



## Amgens bindande EU-företagsbestämmelser – personuppgiftsansvarig (EU-BCR)

Uppdaterades senast: 12 december 2023

### Inledning

- (A) Amgen är ett ledande bioteknikföretag som hjälper patienter med svår sjukdom. I dessa bindande EU-företagsbestämmelser – personuppgiftsansvarig ("EU-BCR") uttrycks Amgens åtagande för integritets- och dataskydd då det syftar till att tillhandahålla adekvat skydd för överföringar och behandling av personuppgifter mellan deltagande företag.
- (B) Alla deltagande företag och all personal har åtagit sig att respektera, och är juridiskt bundna av, dessa EU-BCR med avseende på personuppgifter inom EU-BCR-tillämpningsområdet. Bristande efterlevnad kan leda till disciplinära sanktioner, enligt vad som tillåts enligt lokal lag. Den efterlevnadsansvarige i samarbete med den integritetsansvarige försäkrar att EU-BCR genomdrivs. En förteckning över deltagande företag finns här: <https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf>. Alla deltagande företag kan kontaktas på [privacy@amgen.com](mailto:privacy@amgen.com) angående frågor om dessa EU-BCR.
- (C) Dessa EU-BCR har antagits med hänvisning till EU:s dataskyddslagstiftning. Amgen France ansvarar för att säkerställa att de deltagande företagen följer dessa EU-BCR. Personer kan genomdriva dessa EU-BCR gentemot Amgen France som en tredjepartsmottagare enligt beskrivningen nedan. Dessa EU-BCR finns på Amgens webbplats [www.amgen.com/bcr](http://www.amgen.com/bcr). Du kan även begära ett exemplar genom att kontakta Amgen på [privacy@amgen.com](mailto:privacy@amgen.com).

### 1. Tillämpningsområde

- 1.1. Amgens EU-BCR gäller för överföringar och behandling, automatiserad eller manuell, av alla personuppgifter om registrerade som utförs av ett deltagande företag som agerar personuppgiftsansvarig eller agerar personuppgiftsbiträde för ett annat deltagande företag som agerar personuppgiftsansvarig i något av följande fall:
  - 1.1.1. Det deltagande företag som behandlar personuppgifter är etablerat i EU.
  - 1.1.2. Det deltagande företag som behandlar personuppgifter är inte etablerat i EES och har mottagit personuppgifter från ett deltagande företag som är etablerat i EES.
  - 1.1.3. För vidare överföringar av personuppgifter från uppgiftsinförare till uppgiftsinförare.
- 1.2. En översikt av dataflödena i enlighet med dessa EU-BCR finns i bilaga 1.

## 2. Definitioner

<b>Villkor</b>	<b>Definitioner</b>
<b>Amgen France</b>	Amgen S.A.S., ett företag bildat i Frankrike med registrerat säte på 25 quai du Président Paul Doumer, 92400 Courbevoie.
<b>Gällande lagstiftning</b>	EU:s lagar eller (i tillämpliga fall) den nationella eller lokala lagstiftningen i EES-medlemsstaterna (inklusive men inte begränsat till EU:s dataskyddslagstiftning).
<b>Efterlevnadschef</b>	En person på divisionen för hälso- och sjukvårdsefterlevnad på avdelningen för global efterlevnad och affärsetik på ett deltagande företag som har delegerat ansvaret för dataskydd och -integritet och, om det är en annan person än det lokala dataskyddsombudet, hjälper det lokala dataskyddsombudet med dess ansvar och uppgifter.
<b>Samtycke</b>	En fritt given specifik, informerad och otvetydig indikation på en registrerads önskemål, genom vilket den registrerade, genom ett uttalande eller genom en tydlig jakande åtgärd, anger samtycke till behandling av personuppgifter som rör honom eller henne.
<b>Personuppgiftsansvarig</b>	En enhet som fattar beslut om insamling och behandling av personuppgifter, inbegripet beslut om ändamålet med behandlingen av personuppgifter och hur behandlingen går till.
<b>Uppgiftsutförare</b>	Ett deltagande företag som agerar personuppgiftsansvarig, är etablerat i EES och överför personuppgifter till en uppgiftsinförare.
<b>Uppgiftsinförare</b>	Ett deltagande företag som inte är etablerat i EES som antingen (a) tar emot personuppgifter från en uppgiftsutförare eller (b) tar emot en vidare överföring av personuppgifter i enlighet med artikel 1(c) i dessa EU-BCR.
<b>Personuppgiftsbiträde</b>	En person eller enhet som behandlar personuppgifter på uppdrag av en personuppgiftsansvarig.
<b>Dataskyddsmyndighet</b>	En oberoende offentlig dataskyddsmyndighet som har inrättats av en EES-medlemsstat.
<b>Dataskyddsombud</b>	En person som har nominerats av Amgens integritetsansvarige till ansvarig för tillsyn av integritets- och dataskydd på lokal nivå samt implementering av lämpliga och nödvändiga kontroller.
<b>Registrerad</b>	En fysisk person som kan identifieras, direkt eller indirekt, genom hänvisning till personuppgifter. En registrerad kan (utan begränsning) vara <ul style="list-style-type: none"><li>• en patient/försöksperson i en klinisk prövning (vilket kan innefatta ett barn under 18 år)</li><li>• en vårdpersonal</li></ul>

<b>Villkor</b>	<b>Definitioner</b>
	<ul style="list-style-type: none"> <li>• en anställd</li> <li>• en säljare eller leverantör.</li> </ul>
<b>EES</b>	Medlemsländerna i Europeiska unionen (Österrike, Belgien, Bulgarien, Kroatien, Cypern, Tjeckien, Danmark, Estland, Finland, Frankrike, Tyskland, Grekland, Ungern, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Nederländerna, Polen, Portugal, Rumänien, Slovakien, Slovenien, Spanien och Sverige) samt Island, Liechtenstein och Norge (varav alla är "EES-medlemsstater").
<b>EU:s dataskyddslagstiftning</b>	GDPR och (i tillämpliga fall) lokal eller nationell lagstiftning som rör dataskydd och behandling av personuppgifter och genomförande av GDPR i en relevant EES-medlemsstat.
<b>GDPR</b>	Den allmänna dataskyddsförordningen ((EU) 2016/679).
<b>Deltagande företag</b>	En juridisk person från Amgen-koncernen som är bunden av EU-BCR.
<b>Personuppgifter</b>	<p>Varje upplysning som avser en registrerad, som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet. Exempel på personuppgifter kan vara följande:</p> <ul style="list-style-type: none"> <li>• En registrerads namn, adress, personnummer, körkortsnummer, information om finansiella uppgifter, uppgifter om familjemedlemmar eller medicinska uppgifter.</li> <li>• En vårdpersonals namn, yrkesutbildning och förskrivningspraxis.</li> <li>• E-postadress och annan identifierande information som lämnas av någon som besöker en Amgen-webbplats.</li> </ul> <p>Förteckningen ovan är endast vägledande och inte uttömmande.</p>
<b>Personuppgiftsincident</b>	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
<b>Personal</b>	Alla anställda och tillfälligt anställda (inklusive konsulter, bemanningsföretag och kontraktsanställda) i alla deltagande företag.
<b>Behandling</b>	En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning,

<b>Villkor</b>	<b>Definitioner</b>
	användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
<b>Känsliga personuppgifter</b>	<p>Personuppgifter som röjer ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter i syfte att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons kön liv eller sexuell läggning.</p> <p>Åtskilt från EU:s dataskyddslagstiftning betraktar Amgen även finansiell information och information som kan användas för att begå identitetsstöld (till exempel personnummer, körkortnummer och kreditkorts- eller annan bankkontoinformation) som känsliga personuppgifter.</p>
<b>Tekniska och organisatoriska säkerhetsåtgärder</b>	Tekniska och organisatoriska åtgärder som syftar till att skydda personuppgifter mot oavsiktlig eller olaglig förstörelse eller oavsiktlig förlust, ändring, obehörigt avslöjande eller åtkomst, i synnerhet när behandlingen innefattar överföring av data över ett nätverk, och mot alla andra olagliga former av behandling.
<b>Tredje part</b>	<p>En fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, det deltagande företaget som agerar personuppgiftsansvarig och ett deltagande företag som agerar personuppgiftsbiträde.</p> <p>På Amgen anses en leverantör vara en tredje part. Beroende på omständigheterna kan en tredje part fungera som personuppgiftsansvarig eller personuppgiftsbiträde i samband med behandling av personuppgifter.</p>
<b>Leverantör</b>	En fysisk eller juridisk person, verksamhet eller organisation som tillhandahåller varor eller tjänster till ett deltagande företag enligt ett avtalsförhållande eller är en mottagare av personuppgifter från ett sådant deltagande företag för att kunna tillhandahålla dessa varor eller tjänster.

Amgen ska tolka villkoren i dessa EU-BCR i enlighet med EU:s dataskyddslagstiftning.

### 3. Ändamålsbegränsning

- 3.1. Personuppgifter ska behandlas för uttryckligt angivna, särskilda och berättigade ändamål i enlighet med artikel 5.1 b i GDPR.
- 3.2. Personuppgifter behandlas inte på sätt som är oförenliga med de berättigade ändamålen för vilka personuppgifterna samlades in eller gällande lagstiftning. Uppgiftsinförare är skyldiga att hålla fast vid de ursprungliga ändamålen när de lagrar eller ytterligare behandlar personuppgifter eller behandlar personuppgifter som har överförts till dem av ett annat

deltagande företag. Ändamålet med behandling av personuppgifter får endast ändras med samtycke från den registrerade eller i den utsträckning som tillåts enligt gällande lagstiftning.

- 3.3. Känsliga personuppgifter förses med ytterligare skyddsåtgärder såsom genom EU:s dataskyddslagstiftning.

#### **4. Datakvalitet och proportionalitet**

- 4.1. Personuppgifter måste vara korrekta och vid behov hållas uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga, med hänsyn till de ändamål för vilka de behandlas, raderas eller rättas utan dröjsmål.
- 4.2. Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, i enlighet med artikel 5(1)(c) i GDPR.
- 4.3. Behandlingen av personuppgifter styrs av målet att begränsa insamlingen, behandlingen eller användningen av personuppgifter till endast det som är nödvändigt, det vill säga så lite personuppgifter som möjligt. Möjligheten till anonyma eller pseudonyma uppgifter måste övervägas, förutsatt att kostnaden och ansträngningen står i proportion till det önskade ändamålet.
- 4.4. Personuppgifter som inte längre krävs för det affärsändamål för vilket de ursprungligen samlades in och lagrades måste raderas enligt Amgens registerlagringsschema. Om lagstadgade lagringsperioder eller arkiveringsskyldighet gäller blockeras uppgifterna i stället för att raderas. Efter lagringsperioden eller arkiveringsskyldigheten raderas uppgifterna.

#### **5. Rättslig grund för behandling av personuppgifter**

- 5.1. Behandling av personuppgifter är endast tillåten om minst en av följande förutsättningar uppfylls:
  - 5.1.1. Den registrerade har gett sitt samtycke till behandlingen av hans eller hennes personuppgifter för ett eller flera specifika ändamål.
  - 5.1.2. Behandlingen är nödvändig för att fullgöra ett avtal som den registrerade är part i eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås.
  - 5.1.3. Behandlingen är nödvändig för att uppfylla en rättslig skyldighet som den personuppgiftsansvarige är föremål för enligt gällande lagstiftning.
  - 5.1.4. Behandlingen är nödvändig för att skydda den registrerades eller en annan fysisk persons grundläggande intressen, såsom liv, hälsa eller säkerhet.
  - 5.1.5. Behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppgift att utföra.
  - 5.1.6. Behandlingen är nödvändig på grund av en personuppgiftsansvarigs eller en tredje parts berättigade intressen, utom där sådana intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter.

- 5.2. Behandling av personuppgifter relaterade till fällande domar i brottmål och överträdelser ska endast utföras när behandlingen godkänns enligt gällande lagstiftning vad gäller lämpliga skyddsåtgärder för de registrerades rättigheter och friheter.

## **6. Behandling av känsliga personuppgifter**

- 6.1. Om det deltagande företaget, enligt ett specifikt och berättigat ändamål, behöver behandla känsliga personuppgifter gör det deltagande företaget bara det om:
- 6.1.1. Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa känsliga personuppgifter för ett eller flera specifika ändamål, utom då gällande lagstiftning föreskriver att förbudet i artikel 9.1 i GDPR inte kan upphävas av den registrerade.
  - 6.1.2. Behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt gällande lagstiftning eller ett kollektivavtal i enlighet med gällande lagstiftning, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.
  - 6.1.3. Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
  - 6.1.4. Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.
  - 6.1.5. Behandlingen rör känsliga personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
  - 6.1.6. Behandlingen av känsliga personuppgifter är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk.
  - 6.1.7. Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av gällande lagstiftning, vilken ska stå i proportion till det eftersträlvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
  - 6.1.8. Behandlingen av känsliga personuppgifter är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av gällande lagstiftning eller enligt avtal med yrkesverksamma på hälsoområdet, och om dessa känsliga personuppgifter behandlas av eller under ansvar av en hälso- och sjukvårdspersonal måste en sådan yrkesverksam omfattas av tystnadsplikt enligt

gällande lagstiftning eller regler som har fastställts av behöriga organ i en EES-medlemsstat eller av en annan person som också omfattas av tystnadsplikt enligt gällande lagstiftning eller regler som har fastställts av behöriga organ i en EES-medlemsstat.

- 6.1.9. Behandlingen av känsliga personuppgifter är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av gällande lagstiftning, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt.
- 6.1.10. Behandlingen av känsliga personuppgifter är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i GDPR, på grundval av gällande lagstiftning, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

## **7. Rätt till insyn och information**

- 7.1. Alla deltagande företag ska behandla personuppgifter på ett öppet sätt. Amgen har åtagit sig att göra EU-BCR, inbegripet kontaktuppgifter, lättillgängliga och lättåtkomliga för alla registrerade och att informera registrerade om överföring och behandling av deras personuppgifter. Dessa EU-BCR finns på Amgens webbplats [www.amgen.com/bcr](http://www.amgen.com/bcr). Du kan även begära ett exemplar genom att kontakta Amgen på [privacy@amgen.com](mailto:privacy@amgen.com). Amgen använder även olika kommunikationsmedel såsom företagswebbplatser, inbegripet interna webbplatser och nyhetsbrev, kontrakt och specifika integritetsmeddelanden för att uppfylla detta tillgänglighetskrav. Dessutom informerar Amgen de registrerade, med hjälp av dessa kommunikationsmedel, om uppdateringar eller ändringar av EU-BCR eller förteckningen över deltagande företag utan onödigt dröjsmål.
- 7.2. Registrerade vars personuppgifter behandlas av ett deltagande företag ska förse med den information som anges i artiklarna 13 och 14 i GDPR.
- 7.3. Om inte personuppgifter tas emot från en registrerad gäller inte skyldigheten att underrätta den registrerade om tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning eller om registrering eller utlämnande uttryckligen föreskrivs i lagstiftning.

## **8. Rätt till tillgång, rättelse, radering och begränsning av uppgifter**

- 8.1. Varje registrerad har rätt att få bekräftelse från det deltagande företaget om huruvida personuppgifter som rör honom eller henne behandlas eller inte, och, i så fall, tillgång till personuppgifterna och informationen som krävs enligt artikel 15.1 i GDPR. Uppföljningen av en sådan begäran, inklusive möjligheten att ta ut en avgift eller tidsramen för att besvara en sådan begäran, är förbehåll för gällande lagstiftning och kommuniceras på lämpligt sätt till den registrerade när han eller hon lämnar in sin begäran.
- 8.2. Varje registrerad har rätt att få rättelse, radering eller begränsning av personuppgifter, särskilt om uppgifterna är ofullständiga eller felaktiga.

- 8.3. Varje registrerad har, av skäl som hänför sig till hans eller hennes specifika situation, rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på genomförandet av en uppgift som utförs i allmänt intresse eller det deltagande företags eller en tredje parts berättigade intressen (inbegripet profilering som grundar sig på detta). Det deltagande företaget får inte längre behandla personuppgifterna såvida det inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.
- 8.4. Varje registrerad har rätt att (kostnadsfritt) invända mot behandling av personuppgifter som avser honom eller henne för direkt marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring. Om den registrerade invänder mot behandling av personuppgifter som rör honom eller henne för direkt marknadsföring måste det deltagande företaget upphöra med att behandla personuppgifterna för sådana ändamål.
- 8.5. Varje registrerad har rätt att underrättas om tredje parter som personuppgifter har lämnats ut till om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett, i enlighet med artikel 19 i GDPR.
- 8.6. Varje registrerad har rätt att få kännedom om bakomliggande logik i samband med automatisk behandling av personuppgifter i enlighet med artikel 13(2)(f) i GDPR.
- 8.7. Om behandlingen är baserad på samtycke har varje registrerad rätt att när som helst återkalla sitt samtycke. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas.
- 8.8. Varje registrerad har rätt att klaga till det deltagande företaget angående behandlingen av personuppgifter genom den interna klagomålsmekanism som tillhandahålls i enlighet med artikel 17.
- 8.9. Begäranden i samband med denna artikel 8 (eller artikel 9 nedan) ska skickas till det deltagande företaget på [privacy@amgen.com](mailto:privacy@amgen.com). Det rekommenderas starkt att göra begäranden via e-post, men det utesluter inte att en registrerad gör en muntlig begäran. Det deltagande företaget ska utan dröjsmål, och senast inom en månad efter mottagandet av begäran, informera den registrerade om resultatet av hans eller hennes begäran (inbegripet i tillämpliga fall skälen till att inte vidta åtgärder och möjligheten att lämna in ett klagomål till den behöriga dataskyddsmyndigheten eller ansöka om rättsmedel). Denna period på en månad kan vid behov förlängas med ytterligare två månader, med hänsyn till begärandenas komplexitet och antal. Det deltagande företaget ska informera den registrerade om en sådan förlängning inom en månad efter mottagandet av begäran, tillsammans med skälen till förseningen. Information som tillhandahållits, all kommunikation och samtliga åtgärder som vidtas enligt denna artikel 8 (eller artikel 9 nedan) ska tillhandahållas kostnadsfritt. Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen (a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller (b) vägra att tillmötesgå begäran. Det åligger det deltagande företaget att visa att begäran är uppenbart ogrundad eller orimlig.

## 9. Automatiserade individuella beslut



- 9.1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Det ska inte tillämpas om beslutet
- 9.1.1. är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och det deltagande företaget
- 9.1.2. krävs eller tillåts enligt gällande lagstiftning som också fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen (inbegripet åtminstone rätten till personlig kontakt med det deltagande företaget för att kunna uttrycka sin åsikt och bestrida beslutet)
- 9.1.3. grundar sig på den registrerades uttryckliga samtycke.

## 10. Säkerhet och konfidentialitet

- 10.1. Amgen genomför lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda mot och upptäcka personuppgiftsincidenter. Internationella ramverk, såsom ISO/IEC 27002, används av Amgen för att fastställa dessa säkerhetsåtgärder.
- 10.2. Amgen använder sig av processer för att säkerställa att personuppgiftsincidenter blir föremål för rapportering, uppföljning och lämpliga korrigerande åtgärder, beroende på vad som behövs. Alla personuppgiftsincidenter ska dokumenteras (inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits), och dokumentationen ska på begäran göras tillgänglig för den behöriga dataskyddsmyndigheten. Deltagande företag ska utan onödigt dröjsmål meddela alla personuppgiftsincidenter till Amgen France, den integritetsansvarige och det andra relevanta integritetsombudet/-funktionen samt (om det deltagande företag som har drabbats av en personuppgiftsincident agerar personuppgiftsbiträde) till det deltagande företag som agerar personuppgiftsansvarig. Personuppgiftsincidenter ska, i samarbete med den integritetsansvarige, anmälas till den behöriga dataskyddsmyndigheten utan onödigt dröjsmål (och om möjligt högst 72 timmar efter att personuppgiftsincidenten har kommit till kännedom) såvida det inte är osannolikt att det leder till risk för registrerades rättigheter och friheter. Om personuppgiftsincidenten sannolikt medför hög risk för de registrerades rättigheter och friheter ska de registrerade också underrättas om den utan onödigt dröjsmål.
- 10.3. Informationssäkerhetsriskbedömningar används för att identifiera potentiella hot mot känsliga personuppgifter och genomförande av ytterligare säkerhetskontroller om det behövs.
- 10.4. Vidtagandet av åtgärder ska ske med beaktande av den senaste utvecklingen, i enlighet med artikel 32 i GDPR.
- 10.5. Den informationssäkerhetsansvarige arbetar tillsammans med den integritetsansvarige för att försäkra personuppgifters säkerhet och konfidentialitet.
- 10.6. De tekniska och organisatoriska säkerhetsåtgärderna ska utformas för att genomföra dataskyddsprinciperna enligt artikel 5 i GDPR och principerna om inbyggt dataskydd och dataskydd som standard i enlighet med artikel 25 i GDPR samt för att underlätta efterlevnaden av de krav som ställs av dessa EU-BCR i praktiken.

## 11. Förhållanden med personuppgiftsbiträden (Amgens uppgiftsinförare eller leverantör)

- 11.1. Det deltagande företaget (som agerar personuppgiftsansvarig) väljer omsorgsfullt ett personuppgiftsbiträde, som kan vara ett annat deltagande företag eller en leverantör. Personuppgiftsbiträdet måste ge tillräckliga garantier för sina tekniska och organisatoriska säkerhetsåtgärder som styr behandlingen som ska utföras och måste säkerställa att dessa åtgärder efterlevs.
- 11.2. Om utkontraktering bedöms vara nödvändig efter att verksamhetsbehoven och riskerna med en sådan utkontraktering har bedömts innefattar processen för att välja personuppgiftsbiträde en utvärdering av integritetsriskfaktorerna och att balansera verksamhetsbehoven mot de potentiella riskerna.
- 11.3. Det deltagande företag som agerar som personuppgiftsansvarig och använder skriftliga avtal ska, i enlighet med gällande lagstiftning (och i synnerhet kraven i artikel 28.3 i GDPR), bland annat ge personuppgiftsbiträdet instruktioner om följande:
  - 11.3.1. Personuppgiftsbiträdet ska endast agera enligt instruktioner från det deltagande företag som agerar personuppgiftsansvarig. Behandling av personuppgifter för personuppgiftsbitrådets egna ändamål eller för tredje parts ändamål är förbjuden.
  - 11.3.2. Reglerna för säkerhet och konfidentialitet ska åligga personuppgiftsbiträdet och lämpliga tekniska och organisatoriska åtgärder ska genomföras för att säkerställa en säkerhetsnivå som är lämplig för risken med behandlingen.
  - 11.3.3. Personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
  - 11.3.4. Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av det deltagande företag som agerar personuppgiftsansvarig. Om ett sådant tillstånd ges ska samma dataskyddsskyldigheter som anges i avtalet eller en annan rättsakt mellan det deltagande företag som agerar som personuppgiftsansvarig och personuppgiftsbiträdet åläggas det andra personuppgiftsbiträdet.
  - 11.3.5. Med tanke på behandlingens art ska personuppgiftsbiträdet hjälpa det deltagande företag som agerar personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att det deltagande företaget kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter.
  - 11.3.6. Personuppgiftsbiträdet måste hjälpa det deltagande företag som agerar personuppgiftsansvarig att säkerställa efterlevnad av skyldigheterna avseende säkerhet vid behandling, anmälan om en personuppgiftsincident till den behöriga dataskyddsmyndigheten, underrättelse till den registrerade om en personuppgiftsincident, dataskyddskonsekvensbedömningar och tidigare samråd med den behöriga dataskyddsmyndigheten, med hänsyn till behandlingens natur och den information som är tillgänglig för den personuppgiftsansvarige.
  - 11.3.7. Beroende på vad det deltagande företag som agerar personuppgiftsansvarig väljer ska personuppgiftsbiträdet radera eller återlämna alla personuppgifter till det

deltagande företag som agerar personuppgiftsansvarig efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt EU:s dataskyddslagstiftning.

- 11.3.8. Personuppgiftsbiträdet måste ge det deltagande företag som agerar personuppgiftsansvarig tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel 11 har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av det deltagande företag som agerar personuppgiftsansvarig eller av en annan revisor som bemyndigats av det.
- 11.4. Det deltagande företag som agerar personuppgiftsansvarig ska se till att personuppgiftsbiträdet förblir fullständigt förenligt med de överenskomna tekniska och organisatoriska säkerhetsåtgärderna.
- 11.5. Det deltagande företag som agerar personuppgiftsansvarig behåller ansvaret för behandlingens legitimitet och är fortfarande ansvarigt för den registrerades rättigheter. I den mån personuppgiftsbiträdet omfattas av EU:s dataskyddslagstiftning ska den också vara ansvarig för sina skyldigheter och ansvarsområden som personuppgiftsbiträde enligt sådan lagstiftning.
- 11.6. För att sörja för de avtalsförpliktelser som anges i denna artikel om personuppgiftsbiträden tillhandahålls en avtalsmall som heter "dataintegritetsschema" som ska användas av deltagande företag som agerar som personuppgiftsansvariga. Det deltagande företag som agerar som personuppgiftsansvarig kan, beroende på de specifika omständigheterna i varje avtalsarrangemang, förhandla om andra bestämmelser än de som anges i dataintegritetsschemat, men avtalsbestämmelserna måste fortfarande täcka åtminstone de skyldigheter som anges ovan i denna artikel 11.
- 11.7. Varje deltagande företag som agerar personuppgiftsbiträde och lyder under EU:s dataskyddslagstiftning måste föra ett register över alla kategorier av behandling som utförs på uppdrag av ett deltagande företag som agerar personuppgiftsansvarig. Registret ska föras skriftligt, inklusive i elektronisk form, ska på begäran göras tillgängligt för den integritetsansvarige och den behöriga dataskyddsmyndigheten och ska innehålla följande information: (a) namn och kontaktuppgifter för det deltagande företag som agerar personuppgiftsbiträde och för varje deltagande företag som agerar personuppgiftsansvarig på uppdrag av vilket det agerar, samt i tillämpliga fall det deltagande företags företrädare samt dataskyddsombudet, (b) kategorierna av behandling som utförs på uppdrag av varje deltagande företag som agerar personuppgiftsansvarig, (c) i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som bygger på ett undantag enligt artikel 49 i GDPR, dokumentationen av lämpliga skyddsåtgärder och (d) om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.

## **12. Begränsningar av överföringar och vidare överföringar**

- 12.1. Alla överföringar av personuppgifter som omfattas av dessa EU-BCR till tredje parter utanför EES ska respektera EU:s dataskyddslagstiftning om överföringar och vidare överföringar av personuppgifter genom att använda standardavtalsklausulerna som har godkänts enligt kommissionens genomförandebeslut (EU) av den 4 juni 2021 om standardavtalsklausuler för

överföring av personuppgifter till tredjeländer i enlighet med GDPR eller på annat adekvat sätt enligt kapitel V i GDPR (inklusive, undantagsvis, om ett undantag gäller en specifik situation i enlighet med artikel 49 i GDPR).

- 12.2. Alla överföringar av personuppgifter som omfattas av dessa EU-BCR till personuppgiftsbiträden utanför EES ska respektera EU:s dataskyddslagstiftning för personuppgiftsbiträden (och kraven i artikel 11 ovan) utöver reglerna om överföringar och vidare överföringar av personuppgifter som anges i denna artikel 12 och i EU:s dataskyddslagstiftning.
- 12.3. Innan personuppgifter överförs till en uppgiftsinförare eller (med avseende på pågående överföringar) innan någon uppdaterad lokal nationell lagstiftning träder i kraft ska uppgiftsutföraren, tillsammans med den integritetsansvarige och Amgen France, med hjälp av uppgiftsinföraren och med hänsyn till omständigheterna kring överföringen, utvärdera om lokal nationell lagstiftning hindrar uppgiftsinföraren från att uppfylla sina skyldigheter enligt EU-BCR och avgöra om eventuella nödvändiga kompletterande åtgärder ska genomföras. Vid en sådan bedömning tas hänsyn till följande:
  - 12.3.1. De specifika omständigheterna för överföringen (inklusive ändamålen som personuppgifterna överförs och behandlas för, typerna av enheter som är inblandade i behandlingen, den ekonomiska sektorn där överföringen sker, kategorierna och formatet för personuppgifterna som överförs, platsen för behandlingen (inbegripet lagring) och överföringskanalerna som används).
  - 12.3.2. Lagarna och praxisen i destinationstredjelandet som är relevanta med tanke på de specifika omständigheterna för överföringen (inbegripet dem som kräver att uppgifter lämnas ut till offentliga myndigheter eller ger tillgång till uppgifter till sådana myndigheter) och tillämpliga begränsningar och skyddsåtgärder.
  - 12.3.3. Relevanta avtalsenliga, tekniska eller organisatoriska skyddsåtgärder som införts i samband med överföringen, inbegripet åtgärder som vidtas under överföringen och behandlingen av personuppgifterna i destinationslandet.

Vidare ska en sådan bedömning grundas på förståelsen att lagar och praxis i destinationstredjelandet respekterar den registrerades grundläggande rättigheter och friheter och inte går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att säkerställa något av följande mål: (a) den nationella säkerheten, (b) försvaret, (c) den allmänna säkerheten, (d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten, (e) andra viktiga mål av generellt allmänt intresse, särskilt viktiga ekonomiska eller finansiella intressen, däribland penning-, budget- eller skattefrågor, folkhälsa och social trygghet, (f) skydd av rättsväsendets oberoende och rättsliga åtgärder, (g) förebyggande, förhindrande, utredning, avslöjande och lagföring av överträdelser av etiska regler som gäller för lagreglerade yrken, (h) en tillsyns-, inspektions- eller regleringsfunktion som har samband med myndighetsutövning i fall som nämns i tidigare mål, (i) skydd av den registrerade eller andras rättigheter och friheter eller (j) verkställighet av civilrättsliga krav.

Den integritetsansvarige ska granska och godkänna den dokumenterade bedömningen och eventuella föreslagna kompletterande åtgärder. Om resultatet av bedömningen visar på ett behov att genomföra kompletterande åtgärder ska uppgiftsutföraren genomföra dessa åtgärder. Om inga kompletterande åtgärder kan vidtas (eller om det instrueras av den

integritetsansvarige eller en behörig dataskyddsmyndighet) ska uppgiftsutföraren avbryta överföringen. Resultatet av bedömningen och föreslagna kompletterande åtgärder ska registreras och lämnas till den behöriga dataskyddsmyndigheten om det är nödvändigt.

Den integritetsansvarige och Amgen France informerar alla deltagande företag om den genomförda bedömningen och om dess resultat så att de identifierade kompletterande åtgärderna kan tillämpas där samma typ av överföringar utförs av andra deltagande företag eller, om inte effektiva kompletterande åtgärder kan vidtas, så att sådana överföringar avbryts eller avslutas.

- 12.4. Uppgiftsinföraren ska omgående meddela uppgiftsutföraren, Amgen France och den integritetsansvarige om den har skäl att tro att den är eller har blivit föremål för lagar eller praxis som skulle hindra den från att uppfylla sina skyldigheter enligt dessa EU-BCR, inbegripet efter en ändring av lokala nationella lagar i det tredje landet enligt beskrivningen i artikel 12.3 eller en åtgärd såsom en begäran om utlämnande enligt beskrivningen i artikel 16.3. Dessutom ska uppgiftsutförarna (tillsammans med den integritetsansvarige) fortlöpande och i förekommande fall med hjälp av uppgiftsinförarna övervaka utvecklingen i de tredje länder till vilka uppgiftsutförarna har överfört personuppgifter som negativt skulle kunna påverka den inledande bedömningen av skyddsnivån för personuppgifter och de beslut som fattas med avseende på sådana överföringar.
- 12.5. Efter avbrytandet av en överföring måste uppgiftsutföraren avsluta överföringen eller uppsättningen överföringar om inte uppgiftsinföraren kan följa EU-BCR eller om inte efterlevnad återställs inom en månad efter avbrytandet. I sådana fall måste uppgiftsinföraren, beroende på vad uppgiftsutföraren väljer, antingen återlämna eller förstöra alla personuppgifter som har överförts före avbrytandet, och eventuella kopior därav.
- 12.6. Personuppgiftsflöden som inte omfattas av dessa EU-BCR eller som inte härrör från ett deltagande företag som är etablerat i en EES-medlemsstat anses inte vara en överföring av personuppgifter enligt dessa EU-BCR och omfattas följaktligen inte av kraven i dessa EU-BCR.

### **13. Utbildningsprogram**

- 13.1. Såsom beskrivs i bilaga 2 tillhandahåller Amgen lämplig och uppdaterad utbildning om integritetsprinciper och mer specifikt om EU-BCR till all personal. Utbildningen innehåller också information om konsekvenserna enligt straff- och arbetsrätt eller deras tjänsteavtal för personal som bryter mot EU-BCR.
- 13.2. Utbildningen är obligatorisk och repeteras en gång om året. Framgångsrikt deltagande i utbildningen dokumenteras.
- 13.3. Specifika utbildningar ges från fall till fall till personal som har permanent eller regelbunden tillgång till personuppgifter, eller som är inblandade i insamlingen av personuppgifter eller i utvecklingen av verktyg som används för att behandla personuppgifter.
- 13.4. Dessutom tillhandahåller Amgens team för global integritetsefterlevnad lämplig information och resurser relaterade till integritet, inbegripet på Amgens intranätportal.

### **14. Gransknings- och övervakningsprogram**

- 14.1. Den integritetsansvarige säkerställer att alla deltagande företag (och deras efterlevnad av dessa EU-BCR) ingår i gransknings- och övervakningsprogrammet ur ett integritets- och dataskyddsperspektiv. Omfattande granskningar utförs regelbundet, inte mer sällan än vartannat till vart tredje år (för deltagande företag med medelhög till hög riskprofil baserat på granskningsavdelningens riskbedömningsmetodik) och vart fjärde till femte år (för deltagande företag med en låg riskprofil baserat på granskningsavdelningens riskbedömningsmetodik), av det interna granskningsteamet eller oberoende, externa certifierade granskare. Omfattande granskningar innefattar dataskydds- och integritetsfrågor inom deras tillämpningsområde (inbegripet efterlevnad av dessa EU-BCR, där det är tillämpligt för och används av ett deltagande företag). Utöver omfattande granskningar, och utan att det påverkar tidsramarna som anges ovan, utförs granskningar i andra omfattningar, inbegripet tvärfunktionella eller problemspecifika granskningar (till exempel efterlevnad av EU-BCR), en begränsad granskning av en eller flera system för behandling av personuppgifter eller en begränsad granskning av en eller flera funktionella avdelningar (till exempel teamet för global integritetsefterlevnad). Granskningsprogrammet utvecklas och godkänns i samarbete med chefsgranskaren och den efterlevnadsansvarige som är förste vice vd. Den integritetsansvarige, den efterlevnadsansvarige och den informationsansvarige kan inleda EU-BCR-relaterade ad hoc-granskningar när som helst. Exempel på när det kan ske är som åtgärd vid ett identifierat efterlevnadsproblem eller en rapport om väsentligt bristande efterlevnad, en personuppgiftsincident och en väsentlig ändring av EU:s dataskyddslagstiftning. Revisionsprogrammet täcker alla aspekter av EU-BCR, inbegripet metoder för att säkerställa att korrigerande åtgärder sker.
- 14.2. Alla EU-BCR-granskningsrapporter kommuniceras till den efterlevnadsansvarige och den integritetsansvarige inom skälig tid. EU-BCR-granskningsammanfattningar och -resultat, såväl som annan relevant information, rapporteras också regelbundet till Amgen Incs styrelse via lämpliga kommittéer (till exempel kommittén för företagsansvar och efterlevnad eller styrelsens granskningskommitté), till styrelsen för Amgen France och (i tillämpliga fall, till exempel i samband med ett resultat som kräver korrigerande) till det relevanta deltagande företaget. Kommittén för företagsansvar och efterlevnad i Amgen, Incs styrelse sammanträder fem gånger om året. Integritet och dataskydd behandlas årligen, vanligtvis på oktobermötet.
- 14.3. Den behöriga dataskyddsmyndigheten kan på begäran få en kopia av EU-BCR-relaterade granskningsrapporter.
- 14.4. Varje deltagande företag ska samarbeta med och acceptera, utan begränsningar, att bli granskad av den behöriga dataskyddsmyndigheten. Varje granskad enhet måste omedelbart informera den integritetsansvarige om den får information om en sådan granskning eller en sådan granskning äger rum.

## **15. Efterlevnad och övervakning av efterlevnad**

- 15.1. Amgen utser lämplig personal, inklusive i tillämpliga fall ett nätverk av dataskyddsombud, med stöd från högsta ledningen att overse och säkerställa efterlevnad av dataskyddsregler. Den integritetsansvarige leder teamet för global integritetsefterlevnad som är ett globalt team som ger expertsupport över hela världen till Amgen-enheter (inbegripet deltagande företag).
- 15.2. På Amgen är den integritetsansvariges ansvarsområden bland annat att
- 15.2.1. ge råd till styrelsen

- 15.2.2. säkerställa efterlevnad av skyddet av personuppgifter på global nivå (inbegripet att ha det övergripande ansvaret för EU-BCR)
  - 15.2.3. rapportera regelbundet om efterlevnaden av skyddet av personuppgifter (inbegripet till den efterlevnadsansvarige)
  - 15.2.4. arbeta med den behöriga dataskyddsmyndighetens utredningar.
- 15.3. I teamet för global integritetsefterlevnad ingår den integritetsansvarige (som, utöver ansvarsområdena som anges ovan, överser det globala nätverket av dataskyddsombud), det europeiska dataskyddsombudet och andra lokala dataskyddsombud. Teamet för global integritetsefterlevnad har det övergripande ansvaret för dataskydd och integritetsefterlevnad globalt på Amgen.
- 15.4. Det europeiska dataskyddsombudet har utsetts av Amgen till dataskyddsombud för EES, Storbritannien och Schweiz. Det europeiska dataskyddsombudet har de uppgifter som anges i artikel 39 i GDPR. Amgen ska se till att det europeiska dataskyddsombudets uppgifter och uppdrag inte leder till en intressekonflikt med sådana uppgifter. Det europeiska dataskyddsombudet har en direktrapporteringsväg till den integritetsansvarige (som utgör en del av den högsta ledningsnivån för Amgen) och får stöd av den lokala efterlevnadschefen i Frankrike. Det europeiska dataskyddsombudet kan kontakta den integritetsansvarige om frågor eller problem uppstår när han eller hon utför sitt uppdrag. Det europeiska dataskyddsombudet kan kontaktas på [privacy@amgen.com](mailto:privacy@amgen.com)
- 15.5. På lokal nivå ansvarar dataskyddsombud för att sköta lokala integritetsrelaterade begäranden från registrerade, för att säkerställa efterlevnad på lokal nivå med stöd från teamet för global integritetsefterlevnad och för att rapportera allvarliga integritetsproblem till den integritetsansvarige. Amgen upprätthåller ett dataskyddsombudsnätverk och säkerställer att ett dataskyddsombud utnämns eller tilldelas för varje land där Amgen har en företagsenhet (det deltagande företaget) och gällande lagstiftning i jurisdiktionen för det deltagande företaget kräver en sådan utnämning.
- 15.6. Vanligtvis antingen är dataskyddsombud, eller stöds av, de lokala efterlevnadscheferna som rapporterar till avdelningen för global efterlevnad och affärsetik. Teamet för global integritetsefterlevnad är en del av, och rapporterar till, teamet för global efterlevnad och affärsetik som leds av den efterlevnadsansvarige. Den efterlevnadsansvarige har det övergripande ansvaret för Amgen-koncernens rättsliga och regulatoriska efterlevnad världen över. I sällsynta fall, på grund av de specifika omständigheterna för ett deltagande företag eller andra speciella omständigheter, kan dataskyddsombudet komma från en annan funktion, till exempel regleringsfunktionen. Under alla omständigheter säkerställer teamet för global integritetsefterlevnad att dataskyddsombuden och efterlevnadscheferna är utbildade på lämpligt sätt och har en tillräcklig nivå av ledning och expertis för att utföra sin roll. Dessutom har dataskyddsombuden en direktrapporteringsväg till den integritetsansvarige och får hjälp av teamet för global integritetsefterlevnad om de behöver ytterligare vägledning.
- 15.7. Varje deltagande företag som agerar personuppgiftsansvarig ska ansvara för och kunna påvisa efterlevnad av EU-BCR. Som en del av detta krav måste alla deltagande företag:
- 15.7.1. Föra ett register över alla kategorier av behandling som utförts i enlighet med kraven i artikel 30.1 i GDPR. Registret ska föras skriftligt, inklusive i elektronisk

form, ska på begäran göras tillgängligt för den integritetsansvarige och den behöriga dataskyddsmyndigheten och ska innehålla följande information: (a) namn och kontaktuppgifter för det deltagande företaget som agerar personuppgiftsansvarig, dess företrädare samt dataskyddsombudet, (b) ändamålen med behandlingen, (c) en beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter, (d) de kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer, (e) i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation, inbegripet identifiering av tredjelandet eller den internationella organisationen och, vid sådana överföringar som bygger på ett undantag, dokumentationen av lämpliga skyddsåtgärder, (f) om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter och (g) om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.

- 15.7.2. Genomföra konsekvensbedömningar avseende dataskydd för behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter i enlighet med artikel 35 i GDPR. Om en konsekvensbedömning avseende dataskydd enligt artikel 35 indikerar att behandlingen skulle leda till en hög risk utan vidtagna åtgärder av det deltagande företaget för att minska risken, måste den integritetsansvarige rådfrågas före behandlingen, som sedan ska samråda med den behöriga dataskyddsmyndigheten i enlighet med artikel 36 i GDPR.

## **16. Åtgärder ifall nationell lagstiftning förhindrar efterlevnad av EU-BCR**

- 16.1. Om ett deltagande företag har anledning att tro att de lagar som gäller för det hindrar det deltagande företaget från att uppfylla sina skyldigheter enligt EU-BCR eller har en väsentlig effekt på de garantier som reglerna tillhandahåller ska det omgående informera den integritetsansvarige (förutom om det förbjuds av en brottsbekämpande myndighet, såsom ett förbud enligt straffrätt för att bevara sekretessen för en brottsutredning) och Amgen France.
- 16.2. Om det blir en konflikt mellan den lokala nationella lagstiftningen och åtagandena i EU-BCR avgör den integritetsansvarige tillsammans med det lokala dataskyddsombudet vilka juridiskt lämpliga åtgärder som krävs. Om det är nödvändigt rådgör den integritetsansvarige även med den behöriga dataskyddsmyndigheten.
- 16.3. Om något lagkrav som ett deltagande företag är föremål för i ett tredje land sannolikt får en väsentlig negativ effekt på garantierna som tillhandahålls av EU-BCR ska den integritetsansvarige, Amgen France och uppgiftsutföraren omgående underrättas av uppgiftsinföraren, och den integritetsansvarige ska meddela den behöriga dataskyddsmyndigheten och (om möjligt) de registrerade. Detta innefattar (a) en rättsligt bindande begäran om utlämnande av personuppgifter från en brottsbekämpande myndighet eller ett statligt säkerhetsorgan, och i ett sådant fall ska den behöriga dataskyddsmyndigheten tydligt informeras om begäran, inbegripet information om uppgifterna som begärs, det begärande organet och den rättsliga grunden för utlämningen och svaret som lämnas (såvida det inte är förbjudet, såsom vid ett förbud enligt straffrätt för att bevara sekretessen för en brottsutredning) och (b) eventuell direkt åtkomst av offentliga myndigheter till personuppgifter som överförs i enlighet med dessa EU-BCR enligt lagarna i destinationslandet, och i sådant fall ska en sådan underrättelse innehålla all information som är tillgänglig för det deltagande företaget (såvida det inte är förbjudet, såsom vid ett förbud enligt straffrätt för att bevara sekretessen för en brottsutredning).



- 16.4. Om avbrytandet eller underrättelsen i särskilda fall inte tillåts gör det deltagande företag som tar emot begäran sitt bästa för att beviljas undantag från detta förbud för att kommunicera så mycket information som möjligt och så snart som möjligt och kunna påvisa (på begäran av uppgiftsutföraren) att det har gjort det.
- 16.5. Uppgiftsinföraren förser med jämna mellanrum uppgiftsutföraren med så mycket relevant information som möjligt om mottagna begäranden (i synnerhet antalet begäranden, typen av personuppgifter som begärs, identiteten på de begärande myndigheterna och huruvida begärandena har bestridits samt resultatet av sådana invändningar). Uppgiftsinföraren behåller sådan information så länge som personuppgifterna omfattas av de skyddsåtgärder som tillhandahålls av EU-BCR och gör dem tillgängliga för den behöriga dataskyddsmyndigheten på begäran. Om uppgiftsinföraren delvis eller helt förbjuds att förse uppgiftsutföraren med ovanstående information informerar uppgiftsinföraren uppgiftsutföraren om det utan onödigt dröjsmål.
- 16.6. Uppgiftsinföraren ska, tillsammans med den integritetsansvarige, granska lagenligheten för en begäran om utlämnande från en offentlig myndighet för att avgöra om den faller inom de befogenheter som den begärande offentliga myndigheten är beviljade. Uppgiftsinföraren ifrågasätter begäran om den, efter en sådan bedömning, kommer fram till (tillsammans med den integritetsansvarige) att det finns rimliga skäl att anse att begäran är olaglig enligt lagarna i destinationslandet, tillämpliga skyldigheter enligt internationell lagstiftning eller principen om internationell hövlighet. Om uppgiftsinföraren anser att det finns sådana rimliga skäl att betrakta begäran som olaglig undersöker den möjligheten att överklaga. Om uppgiftsinföraren ifrågasätter en begäran ansöker den om interimistiska åtgärder i syfte att upphäva effekterna av begäran tills den behöriga rättsliga myndigheten har beslutat om dess saklighet. Uppgiftsinföraren lämnar inte ut de begärda personuppgifterna förrän det krävs enligt gällande lagstiftning och förfaranderegler i destinationslandet. Uppgiftsinföraren dokumenterar sin rättsliga bedömning och eventuella invändningar mot begäran om utlämnande och, i den utsträckning det är tillåtet enligt lagarna i destinationslandet, gör dokumentationen tillgänglig för uppgiftsutföraren och, på begäran, den behöriga dataskyddsmyndigheten.
- 16.7. Uppgiftsinföraren tillhandahåller den minsta tillåtna mängden information när den svarar på en begäran om utlämnande, baserat på en rimlig tolkning av begäran.
- 16.8. Under alla omständigheter ska överföringar av personuppgifter från ett deltagande företag till en offentlig myndighet inte vara omfattande, oproportionerliga eller urskillningslösa på ett sätt som skulle gå utöver vad som är nödvändigt i ett demokratiskt samhälle.
- 16.9. För deltagande företag som är belägna i EES kan domar från en domstol och beslut från en administrativ myndighet i ett tredjeland som kräver att en personuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter endast godkännas eller verkställas om de grundas på ett internationellt avtal, såsom ett avtal om ömsesidig rättslig hjälp, som är i kraft mellan det begärande tredjelandet och EU eller en EES-medlemsstat, utan att det påverkar andra grunder för överföring enligt kapitel V i GDPR.

## **17. Interna klagomålsmekanismer**

- 17.1. Amgen nyttjar sin befintliga klagomålshanteringsprocess för att inkludera hantering av EU-BCR-relaterade klagomål eller problem.

- 17.2. Registrerade kan när som helst klaga på att ett deltagande företag inte följer EU-BCR. Sådana klagomål hanteras av teamet för global integritetsefterlevnad under ledning av den integritetsansvarige och i samarbete med det relevanta lokala dataskyddsombudet.
- 17.3. Amgen rekommenderar att sådana klagomål lämnas skriftligen via post eller e-post direkt till teamet för global integritetsefterlevnad eller till det deltagande företaget. Teamet för global integritetsefterlevnad kan kontaktas med hjälp av kontaktuppgifterna nedan:

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

E-post: [privacy@amgen.com](mailto:privacy@amgen.com)

- 17.4. Amgen-personal kan, när det är acceptabelt enligt de lagar som gäller för det deltagande företaget, använda verksamhetens hjälplinje avseende uppförande för att rapportera ett EU-BCR-klagomål.
- 17.5. Om klagomålet tas emot lokalt av det deltagande företaget ska dataskyddsombudet om nödvändigt översätta det och utan onödigt dröjsmål vidarebefordra det till teamet för global integritetsefterlevnad.
- 17.6. Ett första svar lämnas till den registrerade inom tio (10) arbetsdagar som informerar honom eller henne om att klagomålet är under behandling och att han eller hon kommer att få ett konkret svar utan onödigt dröjsmål och under alla omständigheter inom en månad efter mottagandet av begäran. Beroende på komplexiteten och antalet begäranden kan en månadsperiod förlängas med högst två ytterligare månader, i vilket fall den registrerade ska informeras om detta. Det konkreta svaret innehåller detaljer om våra undersökningsresultat och eventuella åtgärder som Amgen har vidtagit eller föreslår att vidta. Om Amgen avgör att inga åtgärder bör vidtas ska detta förklaras för den registrerade och skälen till beslutet ska uppges.
- 17.7. Om klagomålet bifalls av Amgen vidtar Amgen lämpliga korrigerande åtgärder. Dessa åtgärder beslutas från fall till fall av den integritetsansvarige, teamet för global integritetsefterlevnad, den lokala dataskyddsmyndigheten och, i tillämpliga fall, andra relevanta avdelningar. Om teamet för global integritetsefterlevnad upptäcker oegentligheter i samband med någon person vidtas lämpliga disciplinära åtgärder, upp till och inklusive uppsägning av anställning eller tillfällig anställning, i den utsträckning som tillåts enligt gällande lagstiftning.
- 17.8. Den registrerade får ett svar som informerar honom eller henne om utgången av klagomålet. Det ska ske utan onödigt dröjsmål och i alla händelser inom en månad efter mottagandet av klagomålet (med tillräcklig information för att Amgen ska kunna identifiera klagomålets art och, endast när det rimligen är nödvändigt, med information som begärs för att bekräfta den klagandes identitet). Beroende på komplexiteten och antalet begäranden kan en månadsperiod förlängas med högst två ytterligare månader, i vilket fall den registrerade ska informeras om detta.
- 17.9. Den registrerade informeras om att han eller hon kan inkomma med ett anspråk till domstolen i en EES-medlemsstat eller den behöriga dataskyddsmyndigheten om han eller hon inte är nöjd med Amgens svar. Det är emellertid inte ett krav för en registrerad att först gå igenom Amgens klagomålshanteringsprocess innan han eller hon får inkomma med ett anspråk till domstolen i en EES-medlemsstat eller den behöriga dataskyddsmyndigheten.

- 17.10. Klagomålshanteringsprocessen offentliggörs genom publiceringen av EU-BCR enligt artikel 7 ovan.

## **18. Tredjepartsförmånstagares rättigheter och skyldigheter**

- 18.1. En registrerad vars personuppgifter härrör från EES eller skyddas av EU:s dataskyddslagstiftning och överförs till deltagande företag utanför EES ska ha rätt att genomdriva EU-BCR som tredjepartsförmånstagare och ska ha rätt att söka rättslig gottgörelse, erhålla rättslig prövning och, i förekommande fall, få ersättning för faktisk skada som har uppkommit till följd av en överträdelse av dessa EU-BCR. En sådan typ av talan kan väckas av den registrerade i en behörig dataskyddsmyndighet (vilket kan vara dataskyddsmyndigheten i den EES-medlemsstat där den registrerade har sin hemvist, dataskyddsmyndigheten på den registrerades arbetsplats eller dataskyddsmyndigheten på platsen där den påstådda överträdelsen har inträffat). Registrerade kan också väcka talan i en behörig domstol i en EES-medlemsstat (vilket kan vara domstolen i EES-medlemsstaten där det relevanta deltagande företaget har en anläggning eller domstolen i EES-medlemsstaten där den registrerade har sin hemvist). En registrerad kan företrädas i utövandet av sin rätt till ett effektivt rättsmedel mot ett deltagande företag av ett icke-vinstdrivande organ, en organisation eller en förening förutsatt att organet, organisationen eller föreningen har bildats korrekt i enlighet med gällande lagstiftning, har lagstadgade mål som ligger i allmänhetens intresse och är aktiv inom området för skydd av registrerades rättigheter och friheter i samband med skyddet av deras personuppgifter. Den registrerade ska kunna genomdriva följande artiklar som tredjepartsförmånstagare:
- 18.1.1. Artiklarna 1 (Tillämpningsområde), 2 (Definitioner), 3 (Ändamålsbegränsning), 4 (Datakvalitet och proportionalitet), 5 (Rättslig grund för behandling av personuppgifter) och 6 (Behandling av känsliga personuppgifter).
  - 18.1.2. Artikel 7 (Rätt till insyn och information).
  - 18.1.3. Artiklarna 8 (Rätt till tillgång, rättelse, radering och begränsning av uppgifter) och 9 (Automatiserade individuella beslut).
  - 18.1.4. Artikel 10 (Säkerhet och konfidentialitet), 11 (Förhållanden med personuppgiftsbiträden (Amgens uppgiftsinförare eller leverantör)) och 12 (Begränsning av överföringar och vidare överföringar).
  - 18.1.5. Artiklarna 16 (Åtgärder ifall nationell lagstiftning förhindrar efterlevnad av EU-BCR) och 21 (Förhållande mellan nationell lagstiftning och EU-BCR).
  - 18.1.6. Artikel 18 (Tredjepartsförmånstagares rättigheter och skyldigheter).
  - 18.1.7. Artikel 19 (Ömsesidigt bistånd och samarbete med dataskyddsmyndigheter).
- 18.2. För tydlighetens skull omfattar inte tredjepartsförmånstagares rättigheter de artiklar eller delar av dessa EU-BCR som rör interna mekanismer som har genomförts på deltagande företag eller Amgen-koncernen, såsom information om utbildning (inbegripet bilaga 2), granskningsprogram, interna nätverk och struktur för efterlevnad och mekanismen för uppdatering av EU-BCR.

- 18.3. Amgen France påtar sig ansvar för och samtycker till att vidta sådana åtgärder som rimligen är nödvändiga för att åtgärda handlingar av deltagande företag som är etablerade utanför EES. Amgen France ska betala ersättning för materiella eller icke-materiella skador till följd av överträdelse av dessa EU-BCR, såvida det inte kan påvisa att det deltagande företag som är etablerat utanför EES inte är ansvarigt för den händelse som har gett upphov till skadan. Amgen France har tillräckliga ekonomiska medel och försäkringsskydd för att täcka skador enligt EU-BCR.
- 18.4. En registrerad som har lidit skada till följd av att ett deltagande företag som inte är etablerat i EES har överträtt dessa EU-BCR har rätt att, i förekommande fall, få ersättning från Amgen France för den skada som han eller hon har åsamkats och domstolar eller andra behöriga myndigheter i EES ska ha jurisdiktion. Den registrerade ska ha rättigheter och rättsmedel gentemot Amgen France som om överträdelsen hade orsakats av Amgen France i EU i stället för av det deltagande företag som inte är etablerat i EES. Om det deltagande företag som inte är etablerat i EES är ansvarigt eller ställs till svars för en sådan överträdelse ska det i den mån det är ansvarigt eller skyldigt hålla Amgen France skadeslöst mot kostnader, avgifter, skador, utgifter eller förluster som Amgen France ådrar sig i samband med en sådan överträdelse.
- 18.5. Om en registrerad påstår att han eller hon har lidit skada och fastställt att skadan sannolikt har uppstått på grund av en överträdelse av dessa EU-BCR ska bevisbördan för att påvisa att skadan, som den registrerade har ådragit sig på grund av en överträdelse av dessa EU-BCR, inte kan hänföras till det relevanta deltagande företaget ligga hos Amgen France. Om Amgen France kan påvisa att det deltagande företag som är etablerat utanför EES inte är ansvarigt för den händelse som har gett upphov till skadan ska det inte hållas skyldigt eller ansvarigt för skadan.

## **19. Ömsesidigt bistånd och samarbete med dataskyddsmyndigheter**

- 19.1. Deltagande företag ska samarbeta och hjälpa varandra för att hantera en begäran eller ett klagomål från en registrerad eller en utredning eller en förfrågan från den behöriga dataskyddsmyndigheten.
- 19.2. Deltagande företag ska, i samarbete med den integritetsansvarige, besvara EU-BCR-relaterade begäranden från den behöriga dataskyddsmyndigheten inom en lämplig tidsram med hänsyn till omständigheterna kring begäran (och oavsett inte senare än någon tidsfrist som har ålagts av den behöriga dataskyddsmyndigheten) och lämna lämpliga detaljer baserat på den information som rimligen är tillgänglig för det deltagande företaget. I samband med genomförandet och den pågående tillämpningen av EU-BCR ska deltagande företag ta vederbörlig hänsyn till den behöriga dataskyddsmyndighetens kommunikation och rekommendationer och följa alla formella beslut eller meddelanden som utfärdas av den behöriga dataskyddsmyndigheten.
- 19.3. En tvist som rör en behörig dataskyddsmyndighets utövande av övervakning av efterlevnaden av dessa EU-BCR löses av domstolen i den dataskyddsmyndighetens medlemsstat, i enlighet med den medlemsstatens gällande lagstiftning.

## **20. Uppdateringar och ändringar av EU-BCR**

- 20.1. Amgen förbehåller sig rätten att när som helst ändra eller uppdatera dessa EU-BCR. En sådan uppdatering av EU-BCR kan specifikt vara nödvändig till följd av nya rättsliga krav, betydande

förändringar av strukturen i Amgen-koncernen eller officiella krav som ställs av den behöriga dataskyddsmyndigheten.

- 20.2. Amgen ska omgående och utan onödigt dröjsmål rapportera väsentliga ändringar av EU-BCR eller förteckningen över deltagande företag till alla andra deltagande företag och till den behöriga dataskyddsmyndigheten för att beakta ändringar av den gällande lagstiftningen, regelverket eller Amgen-koncernstrukturen. I synnerhet när en ändring skulle påverka skyddsnivån som ges av EU-BCR ska den integritetsansvarige omgående meddela en sådan ändring i förväg till den behöriga dataskyddsmyndigheten med en kort förklaring av skälen till ändringen. Vissa ändringar kan kräva ett nytt godkännande av den behöriga dataskyddsmyndigheten.
- 20.3. Den integritetsansvarige ska föra en fullständig uppdaterad förteckning över de deltagande företagen i EU-BCR och följa eventuella uppdateringar av reglerna samt på begäran tillhandahålla nödvändig information till de registrerade eller den behöriga dataskyddsmyndigheten. Administrativa ändringar av EU-BCR rapporteras regelbundet till deltagande företag.
- 20.4. Ingen överföring av personuppgifter görs till ett nytt deltagande företag enligt garantierna från EU-BCR förrän det nya deltagande företaget är bundet av EU-BCR och i överensstämmelse med EU-BCR.
- 20.5. Administrativa ändringar av EU-BCR eller förteckningen över deltagande företag rapporteras regelbundet till de deltagande företagen och rapporteras minst en gång om året till den behöriga dataskyddsmyndigheten med en kort förklaring av skälen till uppdateringen.
- 20.6. Väsentliga ändringar av EU-BCR meddelas också på något sätt till de registrerade enligt artikel 7 i EU-BCR.

## **21. Förhållande mellan nationell lagstiftning och EU-BCR**

- 21.1. Om de lokala nationella lagarna som gäller ett deltagande företag kräver en högre skyddsnivå för personuppgifter har de företrädare framför EU-BCR. Om de lokala nationella lagarna som gäller ett deltagande företag ger en lägre skyddsnivå för personuppgifter än EU-BCR är det EU-BCR som gäller.
- 21.2. Om skyldigheter som härrör från de lokala nationella lagarna som gäller ett deltagande företag är i konflikt med EU-BCR ska det deltagande företaget utan onödigt dröjsmål informera den integritetsansvarige och följa de ytterligare krav som anges i artikel 16 ovan.
- 21.3. Under alla omständigheter ska personuppgifter behandlas i enlighet med artikel 5 i GDPR och relevant lokal lagstiftning.

## **22. Slutbestämmelser**

- 22.1. EU-BCR ska träda i kraft efter godkännande av den behöriga dataskyddsmyndigheten och gälla de deltagande företagen vid undertecknandet av EU-BCR-antagandeavtalet.
- 22.2. Ingen överföring ska göras till ett deltagande företag som inte är bundet av dessa EU-BCR. Om en uppgiftsinförare slutar att vara bunden av EU-BCR måste den omgående återlämna eller radera alla personuppgifter (inbegripet kopior därav) som har överförts enligt dessa EU-BCR, förutom om uppgiftsinföraren tillhandahåller juridiskt bindande skyldigheter att

upprätthålla skyddet av personuppgifterna i enlighet med kapitel V i GDPR, i vilket fall den kan lagra personuppgifter som har överförts enligt dessa EU-BCR.

- 22.3. Uppgiftsinföraren måste omgående informera uppgiftsutföraren, Amgen France och den integritetsansvarige om den av någon anledning inte kan följa dessa EU-BCR (inbegripet de situationer som beskrivs i artikel 12.3 ovan). Om uppgiftsinföraren bryter mot dessa EU-BCR eller inte kan följa dem måste uppgiftsutföraren meddela den integritetsansvarige och avbryta överföringen av personuppgifter.
- 22.4. Beroende på vad uppgiftsutföraren väljer måste uppgiftsinföraren omgående återlämna eller radera alla personuppgifter (inklusive kopior därav) som har överförts enligt dessa EU-BCR, och uppgiftsinföraren ska intyga detsamma till uppgiftsutföraren om
  - 22.4.1. uppgiftsutföraren har avbrutit överföringen av personuppgifter, och efterlevnad av dessa EU-BCR inte återställs inom rimlig tid, och i alla händelser inom en månad efter avbrytandet
  - 22.4.2. uppgiftsinföraren överträder kraven i dessa EU-BCR på ett väsentligt sätt
  - 22.4.3. uppgiftsinföraren inte följer ett bindande beslut från en behörig domstol eller behörig dataskyddsmyndighet gällande dess skyldigheter enligt dessa EU-BCR.

Tills personuppgifterna har raderats eller återlämnats måste uppgiftsinföraren fortsätta att säkerställa efterlevnad av dessa EU-BCR. Om lokala nationella lagar som gäller uppgiftsinföraren förbjuder återlämnande eller radering av de personuppgifter som har överförts enligt dessa EU-BCR måste uppgiftsinföraren fortsätta att säkerställa efterlevnad av dessa EU-BCR och endast behandla personuppgifterna i den utsträckning och så länge som krävs enligt sådana lokala nationella lagar.

## **23. Bilagor**

De bifogade bilagorna är integrerade delar av EU-BCR.

Bilaga 1: Översikt över Amgen-dataflöden

Bilaga 2: Översikt över Amgen-utbildningsprogrammet

**Bilaga 1: Översikt över Amgen-dataflöden**

Registrerade	Kategorier av uppgifter	Ändamål	Överföring
Anställd	<p>Identifieringsuppgifter som namn, adress, födelsedatum och födelseort, anställningsdatum, personnummer, kreditkortsnummer, bankkonto och finansiell information samt körkorts- och myndighetsutfärdade ID-kortnummer</p> <p>Semester och förmåner, klagomål, bonusar, befordringar, granskningar och utvärderingar, arbetsregister, information om sjukförsäkring och socialförsäkring, pensionsplan och information om aktieoptioner</p> <p>Skattemässiga och finansiella personuppgifter</p> <p>Känsliga uppgifter som nationellt ursprung, om det är tillåtet enligt lokal lagstiftning</p>	<p>Personallednings-, IT-support- och administrationsändamål i samband med anställningsförhållandet och -förmånerna, eller administration av förmåner efter avslutad anställning samt att följa Amgens juridiska, administrativa och företagsrelaterade skyldigheter</p>	<p>Amgens globala databaser finns i USA där Amgen Inc. har sitt huvudkontor.</p> <p>Data flödar från Amgen France (eller relevant uppgiftsutförare) till Amgen Inc. i USA eller till deltagande företag i Schweiz. Sedan kan uppgifterna</p> <ul style="list-style-type: none"> <li>- lagras där</li> <li>- analyseras i syfte att få fram global statistik och rapporter</li> <li>- delas vidare inom Amgen-koncernen till andra deltagande företag om det finns ett verksamhetsbehov för sådan åtkomst av specifik personal eller verksamhetsfunktioner på de deltagande företagen (till exempel en anställd som söker ett jobb utanför landet eller måste rapportera till en chef som är baserad utanför landet). I de flesta fall agerar sådana deltagande företag även personuppgiftsansvariga, men beroende på</li> </ul>
Vårdpersonal	<p>Namn och verksamhetskontaktuppgifter inbegripet telefonnummer, e-postadress och expertområde</p> <p>Yrkesbakgrund (CV)</p> <p>Deltagande i annan forskning</p> <p>Finansiell information (fakturerings- och betalningsinformation)</p>	<p>Administration och ledning av Amgens yrkesmässiga och vetenskapliga aktiviteter – forskning och utveckling (till exempel deltagande i medicinsk forskning, kliniska studier, yrkesmässiga möten eller kongresser)</p> <p>Främjande av Amgens produkter och tjänster</p> <p>Offentliggörande av finansiell information om det krävs enligt gällande lagstiftning eller efterlevnad av branschkod</p> <p>Regelefterlevnad såsom säkerhetsövervakning och rapportering av biverkningar</p>	

Säljare/leverantörer	Personens namn, organisationens namn och verksamhetskontaktuppgifter  Fakturerings- och betalningsinformation	Behandling av betalningar till säljare och leverantörer  Regulatorisk efterlevnad, till exempel skatteregler	verksamhetsbehovet kan deltagande företag även agera personuppgiftsbiträden (till exempel när de tillhandahåller IT-support eller support relaterad till personalservicecentret).
Försökspersoner i kliniska prövningar (vilket kan vara barn under 18 år om en pediatrik patient är inblandad i en klinisk studie som sponsras av Amgen).	Kodade data – patientnamn och kontaktuppgifter ersätts av ett internt genererat identifikationsnummer. Endast på den kliniska prövningens plats (sjukhuset/forskningsplatsen) finns förteckningen för att knyta identifikationsnumret tillbaka till patientens namn.  Indirekta identifierare såsom födelseår eller födelsedatum (fullständigt födelsedatum samlas bara in för pediatrika studier), kön, vikt och längd.  Nödvändiga hälsorelaterade uppgifter enligt beskrivningen i forskningsstudieprotokollet.  Andra uppgifter om patienten som är nödvändiga för genomförandet av forskningen inbegripet etnicitet, familjesituation (såsom antal barn), konsumtion av droger, alkohol, läkemedel, vanor eller beteenden, yrkessituation såsom jobb, arbetslöshet och deltagande i andra forskning.	Administration och ledning av biomedicinsk forskning (kliniska prövningar och observationsstudier)	
Patienter (vilket kan vara barn under 18 år om det finns en biverkning som involverar användning av ett Amgen-läkemedel)	Indirekta identifierare för patienten såsom ålder, födelseår eller födelsedatum, patientens initialer (enligt lokal lag), kön, vikt/längd eller patientens identifikationsnummer (exklusive nationella hälsorelaterade identifierare).	Regelefterlevnad och farmakovigilans såsom säkerhetsövervakning och rapportering av biverkningar (om det är tillåtet enligt lokal lagstiftning)	



<p>med en pediatrik indikation).</p>	<p>Uppgifter om identifieringen av Amgen-läkemedlet, såsom vilket läkemedel eller vilken enhet som används, enheters serienummer, läkemedlets tillförselmetod eller dosering och läkemedlets parti- och tillverkningsattsnummer.</p> <p>Hälsorelaterade uppgifter såsom administrerade behandlingar, resultat av undersökningar, information om eventuella biverkningar, medicinsk historik för patienten eller patientens familj, associerade sjukdomar eller händelser, riskfaktorer och information om förskrivning och användning av läkemedel och om yrkesuppförandet hos vårdpersonal som är inblandade i behandlingen av patientens sjukdom.</p> <p>Andra uppgifter om patienten som är nödvändiga för bedömningen av den negativa hälsohändelsen i enlighet med regelefterlevnadskrav såsom etnicitet, yrkesliv, konsumtion av droger, alkohol och läkemedel och vanor eller beteenden.</p>		
--------------------------------------	---	--	--

## **Bilaga 2: Översikt över Amgen-utbildningsprogrammet**

### ***Utbildnings- och medvetenhetsprogram för integritets- och dataskydd***

Syftet med utbildningsprogrammet för integritets- och dataskydd är att säkerställa att all Amgen-personal får ordentlig utbildning i Amgens EU-BCR och rättsliga skyldigheter som påverkar behandlingen av personuppgifter. Programmet består av olika delar.

#### **Allmän utbildning för all Amgen-personal**

All Amgen-personal måste genomföra en årlig onlineutbildning om dataskydd som en del av uppförandekodsutbildningen. Utbildningen är obligatorisk och övervakad och tar vanligtvis cirka 75 minuter att genomföra. Utbildningen innehåller även information EU-BCR och om konsekvenserna enligt straff- och arbetsrätt eller deras tjänsteavtal för personal som bryter mot EU-BCR.

#### **Särskild utbildning för dataskyddsombud**

Alla Amgen-dataskyddsombud utbildas regelbundet i nya processer genom regelbundna dataskyddsombudssamtal som utförs av teamet för global integritetsefterlevnad och integritetsworkshoppar på plats eller online på behovsbasis. Alla dataskyddsombud har tillgång till en wikisida med svar på de vanligaste frågorna, vägledning och länkar till externa resurser.

#### **Särskild utbildning för personal**

Särskild utbildning kan ges på behovsbasis online eller på plats eller genom att information läggs ut på Amgens intranät. Utbildningen kan vara inriktad på specifika grupper, till exempel personer som behandlar personuppgifter dagligen eller personer som hjälper andra grupper som behandlar personuppgifter. Till exempel utbildas granskningsgruppen, FoU-funktionerna och den rättsliga avdelningen regelbundet. När det är relevant för specifik personal får de information om rutiner för hantering av begäranden om tillgång till personuppgifter från offentliga myndigheter. Utbildningen kan ske på regional nivå eller på landsnivå. Ytterligare specifik EU-BCR-utbildning kan tas fram på behovsbasis.

#### **Medvetenhet**

Amgen har en särskild sida på intranätet om integritets- och dataskydd med länkar till andra resurser, antingen internt eller externt.

Amgens team för global integritetsefterlevnad samarbetar med informationssäkerhetsavdelningen med Sentinel-programmet, som är ett globalt program för att öka medvetenheten hos Amgen-personal om informationssäkerhet.

#### **Utbildningsstöd**

Alla integritetsrelaterade utbildningar har tagits fram av teamet för global integritetsefterlevnad och godkänts av den integritetsansvarige. Utbildningen kan antingen utföras direkt av en medlem i teamet för global integritetsefterlevnad eller av ett lokalt dataskyddsombud enligt en "utbildning av utbildare-modell".