateerde trainingen zijn ontwikkeld door het Global Privacy Compliance Team en goedgekeurd door de Chief Privacy Officer. De training kan rechtstreeks worden gegeven door een lid van het Global Privacy Compliance Team of door een lokale DPO volgens een 'train the trainer'-model.