Amgen EU Binding Corporate Rules – Controller (EU BCR'er)

Sidst opdateret: 12. december 2023

Introduktion

(A) Amgen er en bioteknologisk leder forpligtet til at betjene patienter med alvorlig sygdom. Disse bindende EU-virksomhedsregler – registeransvarlig (" **EU BCR'er** ") udtrykker Amgens forpligtelse til privatliv og databeskyttelse, da den stræber efter at yde tilstrækkelig beskyttelse til overførsler og behandling af personoplysninger mellem deltagende virksomheder.

(B) Alle deltagende virksomheder og alt personale er forpligtet til at respektere og er juridisk bundet af disse EU BCR'er med hensyn til personoplysninger inden for EU's BCR's anvendelsesområde. Manglende overholdelse kan føre til disciplinære sanktioner, som tilladt i henhold til lokal lovgivning. Chief Compliance Officer sikrer i samarbejde med Chief Privacy Officer, at EU's BCR'er håndhæves. En liste over deltagende virksomheder kan findes her: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies. pdf . Alle deltagende virksomheder kan kontaktes på privacy@amgen.com for ethvert spørgsmål vedrørende disse EU BCR'er.

(C) Disse EU BCR'er er blevet vedtaget med henvisning til EU's databeskyttelseslove. Amgen France er ansvarlig for at sikre, at de deltagende virksomheder overholder disse EU BCR'er. Enkeltpersoner kan håndhæve disse EU BCR'er over for Amgen France som en tredjepartsbegunstiget som beskrevet nedenfor. Disse EU BCR'er er tilgængelige på Amgens websted: www.amgen.com/bcr . Alternativt kan du kontakte Amgen på privacy@amgen.com for at anmode om en kopi.

1. Omfang

1.1. Amgen EU BCR'er gælder for overførsler og behandling, automatiseret eller manuel, af alle personoplysninger om registrerede, udført af en deltagende virksomhed, der fungerer som dataansvarlig eller fungerer som databehandler for en anden deltagende virksomhed, der fungerer som dataansvarlig i et af følgende tilfælde:

1.1.1. den deltagende virksomhed, der behandler personoplysningerne, er etableret i EU; eller

1.1.2. den deltagende virksomhed, der behandler personoplysningerne, ikke er etableret i EØS og har modtaget personoplysningerne fra en deltagende virksomhed etableret i EØS ; eller

1.1.3. til videre overførsel af personlige data fra dataimportører til dataimportører.

1.2. En oversigt over datastrømmene i henhold til disse EU BCR'er findes i bilag 1.

2. Definitioner

Betingelser	*Definitioner*
Amgen Frankrig	Amgen SAS, et selskab stiftet i Frankrig, hvis registrerede hjemsted er 25 quai du Président Paul Doumer, 92400 Courbevoie.
Gældende lov	EU-lovgivningen og/eller (hvis relevant) den nationale eller lokale lovgivning i EØS-medlemsstaterne (herunder uden begrænsning EU's databeskyttelseslove).
Overholdelsesleder	En person i Healthcare Compliance-afdelingen i Worldwide Compliance and Business Ethics-afdelingen hos en deltagende virksomhed, som har uddelegeret ansvar for databeskyttelse og privatliv og, hvor det er forskelligt fra den lokale databeskyttelsesansvarlige, støtter den lokale databeskyttelsesansvarlige med dennes ansvar og opgaver .
Samtykke	Enhver frit givet specifik, informeret og utvetydig indikation af en registrerets ønsker, hvorved den registrerede ved en erklæring eller ved en klar bekræftende handling tilkendegiver sin accept af behandlingen af personoplysninger vedrørende ham/hende.
Dataansvarlig	Enhver enhed, der træffer beslutninger med hensyn til indsamling og behandling af personoplysninger, herunder beslutninger om formålene med og måden, hvorpå personoplysninger behandles.
Dataeksportør	En deltagende virksomhed, der opererer som dataansvarlig etableret i EØS, og som overfører personoplysninger til en dataimportør.
Dataimportør	En deltagende virksomhed, som ikke er etableret i EØS, som enten (a) modtager personoplysninger fra en dataeksportør eller (b) modtager en videre overførsel af personoplysninger i henhold til artikel 1(c) i disse EU-BCR'er.
Databehandler	En person eller enhed, der behandler personoplysninger på vegne af en dataansvarlig.
Databeskyttelsesmyndigheden (DPA)	En uafhængig offentlig databeskyttelsesmyndighed etableret af en EØS-medlemsstat.
Databeskyttelsesansvarlig	En person, der er blevet udpeget af Amgens Chief Privacy Officer som ansvarlig for tilsynet med privatliv og databeskyttelse på lokalt niveau samt implementering af passende og påkrævede kontroller.
Datasubjekt	En fysisk person, der kan identificeres, direkte eller indirekte, ved henvisning til persondata. Et registreret emne kan være (uden begrænsning): • en patient/datasubjekt i kliniske forsøg (som kan omfatte

Betingelser	*Definitioner*
	et barn under 18 år) • en sundhedsperson • en ansat • en leverandør eller leverandør
EØS	Den Europæiske Unions medlemslande (Østrig, Belgien, Bulgarien, Kroatien, Republikken Cypern, Tjekkiet, Danmark, Estland, Finland, Frankrig, Tyskland, Grækenland, Ungarn, Irland, Italien, Letland, Litauen, Luxembourg, Malta, Holland , Polen, Portugal, Rumænien, Slovakiet, Slovenien, Spanien og Sverige) og Island, Liechtenstein og Norge (alle er " **EØS-medlemsstater** ").
EU's databeskyttelseslove	GDPR og (hvis relevant) den lokale eller nationale lovgivning vedrørende databeskyttelse og behandling af personoplysninger og implementering af GDPR i en relevant EØS-medlemsstat.
GDPR	Den generelle databeskyttelsesforordning ((EU) 2016/679).
Deltagende virksomhed	En juridisk enhed fra Amgen-gruppen, der er bundet af EU's BCR'er.
Personlig data	Enhver information relateret til en registreret, såsom et navn, et identifikationsnummer, lokaliseringsdata, en online identifikator eller til en eller flere faktorer, der er specifikke for eller oplysninger, der vedrører den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sociale identitet af den fysiske person. Eksempler på personlige data kan omfatte følgende: • En registrerets navn, adresse, cpr-nummer, kørekortnummer, finansielle kontooplysninger, familieoplysninger eller medicinske data, • Navnet, faglig uddannelse og ordinationspraksis for en sundhedsperson, • E-mailadressen og andre identificerende oplysninger, der er givet af en person, der besøger et Amgen-websted. Ovenstående liste er kun vejledende og ikke udtømmende.
Brud på persondatasikkerheden	Ethvert brud på sikkerheden, der fører til utilsigtet eller ulovlig ødelæggelse, tab, ændring, uautoriseret videregivelse af eller adgang til, transmitterede, lagrede eller på anden måde behandlede personlige data.
Personale	Alle medarbejdere og kontingentarbejdere (inklusive konsulenter, vikarer og kontraktansatte) i enhver deltagende virksomhed.

Betingelser	*Definitioner*
Forarbejdning	Enhver operation eller et sæt af operationer, der udføres på personlige data (eller sæt af personlige data), uanset om det sker ved hjælp af automatiserede midler, såsom indsamling, registrering, organisering, strukturering, opbevaring, tilpasning eller ændring, genfinding, konsultation, brug, videregivelse ved transmission, spredning eller på anden måde tilgængeliggørelse, tilpasning eller kombination, begrænsning, sletning eller ødelæggelse .
Følsomme personoplysninger	Personoplysninger, der afslører race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger eller fagforeningsmedlemskab, og behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, data vedrørende helbred eller data vedrørende en fysisk persons køn liv eller seksuel orientering. Separat til EU's databeskyttelseslove betragter Amgen også finansielle oplysninger og oplysninger, der kan bruges til at begå identitetstyveri (f.eks. CPR-nummer, kørekortnummer, kreditkort- eller andre bankkontooplysninger) som følsomme personlige data.
Tekniske og organisatoriske sikkerhedsforanstaltninger	Teknologiske og organisatoriske foranstaltninger rettet mod at beskytte personoplysninger mod hændelig eller ulovlig ødelæggelse eller utilsigtet tab, ændring, uautoriseret videregivelse eller adgang, især hvor behandlingen involverer transmission af data over et netværk og mod alle andre ulovlige former for behandling.
Tredje part	En fysisk eller juridisk person, offentlig myndighed, agentur eller ethvert andet organ end den registrerede, den deltagende virksomhed, der fungerer som dataansvarlig, og en deltagende virksomhed, der fungerer som databehandler. Hos Amgen betragtes en leverandør som en tredjepart. Afhængigt af omstændighederne kan en tredjepart fungere som dataansvarlig eller databehandler i forhold til behandling af personoplysninger.
Sælger	Enhver fysisk eller juridisk person, virksomhed eller organisation, der leverer varer og/eller tjenester til en deltagende virksomhed i henhold til et kontraktforhold og/eller modtager personoplysninger fra en sådan deltagende virksomhed med henblik på at levere disse varer og/eller tjenester.

Amgen skal fortolke vilkårene i disse EU BCR'er i overensstemmelse med EU's databeskyttelseslove.

3. Formålsbegrænsning

3.1. Personoplysninger skal behandles til eksplicitte, specificerede og legitime formål i henhold til artikel 5(1)(b) i GDPR.

3.2. Personoplysninger vil ikke blive behandlet på måder, der er uforenelige med de legitime formål, som personoplysningerne blev indsamlet til, eller gældende lov. Dataimportører er forpligtet til at overholde originale formål, når de opbevarer og/eller viderebehandler personoplysninger eller behandler personoplysninger, der er overført til dem af en anden deltagende virksomhed. Formålet med behandling af personoplysninger kan kun ændres med samtykke fra den registrerede eller i det omfang, det er tilladt i henhold til gældende lov.

3.3. Følsomme personoplysninger vil blive forsynet med yderligere sikkerhedsforanstaltninger, som f.eks. EU's databeskyttelseslove.

4. Datakvalitet og proportionalitet

4.1. Personoplysninger skal være nøjagtige og, hvor det er nødvendigt, holdes ajourført; der skal tages ethvert rimeligt skridt for at sikre, at personlige data, der er unøjagtige i forhold til de formål, hvortil de behandles, slettes eller rettes uden forsinkelse.

4.2. Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles, i henhold til artikel 5(1)(c) i GDPR.

4.3. Behandlingen af personoplysninger vil være styret af målet om at begrænse indsamling, behandling og/eller brug af personoplysninger til kun det, der er nødvendigt, dvs. så få personoplysninger som muligt. Muligheden for anonyme eller pseudonyme data skal overvejes, forudsat at omkostningerne og indsatsen står mål med det ønskede formål.

4.4. Personlige data, som ikke længere er nødvendige til det forretningsformål, hvortil de oprindeligt blev indsamlet og opbevaret, skal slettes i henhold til Amgens Record Retention Schedule. I tilfælde af at lovbestemte opbevaringsperioder eller juridiske tilbageholdelser gælder, vil dataene blive blokeret i stedet for at blive slettet. Ved udløbet af opbevaringsperioden eller den juridiske tilbageholdelse vil dataene blive slettet.

5. Retsgrundlag for behandling af personoplysninger

5.1. Behandling af personoplysninger er kun tilladt, hvis mindst én af følgende forudsætninger er opfyldt:

5.1.1. Den registrerede har givet sit samtykke til behandling af hans eller hendes personoplysninger til et eller flere specifikke formål.

5.1.2. Behandlingen er nødvendig for opfyldelse af en kontrakt, som den registrerede er part i, eller for at tage skridt på anmodning fra den registrerede forud for indgåelse af en kontrakt.

5.1.3. Behandlingen er nødvendig for at overholde en juridisk forpligtelse, som den dataansvarlige er underlagt i henhold til gældende lov.

5.1.4. Behandlingen er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser, såsom liv, sundhed eller sikkerhed.

5.1.5. Behandlingen er nødvendig for udførelsen af en opgave, der udføres i offentlighedens interesse eller under udøvelsen af offentlig myndighed, der er tillagt den dataansvarlige.

5.1.6. Behandlingen er nødvendig af hensyn til de legitime interesser, der forfølges af den dataansvarlige eller af en tredjepart, undtagen hvor sådanne interesser tilsidesættes af den registreredes interesser eller grundlæggende rettigheder og friheder.

5.2. Behandling af personoplysninger i forbindelse med straffedomme og lovovertrædelser må kun udføres, når behandlingen er godkendt i henhold til gældende lov, der giver passende garantier for de registreredes rettigheder og friheder.

6. Behandling af følsomme personoplysninger

6.1. Hvis den deltagende virksomhed i henhold til et specifikt og legitimt formål skal behandle følsomme personoplysninger, vil den deltagende virksomhed kun gøre det, hvis:

6.1.1. Den registrerede har givet udtrykkeligt samtykke til behandling af disse følsomme personoplysninger til et eller flere specificerede formål, undtagen hvor gældende lov bestemmer, at forbuddet i artikel 9, stk. 1, i GDPR ikke må ophæves af den registrerede.

6.1.2. Behandlingen er nødvendig med henblik på at varetage den dataansvarliges forpligtelser og specifikke rettigheder inden for ansættelses- og socialsikrings- og socialbeskyttelseslovgivningen, i det omfang det er tilladt i henhold til gældende lov eller ved en kollektiv overenskomst i henhold til gældende lov. sørger for passende garantier for den registreredes grundlæggende rettigheder og interesser.

6.1.3. Behandlingen er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser, hvor den registrerede er fysisk eller juridisk ude af stand til at give sit samtykke.

6.1.4. Behandlingen udføres som led i dens legitime aktiviteter med passende garantier af en fond, forening eller ethvert andet non-profit-søgende organ med et politisk, filosofisk, religiøst eller fagforeningsmæssigt sigte og på betingelse af, at Behandlingen udelukkende vedrører medlemmerne af organet eller til personer, der har regelmæssig kontakt med det i forbindelse med dets formål, og at oplysningerne ikke videregives uden for dette organ uden de registreredes samtykke.

6.1.5. Behandlingen vedrører følsomme personoplysninger, som åbenlyst er offentliggjort af den registrerede.

6.1.6. Behandlingen af følsomme personoplysninger er nødvendig for at etablere, udøve eller forsvare retskrav.

6.1.7. Behandlingen er nødvendig af hensyn til væsentlige offentlige interesser, på grundlag af gældende lov, som skal stå i rimeligt forhold til det forfulgte mål, respektere essensen af retten til databeskyttelse og sørge for passende og

specifikke foranstaltninger til at beskytte de grundlæggende rettigheder og interesser af den registrerede.

6.1.8. Behandlingen af de følsomme personoplysninger er påkrævet til forebyggende eller arbejdsmedicinske formål, til vurdering af medarbejderens arbejdsevne, medicinsk diagnose, levering af sundheds- eller socialhjælp eller behandling eller styring af sundheds- eller socialsystemer og tjenester på grundlag af gældende lov eller i henhold til kontrakt med en sundhedsprofessionel, og hvor disse følsomme personoplysninger behandles af eller under ansvar af en sundhedsperson, skal en sådan fagperson være underlagt tavshedspligt i henhold til gældende lov eller regler etableret af kompetente organer i en EØS-medlemsstat eller af en anden person, der også er underlagt tavshedspligt i henhold til gældende lov eller regler, der er fastsat af kompetente organer i en EØS-medlemsstat.

6.1.9. Behandlingen af følsomme personoplysninger er nødvendig af hensyn til offentlighedens interesse på folkesundhedsområdet, såsom beskyttelse mod alvorlige grænseoverskridende trusler mod sundheden eller sikring af høje standarder for kvalitet og sikkerhed for sundhedspleje og af lægemidler eller medicinsk udstyr, på grundlag af gældende lov, som giver mulighed for passende og specifikke foranstaltninger til at beskytte den registreredes rettigheder og friheder, især tavshedspligt.

6.1.10. Behandlingen af følsomme personoplysninger er nødvendig til arkiveringsformål i offentlighedens interesse, videnskabelige eller historiske forskningsformål eller statistiske formål i overensstemmelse med artikel 89, stk. 1, i GDPR baseret på gældende lov, som skal stå i forhold til det forfulgte mål, essensen af retten til databeskyttelse og sørge for passende og specifikke foranstaltninger til at beskytte den registreredes grundlæggende rettigheder og interesser.

7. Gennemsigtighed og informationsrettigheder

7.1. Alle deltagende virksomheder skal behandle personoplysninger på en gennemsigtig måde. Amgen er forpligtet til at gøre EU's BCR'er, herunder kontaktoplysninger, let tilgængelige og let tilgængelige for alle registrerede og til at informere de registrerede om overførslen og behandlingen af deres personlige data. Disse EU BCR'er er tilgængelige på Amgens websted: www.amgen.com/bcr . Alternativt kan du kontakte Amgen på privacy@amgen.com for at anmode om en kopi. Amgen vil også bruge forskellige kommunikationsmidler såsom virksomhedswebsteder, herunder interne websteder og nyhedsbreve, kontrakter og specifikke fortrolighedsmeddelelser for at opfylde dette tilgængelighedskrav. Derudover vil Amgen informere de registrerede ved hjælp af disse kommunikationsmidler om eventuelle opdateringer eller ændringer af EU's BCR'er eller listen over deltagende virksomheder uden unødig forsinkelse.

7.2. Registrerede, hvis personoplysninger behandles af en deltagende virksomhed, skal have de oplysninger, der er angivet i artikel 13 og 14 i GDPR.

7.3. Hvis personoplysningerne ikke modtages fra en registreret, gælder forpligtelsen til at informere den registrerede ikke, hvis leveringen af sådanne oplysninger viser sig umulig eller vil medføre en uforholdsmæssig stor indsats, eller hvis registrering eller videregivelse er udtrykkeligt fastsat ved lov.

8. Retten til adgang, berigtigelse, sletning og begrænsning af data

8.1. Enhver registreret har ret til at få en bekræftelse fra den deltagende virksomhed på, om personoplysninger vedrørende ham eller hende behandles eller ej , og, hvor det er tilfældet, adgang til personoplysningerne og de oplysninger, der kræves afgivet i henhold til artikel 15, stk. 1, i GDPR. Opfølgningen på denne anmodning, herunder muligheden for at opkræve et gebyr eller tidsrammen for at besvare en sådan anmodning, vil være underlagt gældende lov og kommunikeret passende til den registrerede, når han/hun indsender sin anmodning.

8.2. Enhver registreret har ret til at få berigtigelse, sletning eller begrænsning af personlige data, især hvor dataene er ufuldstændige eller unøjagtige.

8.3. Enhver registreret har ret til til enhver tid at gøre indsigelse mod behandlingen af deres personoplysninger på et hvilket som helst tidspunkt af grunde relateret til deres særlige situation baseret på udførelsen af en opgave udført i offentlighedens interesse eller den deltagende virksomheds legitime interesser eller en Tredjepart (herunder profilering baseret på disse grunde). Den deltagende virksomhed skal ikke længere behandle personoplysningerne, medmindre den påviser tvingende legitime grunde for behandlingen, som tilsidesætter den registreredes interesser, rettigheder og friheder eller for etablering, udøvelse eller forsvar af retskrav.

8.4. Enhver registreret har ret til (gratis) at gøre indsigelse mod behandlingen af personoplysninger vedrørende ham eller hende med henblik på direkte markedsføring, hvilket omfatter profilering i det omfang, det er relateret til sådan direkte markedsføring. Hvis den registrerede udøver sin ret til at gøre indsigelse mod behandlingen af personoplysninger vedrørende ham eller hende med henblik på direkte markedsføring, skal den deltagende virksomhed ophøre med at behandle personoplysningerne til dette formål.

8.5. Enhver registreret har ret til at modtage meddelelsen til tredjeparter, som personoplysningerne er blevet videregivet til, om enhver berigtigelse, sletning eller begrænsning i henhold til artikel 19 i GDPR.

8.6. Enhver registreret har ret til at kende logikken i enhver automatisk behandling af personoplysninger i henhold til artikel 13(2)(f) i GDPR.

8.7. Hvor behandlingen er baseret på samtykke, har enhver registreret ret til at trække sit samtykke tilbage til enhver tid. Tilbagetrækningen af samtykke påvirker ikke lovligheden af Behandling baseret på samtykke før tilbagetrækningen.

8.8. Enhver registreret har ret til at klage til den deltagende virksomhed vedrørende behandlingen af personoplysninger gennem den interne klagemekanisme, der er fastsat i henhold til artikel 17.

8.9. Enhver anmodning i henhold til denne artikel 8 (eller artikel 9 nedenfor) skal sendes til den deltagende virksomhed på: privacy@amgen.com . Selvom det stærkt opfordres til at fremsætte anmodninger via e-mail, udelukker dette ikke, at en registreret fremsætter en mundtlig anmodning. Den deltagende virksomhed skal informere den registrerede uden forsinkelse om resultatet af deres anmodning og senest inden for en måned efter modtagelsen af anmodningen (herunder, hvor det er relevant, årsagerne til ikke at handle og muligheden for at indgive en klage til den kompetente databeskyttelsesmyndighed og /eller søger en retssag). Denne periode på en måned kan forlænges med yderligere to måneder, hvis det er nødvendigt, under hensyntagen til kompleksiteten og antallet af anmodninger. Den deltagende virksomhed skal informere den registrerede om enhver sådan forlængelse

inden for en måned efter modtagelsen af anmodningen sammen med årsagerne til forsinkelsen. Enhver kommunikation, handling og/eller information givet i forbindelse med en anmodning i henhold til denne artikel 8 (eller artikel 9 nedenfor) skal leveres til den registrerede gratis. Hvis anmodninger fra en registreret er åbenlyst ubegrundede eller overdrevne, især på grund af deres gentagne karakter, kan den deltagende virksomhed enten: (a) opkræve et rimeligt gebyr under hensyntagen til de administrative omkostninger ved at give informationen eller kommunikationen eller udføre den anmodede handling ; eller (b) nægte at reagere på anmodningen. Det deltagende selskab bærer byrden med at påvise anmodningens åbenlyst ubegrundede eller overdrevne karakter.

9. Automatiserede individuelle beslutninger

9.1. Den registrerede har ret til ikke at blive underlagt en afgørelse, der udelukkende er baseret på automatiseret behandling, herunder profilering, som har retsvirkninger for ham eller hende eller på lignende måde påvirker ham eller hende væsentligt, medmindre denne afgørelse:

9.1.1. er nødvendig for at indgå eller udføre en kontrakt mellem den registrerede og den deltagende virksomhed;

9.1.2. er påkrævet eller godkendt af gældende lov, som også fastsætter passende foranstaltninger til at beskytte den registreredes rettigheder og friheder og legitime interesser (herunder i det mindste retten til at opnå menneskelig indgriben fra den deltagende virksomheds side, for at udtrykke hans eller hendes synspunkter og at anfægte afgørelsen); eller

9.1.3. er baseret på den registreredes udtrykkelige samtykke.

10. Sikkerhed og fortrolighed

10.1. Amgen implementerer passende tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte mod og opdage brud på personlige data. Internationale rammer, såsom ISO/IEC 27002, bruges af Amgen til at bestemme disse sikkerhedsforanstaltninger.

10.2. Amgen har processer på plads for at sikre, at brud på persondatasikkerheden er underlagt rapportering, sporing og passende korrigerende handlinger efter behov. Ethvert brud på persondatasikkerheden skal dokumenteres (herunder fakta vedrørende persondatabruddet, dets virkninger og de afhjælpende handlinger, der er truffet), og dokumentationen skal stilles til rådighed for den kompetente databeskyttelsesmyndighed på anmodning. Deltagende virksomheder skal uden unødig forsinkelse underrette ethvert brud på persondatasikkerheden til Amgen France, Chief Privacy Officer og den anden relevante privatlivsansvarlige/funktion og (hvor den deltagende virksomhed, der lider af et brud på persondatasikkerheden, fungerer som databehandler) til den deltagende virksomhed, der handler som Dataansvarlig. Brud på persondatasikkerheden skal i samarbejde med Chief Privacy Officer anmeldes til den kompetente databeskyttelsesmyndighed uden unødig forsinkelse (og hvor det er muligt senest 72 timer efter, at man er blevet opmærksom på databruddet), medmindre det er usandsynligt, at det vil resultere i en risiko for registreredes rettigheder og friheder. Hvor bruddet på persondatasikkerheden sandsynligvis vil resultere i en høj risiko for de registreredes rettigheder og friheder, skal det også meddeles de registrerede uden unødig forsinkelse.

10.3. Informationssikkerhedsrisikovurderinger bruges til at identificere potentielle trusler mod følsomme personoplysninger og implementering af yderligere sikkerhedskontroller efter behov.

10.4. Implementeringen af foranstaltningerne vil tage hensyn til det aktuelle tekniske niveau i henhold til artikel 32 i GDPR.

10.5. Chief Information Security Officer arbejder sammen med Chief Privacy Officer for at sikre sikkerheden og fortroligheden af personlige data.

10.6. De tekniske og organisatoriske sikkerhedsforanstaltninger skal udformes til at implementere databeskyttelsesprincipperne i henhold til artikel 5 i GDPR, databeskyttelse ved design og standardprincipper i henhold til artikel 25 i GDPR og for at lette overholdelse af kravene fastsat af disse EU BCR'er i praksis .

11. Relationer til databehandlere (Amgen-dataimportør eller -leverandør)

11.1. Den deltagende virksomhed (der fungerer som dataansvarlig) vil omhyggeligt vælge en databehandler, som enten kan være en anden deltagende virksomhed eller en leverandør. Databehandleren skal give tilstrækkelige garantier vedrørende deres tekniske og organisatoriske sikkerhedsforanstaltninger for den behandling, der skal udføres, og skal sikre overholdelse af disse foranstaltninger.

11.2. Når outsourcing skønnes nødvendigt efter vurdering af forretningsbehov og risici ved en sådan outsourcing, vil processen med at vælge Databehandleren omfatte en evaluering af privatlivsrisikofaktorer og balancere forretningsbehov mod potentielle risici.

11.3. Den deltagende virksomhed, der optræder som dataansvarlig, vil ved hjælp af skriftlige kontraktlige midler i overensstemmelse med gældende lov (og især kravene i artikel 28(3) i GDPR) instruere databehandleren blandt andet:

11.3.1. Databehandleren handler kun efter instrukser fra den deltagende virksomhed, der fungerer som dataansvarlig, og at behandling af personoplysninger til databehandlerens egne formål eller til formål for en tredjepart er forbudt;

11.3.2. om reglerne vedrørende sikkerhed og fortrolighed, der skal påhvile databehandleren, og at implementere passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der er passende i forhold til risikoen ved behandlingen ;

11.3.3. personer, der er autoriseret til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt ;

11.3.4. Databehandleren må ikke engagere en anden databehandler uden forudgående specifik eller generel skriftlig tilladelse fra den deltagende virksomhed, der fungerer som dataansvarlig, og, hvor en sådan tilladelse er givet, de samme databeskyttelsesforpligtelser som angivet i kontrakten eller anden retsakt mellem Deltagende virksomhed, der fungerer som dataansvarlig og databehandler, skal pålægges denne anden databehandler ;

11.3.5. under hensyntagen til behandlingens karakter skal den bistå den deltagende virksomhed, der fungerer som dataansvarlig, med passende tekniske og

organisatoriske foranstaltninger, så vidt det er muligt, til opfyldelse af den deltagende virksomheds forpligtelse til at reagere på anmodninger om at udøve den registreredes rettigheder ;

11.3.6. den skal bistå den deltagende virksomhed, der fungerer som dataansvarlig, med at sikre overholdelse af forpligtelserne i forbindelse med behandlingssikkerhed, meddelelse om et brud på persondatasikkerheden til den kompetente databeskyttelsesmyndighed, meddelelse af et brud på persondatasikkerheden til den registrerede, vurderinger af databeskyttelseskonsekvenser og forudgående konsultation med den kompetente databeskyttelsesmyndighed under hensyntagen til behandlingens art og de oplysninger, der er tilgængelige for databehandleren ;

11.3.7. efter valg af den deltagende virksomhed, der fungerer som dataansvarlig, skal den slette eller returnere alle personoplysninger til den deltagende virksomhed, der fungerer som dataansvarlig efter afslutningen af leveringen af tjenester i forbindelse med behandlingen, og slette eksisterende kopier, medmindre EU-databeskyttelse Loven kræver opbevaring af personoplysningerne ;

11.3.8. den skal stille alle oplysninger, der er nødvendige for at påvise overholdelse af forpligtelserne i denne artikel 11, til rådighed for den deltagende virksomhed, der fungerer som dataansvarlig, og give mulighed for og bidrage til revisioner, herunder inspektioner, udført af den deltagende virksomhed, der fungerer som dataansvarlig eller en anden revisor bemyndiget af det.

11.4. Den deltagende virksomhed, der fungerer som dataansvarlig, skal sikre, at databehandleren forbliver fuldt ud i overensstemmelse med de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

11.5. Den deltagende virksomhed, der fungerer som dataansvarlig, bevarer ansvaret for legitimiteten af behandlingen og er stadig ansvarlig for den registreredes rettigheder. I det omfang databehandleren er underlagt EU's databeskyttelseslove, er den også ansvarlig for sine forpligtelser og ansvar som databehandler i henhold til sådanne love.

11.6. For at opfylde de kontraktlige forpligtelser , der er angivet i denne artikel om databehandlere, leveres en kontraktlig skabelon med titlen Data Privacy Schedule til brug for deltagende virksomheder, der fungerer som dataansvarlig. Den deltagende virksomhed, der fungerer som dataansvarlig, kan, afhængigt af de specifikke omstændigheder i hver kontraktlig ordning, forhandle andre bestemmelser end dem, der er angivet i databeskyttelsesskemaet, men de kontraktmæssige bestemmelser skal stadig som minimum dække de forpligtelser, der er angivet ovenfor i denne artikel 11.

11.7. Hvert deltagende firma, der fungerer som databehandler, og som er underlagt EU's databeskyttelseslove, skal føre en fortegnelse over alle kategorier af behandlingsaktiviteter, der udføres på vegne af en deltagende virksomhed, der fungerer som dataansvarlig. Denne fortegnelse skal opbevares skriftligt, herunder i elektronisk form, stilles til rådighed for Chief Privacy Officer og den kompetente databeskyttelsesmyndighed på anmodning og skal indeholde følgende oplysninger: (a) navn og kontaktoplysninger på den deltagende virksomhed, der handler som en databehandler og af hver deltagende virksomhed, der fungerer som dataansvarlig, på vegne af hvilken den handler, og, hvor det er relevant, dets repræsentant og DPO; (b) kategorierne af behandling, der udføres på vegne af hver deltagende virksomhed, der fungerer som dataansvarlig; og (c) hvor det er relevant,

overførsler af personoplysninger til et tredjeland eller en international organisation, herunder identifikation af det pågældende tredjeland eller internationale organisation og, i tilfælde af overførsler, der er baseret på en undtagelse i henhold til artikel 49, hvis GDPR, dokumentation af passende sikkerhedsforanstaltninger; og (d) hvor det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

12. Begrænsninger for overførsler og videreoverførsler

12.1. Alle overførsler af personoplysninger, der er underlagt disse EU-BCR'er, til tredjeparter, der befinder sig uden for EØS, skal respektere EU's databeskyttelseslove om overførsler og videre overførsler af personoplysninger, enten ved at gøre brug af standardkontraktklausulerne godkendt i henhold til Kommissionens gennemførelsesbeslutning (EU) af 4. juni 2021 om standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande i henhold til GDPR eller på anden passende måde i henhold til kapitel V i GDPR (herunder, undtagelsesvis, hvis en undtagelse gælder for en specifik situation i henhold til artikel 49 i GDPR).

12.2. Alle overførsler af personoplysninger, der er underlagt disse EU-BCR'er til databehandlere uden for EØS, skal respektere EU's databeskyttelseslove vedrørende databehandlere (og kravene i artikel 11 ovenfor) ud over reglerne om overførsler og videreoverførsler af personoplysninger angivet i denne artikel 12 og i EU's databeskyttelseslove.

12.3. Før overførsel af personoplysninger til en dataimportør eller (i forbindelse med løbende overførsler) før enhver opdateret lokal national lovgivning træder i kraft, skal dataeksportøren i samarbejde med Chief Privacy Officer og Amgen France med bistand fra dataimportøren og under hensyntagen til omstændighederne ved overførslen, vurdere, om lokal national lovgivning vil forhindre dataimportøren i at opfylde sine forpligtelser i henhold til EU's BCR'er, og afgøre, om eventuelle nødvendige supplerende foranstaltninger skal implementeres. En sådan vurdering vil tage hensyn til:

12.3.1. de specifikke omstændigheder ved overførslen (herunder de formål, hvortil personoplysningerne overføres og behandles , typen af enheder, der er involveret i behandlingen, den økonomiske sektor, hvori overførslen finder sted, kategorierne og formatet af de overførte personoplysninger, placeringen af behandlingen (herunder lagring) og de anvendte transmissionskanaler);

12.3.2. love og praksis i bestemmelsestredjelandet, der er relevante i lyset af de specifikke omstændigheder ved overførslen (herunder dem, der kræver videregivelse af data til offentlige myndigheder eller bemyndigelse til adgang fra sådanne myndigheder) og de gældende begrænsninger og sikkerhedsforanstaltninger; og

12.3.3. eventuelle relevante kontraktlige, tekniske eller organisatoriske sikkerhedsforanstaltninger, der er indført i forbindelse med overførslen, herunder foranstaltninger, der anvendes under transmissionen og behandlingen af personoplysningerne i destinationslandet.

Endvidere skal en sådan vurdering være baseret på den forståelse, at love og praksis i bestemmelsestredjelandet respekterer den registreredes grundlæggende rettigheder og friheder og ikke går ud over, hvad der er nødvendigt og forholdsmæssigt i et demokratisk samfund for at sikre et af følgende mål. : (a) national sikkerhed; (b) forsvar; c) offentlig sikkerhed; d) forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og

forebyggelse af trusler mod den offentlige sikkerhed e) andre vigtige mål af almen offentlig interesse, især vigtige økonomiske eller finansielle interesser, herunder monetære, budgetmæssige og skattemæssige anliggender, folkesundhed og social sikring f) beskyttelse af domstolenes uafhængighed og retssager; g) forebyggelse, efterforskning, afsløring og retsforfølgning af brud på etik for lovregulerede erhverv; h) overvågnings-, inspektions- eller reguleringsfunktioner forbundet med udøvelsen af offentlig myndighed i de tilfælde, der er nævnt i de foregående mål; (i) beskyttelsen af den registrerede eller andres rettigheder og friheder; og/eller (j) fuldbyrdelse af civilretlige krav.

Chief Privacy Officer skal gennemgå og godkende den dokumenterede vurdering og eventuelle foreslåede supplerende foranstaltninger. Hvis resultatet af vurderingen viser behovet for at implementere supplerende foranstaltninger, skal dataeksportøren gennemføre disse foranstaltninger. Hvis der ikke kan indføres supplerende foranstaltninger (eller hvis det er instrueret af Chief Privacy Officer eller en kompetent databeskyttelsesmyndighed), skal dataeksportøren suspendere overførslen. Resultatet af vurderingen og foreslåede supplerende foranstaltninger skal registreres og sendes til den kompetente databeskyttelsesmyndighed, hvor det er nødvendigt.

Chief Privacy Officer og Amgen France vil informere alle deltagende virksomheder om den udførte vurdering og om dens resultater, således at de identificerede supplerende foranstaltninger kan anvendes, hvor den samme type overførsler udføres af andre deltagende virksomheder, eller hvor effektive supplerende foranstaltninger ikke kan være på plads, suspenderes eller afsluttes sådanne overførsler.

12.4. Dataimportøren skal straks underrette dataeksportøren, Amgen France og Chief Privacy Officer, hvis den har grund til at tro, at den er eller er blevet underlagt love eller praksis, der ville forhindre den i at opfylde sine forpligtelser i henhold til disse EU BCR'er, herunder efter en ændring i den lokale nationale lovgivning i tredjelandet som beskrevet i artikel 12.3 eller en foranstaltning såsom en anmodning om offentliggørelse som beskrevet i artikel 16.3. Derudover skal dataeksportørerne (i samarbejde med Chief Privacy Officer) løbende og hvor det er relevant med bistand fra dataimportørerne overvåge udviklingen i de tredjelande, som dataeksportørerne har overført personoplysninger til, som kunne negativt påvirke den indledende vurdering af beskyttelsesniveauet for personoplysninger og de beslutninger, der træffes i forbindelse med sådanne overførsler.

12.5. Efter en suspension af en overførsel skal dataeksportøren afslutte overførslen eller sættet af overførsler, hvis dataimportøren ikke er i stand til at overholde EU's BCR'er og/eller overensstemmelsen ikke genoprettes inden for en måned efter suspensionen. I så fald skal Dataimportøren, efter Dataeksportørens valg, enten returnere eller destruere alle Personoplysninger, der er blevet overført før suspensionen, og eventuelle kopier heraf.

12.6. Enhver persondatastrøm, der ikke er underlagt disse EU BCR'er og/eller ikke stammer fra et deltagende selskab etableret i en EØS-medlemsstat, betragtes ikke som en overførsel af personoplysninger i henhold til disse EU BCR'er og er derfor ikke underlagt kravene i disse EU BCR'er.

13. Træningsprogram

13.1. Som beskrevet i bilag 2 tilbyder Amgen alt personale passende og opdateret træning om privatlivsprincipper og mere specifikt om EU's BCR'er. Denne uddannelse omfatter også information om konsekvenserne i henhold til straffe- og ansættelseslovgivningen og/eller deres kontrakt for tjenester til personale, der overtræder EU's BCR'er.

13.2. Uddannelsen er obligatorisk og gentages årligt. Succesfuld deltagelse i træning vil blive dokumenteret.

13.3. Specifikke uddannelser vil blive givet fra sag til sag til personale, der har permanent eller regelmæssig adgang til persondata, eller som er involveret i indsamlingen af persondata eller i udviklingen af værktøjer, der bruges til at behandle persondata.

13.4. Derudover leverer Amgens Global Privacy Compliance Team passende information og ressourcer relateret til privatliv, herunder på Amgens intranetportal.

14. Revision og overvågningsprogram

14.1. Chief Privacy Officer sikrer, at alle deltagende virksomheder (og deres overholdelse af disse EU BCR'er) er inkluderet i revisions- og overvågningsprogrammet ud fra et privatlivs- og databeskyttelsesperspektiv. Omfattende revisioner udføres regelmæssigt, ikke sjældnere end hvert 2. til 3. år (for deltagende virksomheder med en mellem til høj risikoprofil baseret på revisionsafdelingens risikovurderingsmetode) og hvert 4. til 5. år (for deltagende virksomheder med en lav risikoprofil baseret på revisionsafdelingens risikovurderingsmetode) af det interne revisionsteam eller uafhængige, eksterne certificerede revisorer. Omfattende revisioner omfatter databeskyttelse og privatlivsspørgsmål inden for deres omfang (herunder overholdelse af disse EU BCR'er, hvor det er relevant for og bruges af en deltagende virksomhed). Ud over omfattende revisioner, og uden at det berører de tidsrammer, der er angivet ovenfor, udføres andre revisionsomfang, herunder tværfunktionelle eller problemspecifikke revisioner (f.eks. overholdelse af EU's BCR'er), en begrænset revision af en eller flere personlige Databehandlingssystemer og/eller en begrænset revision af en eller flere funktionelle afdelinger (f.eks. Global Privacy Compliance Team). Revisionsprogrammet udvikles og aftales i samarbejde med revisionschefen og Chief Compliance Officer, som er Senior Vice-President. Chief Privacy Officer, Chief Compliance Officer og Chief Information Officer kan til enhver tid iværksætte ad hoc EU BCRs-relaterede revisioner. For eksempel som svar på ethvert identificeret overholdelsesproblem eller en rapport om væsentlig manglende overholdelse, et brud på persondatasikkerheden og/eller en væsentlig ændring af EU's databeskyttelseslove. Revisionsprogrammet dækker alle aspekter af EU's BCR'er, herunder metoder til at sikre, at korrigerende handlinger finder sted .

14.2. Alle EU BCRs revisionsrapporter meddeles til Chief Compliance Officer og Chief Privacy Officer rettidigt. EU BCR's revisionsresuméer og -resultater samt anden relevant information rapporteres også regelmæssigt til bestyrelsen for Amgen Inc. via passende udvalg (f.eks. Corporate Responsibility and Compliance Committee og/eller Revisionskomité i bestyrelsen) for at bestyrelsen for Amgen Frankrig og (hvor det er relevant, f.eks. i forbindelse med en konstatering, der kræver afhjælpning) til den relevante deltagende virksomhed. Corporate Responsibility and Compliance Committee i bestyrelsen for Amgen, Inc. mødes fem gange om året. Privatliv og databeskyttelse dækkes årligt, typisk på oktobermødet.

14.3. Den kompetente databeskyttelsesmyndighed kan efter anmodning modtage en kopi af EU BCRs-relaterede revisionsrapporter.

14.4. Hvert deltagende selskab skal samarbejde med og acceptere uden begrænsninger at blive revideret af den kompetente databeskyttelsesmyndighed. Hver revideret virksomhed skal straks informere Chief Privacy Officer, hvis den modtager meddelelse om en sådan revision, eller en sådan revision finder sted.

15. Compliance og tilsyn med compliance

15.1. Amgen udpeger passende personale, herunder hvor det er relevant et netværk af databeskyttelsesansvarlige, med topledelsesstøtte til at overvåge og sikre overholdelse af databeskyttelsesregler. Chief Privacy Officer er ansvarlig for Global Privacy Compliance Team, som er et globalt team, der yder ekspertsupport over hele verden til Amgen-enheder (inklusive deltagende virksomheder).

15.2. Hos Amgen omfatter Chief Privacy Officers ansvar blandt andet:

15.2.1. rådgivning af bestyrelsen ;

15.2.2. at sikre overholdelse af databeskyttelse på globalt plan (herunder at have det overordnede ansvar for EU's BCR'er);

15.2.3. rapportering regelmæssigt om overholdelse af databeskyttelse (herunder til Chief Compliance Officer); og

15.2.4. arbejder med den kompetente databeskyttelsesmyndigheds undersøgelser.

15.3. Global Privacy Compliance Team omfatter Chief Privacy Officer (som, udover de ansvarsområder, der er nævnt ovenfor, fører tilsyn med det globale netværk af databeskyttelsesansvarlige), den europæiske databeskyttelsesansvarlige og andre lokale databeskyttelsesansvarlige. Global Privacy Compliance Team har det overordnede ansvar for databeskyttelse og overholdelse af privatlivets fred på verdensplan hos Amgen.

15.4. Den europæiske databeskyttelsesrådgiver er blevet udpeget af Amgen som databeskyttelsesansvarlig for EØS, Storbritannien og Schweiz. Den europæiske databeskyttelsesrådgiver har de opgaver, der er beskrevet i artikel 39 i GDPR. Amgen vil sikre, at den europæiske databeskyttelsesansvarliges opgaver og pligter ikke resulterer i en interessekonflikt med sådanne opgaver. Den europæiske databeskyttelsesrådgiver har en direkte rapporteringslinje til Chief Privacy Officer (som er en del af det højeste ledelsesniveau for Amgen) og støttes af den lokale Compliance Lead i Frankrig. Den europæiske databeskyttelsesrådgiver kan kontakte Chief Privacy Officer, hvis der opstår spørgsmål eller problemer under udførelsen af deres opgaver. Den europæiske databeskyttelsesrådgiver kan kontaktes på: privacy@amgen.com

15.5. På lokalt niveau er databeskyttelsesansvarlige ansvarlige for at håndtere lokale anmodninger om privatliv fra registrerede, for at sikre overholdelse på lokalt niveau med støtte fra Global Privacy Compliance Team og for at rapportere større privatlivsproblemer til Chief Privacy Officer. Amgen opretholder et databeskyttelsesansvarlig-netværk og sikrer, at der udpeges eller tildeles en DPO for hvert land, hvor Amgen har en virksomhedsenhed (det deltagende selskab), og den gældende lovgivning i jurisdiktionen for et sådant deltagende selskab kræver en sådan udnævnelse.

15.6. Normalt er databeskyttelsesansvarlige enten, eller støttes af, de lokale compliance-ledere, som rapporterer til afdelingen Worldwide Compliance and Business Ethics. Global Privacy Compliance Team er en del af og rapporterer til afdelingen Worldwide Compliance and Business Ethics, som ledes af Chief Compliance Officer. Chief Compliance Officer har det overordnede ansvar for Amgen-gruppens overholdelse af lov og regulering på verdensplan. Sjældent, på grund af de specifikke forhold i en deltagende virksomhed eller andre særlige

omstændigheder, kan den databeskyttelsesansvarlige komme fra en anden funktion, for eksempel regulatorisk. Under alle omstændigheder sikrer Global Privacy Compliance Team, at databeskyttelsesansvarlige og compliance-ledere er uddannet på passende vis og har et tilstrækkeligt niveau af ledelse og ekspertise til at udføre deres rolle. Derudover har de databeskyttelsesansvarlige en direkte rapporteringslinje til Chief Privacy Officer og understøttes af Global Privacy Compliance Team Personale i tilfælde af, at de har brug for yderligere vejledning.

15.7. Enhver deltagende virksomhed, der fungerer som dataansvarlig, skal være ansvarlig for og være i stand til at påvise overholdelse af EU's BCR'er. Som en del af dette krav skal alle deltagende virksomheder:

15.7.1. skal føre en fortegnelse over alle kategorier af behandlingsaktiviteter, der udføres i overensstemmelse med kravene i artikel 30, stk. 1, i GDPR. Denne fortegnelse skal opbevares skriftligt, herunder i elektronisk form, stilles til rådighed for Chief Privacy Officer og den kompetente databeskyttelsesmyndighed på anmodning og skal indeholde følgende oplysninger: (a) navn og kontaktoplysninger på den deltagende virksomhed, der handler som Dataansvarlig, dennes repræsentant og DPO; (b) formålene med behandlingen; (c) en beskrivelse af kategorierne af registrerede og af kategorierne af personoplysninger; (d) kategorierne af modtagere, som personoplysningerne er blevet eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer; e) hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, herunder identifikation af det pågældende tredjeland eller den internationale organisation og, i tilfælde af overførsler, der bygger på en dispensation, dokumentation for passende sikkerhedsforanstaltninger (f) hvor det er muligt, de påtænkte tidsfrister for sletning af de forskellige kategorier af personoplysninger; og (g) hvor det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

15.7.2. udføre databeskyttelseskonsekvensvurderinger for behandlingsoperationer, der sandsynligvis vil resultere i en høj risiko for fysiske personers rettigheder og friheder i overensstemmelse med artikel 35 i GDPR. Hvis en databeskyttelseskonsekvensvurdering i henhold til artikel 35 indikerer, at behandlingen ville resultere i en høj risiko i mangel af foranstaltninger truffet af den deltagende virksomhed for at mindske risikoen, skal Chief Privacy Officer konsulteres inden behandlingen, som derefter skal rådføre sig med den kompetente databeskyttelsesmyndighed i overensstemmelse med artikel 36 i GDPR.

16. Handlinger i tilfælde af national lovgivning, der forhindrer respekt for EU's BCR'er

16.1. Hvis en deltagende virksomhed har grund til at tro, at den gældende lovgivning forhindrer den deltagende virksomhed i at opfylde sine forpligtelser i henhold til EU BCRs eller har en væsentlig indvirkning på de garantier, som reglerne giver, vil den straks informere Chief Privacy Officer (undtagen hvor forbudt af en retshåndhævende myndighed, såsom et forbud i henhold til straffeloven for at bevare fortroligheden af en retshåndhævende undersøgelse) og Amgen Frankrig.

16.2. Hvor der er konflikt mellem lokal national lovgivning og forpligtelserne i EU's BCR'er, vil Chief Privacy Officer i samarbejde med lokale juridiske rådgivere og den lokale databeskyttelsesansvarlige afgøre, hvilke juridisk passende handlinger der er påkrævet. Om

nødvendigt vil Chief Privacy Officer også rådføre sig med den kompetente databeskyttelsesmyndighed.

16.3. Hvis ethvert lovkrav, som en deltagende virksomhed er underlagt i et tredjeland, sandsynligvis vil have en væsentlig negativ indvirkning på garantierne fra EU's BCR'er, skal Chief Privacy Officer, Amgen France og dataeksportøren straks underrettes af dataene. Importøren og Chief Privacy Officer skal underrette den kompetente databeskyttelsesmyndighed og (hvor muligt) de registrerede. Dette omfatter (a) enhver juridisk bindende anmodning om videregivelse af personoplysningerne fra en retshåndhævende myndighed eller statssikkerhedsorgan, og i et sådant tilfælde bør den kompetente databeskyttelsesmyndighed informeres tydeligt om anmodningen, herunder oplysninger om de anmodede data, anmodende organ og det juridiske grundlag for offentliggørelsen og svaret (medmindre andet er forbudt, såsom et forbud i straffeloven for at bevare fortroligheden af en retshåndhævelsesundersøgelse), og (b) enhver direkte adgang for offentlige myndigheder til personoplysninger overføres i henhold til disse EU BCR'er i overensstemmelse med lovene i bestemmelseslandet, og i sådanne tilfælde skal en sådan meddelelse omfatte alle oplysninger, der er tilgængelige for et sådant deltagende selskab (medmindre andet er forbudt, såsom et forbud i straffelovgivningen for at bevare fortroligheden af en retshåndhævelsesundersøgelse).

16.4. Hvis suspensionen og/eller underretningen i specifikke tilfælde er forbudt, vil den deltagende virksomhed, der modtager anmodningen, gøre sit bedste for at opnå retten til at frafalde dette forbud for at kommunikere så mange oplysninger som muligt og så hurtigt som muligt og være i stand til at påvise (efter anmodning fra dataeksportøren), at den gjorde det.

16.5. Dataimportøren vil med jævne mellemrum give dataeksportøren så mange relevante oplysninger som muligt om de modtagne anmodninger (især antallet af anmodninger, typen af personoplysninger, der anmodes om, identiteten af de anmodende myndigheder, om anmodningerne har blevet udfordret og resultatet af sådanne udfordringer). Dataimportøren vil opbevare sådanne oplysninger, så længe de personlige data er underlagt de sikkerhedsforanstaltninger, som EU's BCR'er giver, og vil efter anmodning stille dem til rådighed for den kompetente databeskyttelsesmyndighed. Hvis Dataimportøren er eller bliver helt eller delvist forbudt at give Dataeksportøren de foregående oplysninger, vil Dataimportøren uden unødig forsinkelse informere Dataeksportøren herom.

16.6. Dataimportøren vil i samarbejde med Chief Privacy Officer gennemgå lovligheden af en anmodning om videregivelse fra en offentlig myndighed for at afgøre, om den falder inden for de beføjelser, der er givet til den anmodende offentlige myndighed. Dataimportøren vil anfægte anmodningen, hvis den efter en sådan vurdering konkluderer (i samarbejde med Chief Privacy Officer), at der er rimelig grund til at antage, at anmodningen er ulovlig i henhold til lovene i bestemmelseslandet, gældende forpligtelser i henhold til international lov, og /eller principper for international comity . Hvis dataimportøren mener, at der er sådanne rimelige grunde til at betragte anmodningen som ulovlig, vil den forfølge mulighederne for at klage. Ved anfægtelse af en anmodning vil dataimportøren søge foreløbige forholdsregler med henblik på at suspendere virkningerne af anmodningen, indtil den kompetente retslige myndighed har taget stilling til sagens realitet. Dataimportøren vil ikke afsløre de anmodede personoplysninger, før det er påkrævet i henhold til gældende lovgivning og procedureregler i bestemmelseslandet. Dataimportøren vil dokumentere sin juridiske vurdering og enhver anfægtelse af anmodningen om offentliggørelse og, i det omfang det er tilladt i henhold til lovgivningen i bestemmelseslandet, stille dokumentationen til rådighed for dataeksportøren og, efter anmodning, for den kompetente databeskyttelsesmyndighed.

16.7. Dataimportøren vil give den mindste tilladte mængde information, når han besvarer en anmodning om videregivelse, baseret på en rimelig fortolkning af anmodningen.

16.8. Under alle omstændigheder må overførsler af personoplysninger fra en deltagende virksomhed til enhver offentlig myndighed ikke være massiv, uforholdsmæssig og vilkårlig på en måde, der går ud over, hvad der er nødvendigt i et demokratisk samfund.

16.9. For deltagende virksomheder beliggende i EØS kan enhver dom fra en domstol og enhver afgørelse truffet af en administrativ myndighed i et tredjeland, der kræver, at en dataansvarlig eller databehandler overfører eller videregiver personoplysninger, kun anerkendes eller håndhæves på nogen måde, hvis de er baseret om en international aftale, såsom en traktat om gensidig retshjælp, der er gældende mellem det anmodende tredjeland og EU eller en EØS-medlemsstat, uden at dette berører andre grunde for overførsel i henhold til kapitel V GDPR.

17. Interne klagemekanismer

17.1. Amgen vil bruge sin eksisterende klagebehandlingsproces til at inkorporere håndtering af alle EU BCRs-relaterede klager eller bekymringer.

17.2. Enhver registreret kan til enhver tid klage over, at enhver deltagende virksomhed ikke overholder EU's BCR'er. Sådanne klager vil blive håndteret af Global Privacy Compliance Team under ledelse af Chief Privacy Officer og i samarbejde med den relevante lokale Data Protection Officer.

17.3. Amgen anbefaler, at sådanne klager leveres skriftligt enten via post eller e-mail direkte til Global Privacy Compliance Team eller til den deltagende virksomhed. Global Privacy Compliance Team kan kontaktes ved at bruge kontaktoplysningerne nedenfor:

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

E-mail : privacy@amgen.com

17.4. Amgen Personale kan l, når det er acceptabelt i henhold til gældende love for den deltagende virksomhed, bruge Business Conduct Hotline til at rapportere en EU BCRs klage.

17.5. Hvis klagen modtages lokalt af den deltagende virksomhed, oversætter DPO'en om nødvendigt og sender den uden unødig forsinkelse til Global Privacy Compliance Team.

17.6. Et første svar vil blive givet til den registrerede inden for ti (10) arbejdsdage, der informerer ham/hende om, at deres klage er under behandling, og at han eller hun vil modtage et væsentligt svar uden unødig forsinkelse og under alle omstændigheder inden for en måned efter modtagelsen af anmodning. Under hensyntagen til kompleksiteten og antallet af anmodningerne kan perioden på en måned forlænges med maksimalt to yderligere måneder, i hvilket tilfælde den registrerede informeres herom. Det materielle svar vil omfatte detaljer om vores resultater og enhver handling, Amgen har eller foreslår at tage. Hvis Amgen beslutter, at der ikke skal foretages nogen handling, skal dette forklares til den registrerede sammen med årsagerne til denne afgørelse.

17.7. Hvis klagen gives medhold af Amgen, vil Amgen implementere passende afhjælpende foranstaltninger. Disse foranstaltninger vil blive besluttet fra sag til sag af Chief Privacy

Officer og Global Privacy Compliance Team, den lokale DPO og, hvor det er relevant, enhver anden relevant afdeling. Desuden, hvis Global Privacy Compliance Team opdager individuelle forseelser, vil passende disciplinære foranstaltninger blive truffet, op til og inklusive opsigelse af ansættelse eller engagement, i det omfang det er tilladt i henhold til gældende lov.

17.8. Den registrerede vil modtage et svar, der informerer ham/hende om resultatet af hans klage. Dette skal ske uden unødig forsinkelse og under alle omstændigheder inden for en måned efter modtagelsen af klagen (med tilstrækkelige detaljer til, at Amgen kan identificere klagens art og, kun hvor det med rimelighed er nødvendigt, med alle oplysninger, der anmodes om for at bekræfte klagerens identitet). Under hensyntagen til kompleksiteten og antallet af anmodningerne kan perioden på en måned forlænges med maksimalt to yderligere måneder, i hvilket tilfælde den registrerede informeres herom.

17.9. Den registrerede vil blive informeret om, at hvis han/hun ikke er tilfreds med Amgens svar, kan han/hun indgive et krav ved domstolene i en EØS-medlemsstat eller den kompetente databeskyttelsesmyndighed. Det er dog ikke et krav, at en registreret først gennemgår Amgens klagebehandlingsproces, før han eller hun kan klage til den kompetente databeskyttelsesmyndighed eller indbringe et krav for domstolene i en EØS-medlemsstat.

17.10. Denne klagebehandlingsproces vil blive offentliggjort gennem offentliggørelsen af EU's BCR'er som nævnt i artikel 7 ovenfor.

18. Tredjeparts begunstigedes rettigheder og ansvar

18.1. En registreret, hvis personoplysninger stammer fra EØS eller er beskyttet af EU's databeskyttelseslove og overføres til deltagende virksomheder uden for EØS, har ret til at håndhæve EU BCR'erne som en tredjepartsbegunstiget og har ret til at søge klageadgang, opnå retsmidler og, hvor det er relevant, kompensation for faktiske skader, der er lidt som følge af brud på disse EU BCR'er. Ethvert sådant krav kan indbringes af den registrerede for en kompetent databeskyttelsesmyndighed (som kan være databeskyttelsesmyndigheden i den EØS-medlemsstat, hvor den registrerede sædvanligvis er bosat, eller databeskyttelsesmyndigheden på hans/hendes arbejdsplads eller databeskyttelsesmyndigheden på stedet for den påståede overtrædelse) . Registrerede kan også indbringe et krav ved en kompetent domstol i en EØS-medlemsstat (som kan være domstolene i den EØS-medlemsstat, hvor den relevante deltagende virksomhed har et forretningssted, eller domstolene i den EØS-medlemsstat, hvor den registrerede har sin/ hendes sædvanlige opholdssted) . En registreret kan være repræsenteret i udøvelsen af sin ret til et effektivt retsmiddel mod en deltagende virksomhed af et non-profit organ, organisation eller forening, forudsat at et sådant organ, organisation eller forening er blevet korrekt oprettet i overensstemmelse med gældende lov , har lovbestemte mål, der er i offentlighedens interesse, og er aktiv inden for beskyttelsen af registreredes rettigheder og friheder i forbindelse med beskyttelsen af deres personoplysninger. Den registrerede skal være i stand til at håndhæve følgende artikler som en tredjepartsbegunstiget :

18.1.1. Artikel 1 (Omfang), 2 (Definitioner), 3 (Formålsbegrænsning), 4 (Datakvalitet og -proportionalitet), 5 (Retsgrundlag for behandling af personoplysninger) og 6 (Behandling af følsomme personoplysninger);

18.1.2. Artikel 7 (gennemsigtighed og informationsrettigheder);

18.1.3. Artikel 8 (Ret til adgang, berigtigelse, sletning og begrænsning af data) og 9 (Automatiske individuelle beslutninger);

18.1.4. Artikel 10 (Sikkerhed og fortrolighed), 11 (Forhold til databehandlere (Amgen-dataimportør eller -leverandør) og 12 (begrænsning af overførsler og videreoverførsler);

18.1.5. Artikel 16 (Handlinger i tilfælde af national lovgivning, der forhindrer respekt for EU's BCR'er) og 21 (Forholdet mellem nationale love og EU's BCR'er);

18.1.6. Artikel 18 (Tredjeparts begunstigedes rettigheder og ansvar); og

18.1.7. Artikel 19 (Gensidig bistand og samarbejde med databeskyttelsesmyndighederne).

18.2. For at undgå tvivl omfatter tredjeparts begunstigede rettigheder ikke de artikler og elementer i disse EU BCR'er, der vedrører interne mekanismer implementeret i de deltagende virksomheder eller Amgen-gruppen, såsom detaljer vedrørende uddannelse (inklusive appendiks 2), revisionsprogrammer, interne overholdelsesnetværk og -struktur og mekanismen til opdatering af EU's BCR'er.

18.3. Amgen France påtager sig ansvaret for og indvilliger i at træffe sådanne foranstaltninger, som med rimelighed er nødvendige for at afhjælpe handlinger fra deltagende virksomheder etableret uden for EØS. Amgen France skal betale kompensation for enhver materiell eller ikke-materiel skade som følge af overtrædelse af disse EU BCR'er, medmindre den kan påvise, at den deltagende virksomhed etableret uden for EØS ikke er ansvarlig for den begivenhed, der giver anledning til skaden. Amgen Frankrig har tilstrækkelige økonomiske midler og forsikringsdækning til at dække skader i henhold til EU's BCR'er.

18.4. Enhver registreret, som har lidt skade som følge af et brud på disse EU BCR'er fra en deltagende virksomhed, der ikke er etableret i EØS, er berettiget til, hvor det er relevant, at modtage kompensation fra Amgen France for den lidte skade og domstolene eller andre kompetente myndigheder i EØS skal have jurisdiktion. Den registrerede skal have rettigheder og retsmidler mod Amgen France, som om overtrædelsen var forårsaget af Amgen France i EU i stedet for den deltagende virksomhed, der ikke er etableret i EØS. Hvis det deltagende selskab, der ikke er etableret i EØS, er ansvarligt eller holdes ansvarligt for et sådant brud, vil det i det omfang, det er ansvarligt eller ansvarligt, holde Amgen France skadesløs for enhver omkostning, afgift, skade, udgift eller tab, som Amgen France pådrager sig i forbindelse med til et sådant brud .

18.5. I tilfælde af en påstand fra en registreret om, at han/hun har lidt skade og har fastslået, at det er sandsynligt, at en sådan skade er opstået på grund af en overtrædelse af disse EU-BCR'er, er bevisbyrden for at vise, at de skader, som den registrerede har lidt på grund af et brud på disse EU BCR'er, som ikke kan tilskrives relevant deltagende virksomhed, påhviler Amgen Frankrig. Hvis Amgen France kan påvise, at den deltagende virksomhed, der er etableret uden for EØS, ikke er ansvarlig for den begivenhed, der giver anledning til skaden, er den ikke ansvarlig eller ansvarlig for skaden.

19. Gensidig bistand og samarbejde med databeskyttelsesmyndighederne

19.1. Deltagende virksomheder skal samarbejde og hjælpe hinanden med at håndtere en anmodning eller klage fra en registreret eller en undersøgelse eller forespørgsel fra den kompetente databeskyttelsesmyndighed.

19.2. Deltagende virksomheder vil i samarbejde med Chief Privacy Officer besvare EU BCRs-relaterede anmodninger fra den kompetente databeskyttelsesmyndighed inden for en passende tidsramme i lyset af omstændighederne omkring anmodningen (og under alle omstændigheder ikke senere end enhver frist pålagt af den kompetente databeskyttelsesmyndighed) og i passende detaljer baseret på de oplysninger, der med rimelighed er tilgængelige for den deltagende virksomhed. I forhold til implementeringen og den løbende anvendelse af EU's BCR'er skal de deltagende virksomheder tage behørigt hensyn til kommunikationen og anbefalingerne fra den kompetente databeskyttelsesmyndighed og overholde alle formelle beslutninger eller meddelelser udstedt af den kompetente databeskyttelsesmyndighed.

19.3. Enhver tvist relateret til en kompetent databeskyttelsesmyndigheds udøvelse af tilsyn med overholdelse af disse EU BCR'er vil blive løst af domstolene i den pågældende databeskyttelsesmyndigheds medlemsstat i overensstemmelse med den pågældende medlemsstats gældende lov.

20. EU BCRs opdatering og ændringer

20.1. Amgen forbeholder sig retten til at ændre og/eller opdatere disse EU BCR'er til enhver tid. En sådan opdatering af EU's BCR'er kan være nødvendig specifikt som følge af nye lovkrav, væsentlige ændringer i Amgen-gruppens struktur eller officielle krav pålagt af den kompetente databeskyttelsesmyndighed.

20.2. Amgen vil omgående og uden unødig forsinkelse rapportere alle væsentlige ændringer i EU's BCR'er eller til listen over deltagende selskaber til alle andre deltagende selskaber og til den kompetente databeskyttelsesmyndighed for at tage hensyn til ændringer af gældende lovgivning, det regulatoriske miljø og/eller Amgen-gruppen struktur. Især hvor en ændring ville påvirke beskyttelsesniveauet, der tilbydes af EU's BCR'er, vil Chief Privacy Officer straks på forhånd meddele en sådan ændring til den kompetente databeskyttelsesmyndighed med en kort forklaring af årsagerne til ændringen. Nogle ændringer kan kræve en ny godkendelse fra den kompetente databeskyttelsesmyndighed.

20.3. Chief Privacy Officer vil føre en fuldt opdateret liste over de deltagende virksomheder af EU's BCR'er og spore eventuelle opdateringer af reglerne samt give de nødvendige oplysninger til de registrerede eller den kompetente databeskyttelsesmyndighed efter anmodning. Alle administrative ændringer af EU's BCR'er vil blive rapporteret til de deltagende virksomheder regelmæssigt.

20.4. Der vil ikke blive overført personoplysninger til en ny deltagende virksomhed under EU BCR'ernes garantier, indtil det nye deltagende selskab er reelt bundet af EU BCR'erne og i overensstemmelse med EU BCR'erne.

20.5. Eventuelle administrative ændringer af EU's BCR'er eller til listen over deltagende virksomheder vil blive rapporteret til de deltagende virksomheder regelmæssigt og rapporteret mindst én gang om året til den kompetente databeskyttelsesmyndighed med en kort forklaring vedrørende årsagerne til opdateringen.

20.6. Væsentlige ændringer af EU BCR'erne vil også blive meddelt de registrerede på enhver måde i henhold til artikel 7 i EU BCR'erne.

21. Forholdet mellem nationale love og EU's BCR'er

21.1. Hvor de lokale nationale love, der gælder for en deltagende virksomhed, kræver et højere niveau af beskyttelse af personoplysninger, vil det have forrang frem for EU's BCR'er. Hvis de lokale nationale love, der gælder for en deltagende virksomhed, giver et lavere beskyttelsesniveau for personoplysninger end EU BCR'erne, vil EU BCR'erne blive anvendt.

21.2. I tilfælde af, at forpligtelser hidrørende fra de lokale nationale love, der gælder for en deltagende virksomhed, er i konflikt med EU's BCR'er, skal den deltagende virksomhed informere Chief Privacy Officer uden unødig forsinkelse og skal overholde de yderligere krav, der er angivet i artikel 16 ovenfor.

21.3. Under alle omstændigheder skal personoplysninger behandles i overensstemmelse med artikel 5 i GDPR og relevant lokal lovgivning.

22. Afsluttende bestemmelser

22.1. EU BCR'erne træder i kraft efter godkendelse af den kompetente databeskyttelsesmyndighed og gælder for de deltagende virksomheder ved underskrivelsen af EU BCR's vedtagelsesaftalen.

22.2. Ingen overførsel skal foretages til en deltagende virksomhed, medmindre den er bundet af disse EU-BCR'er. Hvis en dataimportør ophører med at være bundet af EU BCR'erne, skal den omgående returnere eller slette alle personlige data (inklusive kopier heraf), der er blevet overført i henhold til disse EU BCR'er, bortset fra det, forudsat at dataimportøren giver juridisk bindende forpligtelser til at opretholde beskyttelsen af personoplysningerne i overensstemmelse med kapitel V i GDPR, kan den opbevare personoplysninger, der er blevet overført i henhold til disse EU BCR'er.

22.3. Dataimportøren skal straks informere dataeksportøren, Amgen France og Chief Privacy Officer, hvis den af en eller anden grund ikke er i stand til at overholde disse EU BCR'er (inklusive situationerne beskrevet i artikel 12.3 ovenfor). Hvis dataimportøren overtræder disse EU BCR'er eller ikke er i stand til at overholde dem, skal dataeksportøren underrette Chief Privacy Officer og suspendere overførslen af personlige data.

22.4. Efter dataeksportørens valg skal dataimportøren straks returnere eller slette alle personlige data (inklusive kopier heraf), der er blevet overført i henhold til disse EU BCR'er, og skal attestere det samme over for dataeksportøren, hvor:

22.4.1. Dataeksportøren har suspenderet overførslen af personlige data, og overholdelse af disse EU BCR'er genoprettes ikke inden for en rimelig tid og under alle omstændigheder inden for en måned efter suspensionen; eller

22.4.2. Dataimportøren er i væsentlig overtrædelse af disse EU BCR'er; eller

22.4.3. Dataimportøren undlader at overholde en bindende afgørelse truffet af en kompetent domstol eller kompetent databeskyttelsesmyndighed vedrørende sine forpligtelser i henhold til disse EU BCR'er.

Indtil de personlige data er blevet slettet eller returneret, skal dataimportøren fortsat sikre overholdelse af disse EU BCR'er. Hvis lokale nationale love gældende for dataimportøren

forbyder returnering eller sletning af de personlige data, der er overført i henhold til disse EU BCR'er, skal dataimportøren fortsætte med at sikre overholdelse af disse EU BCR'er og kun behandle personoplysningerne i det omfang og så længe som påkrævet i henhold til sådanne lokale nationale love.

23. Bilag

De vedhæftede bilag er en integreret del af EU's BCR'er.

Bilag 1: Oversigt over Amgen-datastrømme

Bilag 2: Oversigt over Amgen træningsprogram

Bilag 1: Oversigt over Amgen-datastrømme

Datasubjekter	Kategorier af data	Formål	Overførsel
Medarbejder	Identifikationsdata såsom navn, adresse, fødselsdato og fødselssted, lejedato, cpr-numre, kreditkortnumre, bankkonto og finansielle oplysninger samt kørekort og offentligt udstedte id- kortnumre Ferier og fordele, klager, bonusser, forfremmelser, anmeldelser og evalueringer, arbejdsoptegnelser, information relateret til sundheds- og velfærdsdækning, pensionsordning og aktieoptionsdetaljer Skattemæssige og økonomiske personoplysninger Følsomme data såsom national oprindelse, når det er tilladt i henhold til lokal lovgivning	Personaleledelse, informationsteknologistøtte og administrationsformål i forbindelse med ansættelsesforholdet og ydelser, eller administration af efterlønsydelser, samt at overholde Amgens juridiske, administrative og virksomhedsmæssige forpligtelser	Amgen globale databaser er placeret i USA, hvor Amgen Inc., hovedkvarteret, er baseret. Data flyder fra Amgen France (eller den relevante dataeksportør) til Amgen Inc. i USA eller til deltagende virksomheder i Schweiz. Derefter kan dataene: - blot opbevares og vedligeholdes der - analyseres for at levere globale statistikker og rapporter - deles videre inde i Amgen-gruppen til andre deltagende virksomheder, hvor der er et forretningsbehov for sådan adgang af specifikke medarbejdere eller forretningsfunktioner hos disse deltagende virksomheder (f.eks.: en medarbejder, der søger job uden for sit land eller skal rapportere til en leder baseret uden for sit land). I de fleste tilfælde vil sådanne deltagende virksomheder fungere som
Sundhedspersonale	Navn, forretningskontaktoplysninger, herunder telefonnummer og e-mailadresse, ekspertiseområde Professionel baggrund (CV) Deltagelse i anden forskning Økonomiske oplysninger (fakturerings- og betalingsoplysninger)	Administration og ledelse af Amgens faglige og videnskabelige aktiviteter – Forskning og udvikling (f.eks. deltagelse i medicinsk forskning, kliniske studier, faglige møder eller kongresser) Promovering af Amgens produkter og tjenester Offentliggørelse af finansielle oplysninger, når det kræves af gældende lovgivning eller overholdelse af branchekodeks Regulativ overholdelse såsom sikkerhedsovervågning og rapportering af uønskede hændelser	

			dataansvarlige, men afhængigt af forretningsbehovet kan deltagende virksomheder også fungere som databehandlere (f.eks. ved at yde IT Help Desk-support eller yde support i forbindelse med HR Connect Service Centre).
Leverandører/leverandører	Personnavn, organisationsnavn, virksomhedskontaktoplysninger Fakturerings- og betalingsoplysninger	Behandling af betalinger til leverandører og leverandører Reguleringsoverholdelse såsom skattelovgivning	
Datapersoner fra kliniske forsøg (som kan omfatte børn under 18 år, hvor der er en pædiatrisk patient involveret i en klinisk undersøgelse sponsoreret af Amgen).	Kodede data – patientnavn og kontaktoplysninger erstattes med et internt genereret identifikationsnummer. Kun det kliniske forsøgssted (hospital/forskningssted) vedligeholder listen for at binde identifikationsnummeret tilbage til patientens navn. Indirekte identifikatorer såsom år eller fødselsdato (fuld fødselsdato indsamles kun til pædiatriske undersøgelser), køn, vægt, højde. Sundhedsdata er nødvendige som beskrevet i forskningsstudieprotokollen. Andre data vedrørende patienten, der er nødvendige for udførelsen af forskningen, herunder etnicitet, familiesituation (såsom antal børn), forbrug af stoffer, alkohol, stoffer, generelle vaner eller adfærd, professionel situation såsom job, arbejdsløshed, deltagelse i andre forskning.	Administration og ledelse af biomedicinsk forskning (kliniske forsøg, observatorieundersøgelser)	
Patienter (hvilket kan omfatte børn under 18 år, hvor der er en bivirkning, der involverer brugen af et Amgen-produkt med en	Indirekte identifikatorer for patienten såsom alder, år eller fødselsdato, patientinitialer (som tilladt i henhold til lokal lovgivning), køn, vægt/højde eller patientens identifikationsnummer (undtagen nationale	Lovgivningsoverholdelse og lægemiddelovervågning, såsom sikkerhedsovervågning og rapportering af uønskede hændelser (når det er tilladt i henhold til lokal lovgivning)	

pædiatrisk indikation).	sundhedsidentifikatorer). Data relateret til identifikation af Amgen-produktet, såsom det anvendte produkt eller den anvendte enhed, serienumre på enheder, leveringsmetode eller dosering af produktet, produkt-/batchnumre. Sundhedsdata, herunder administrerede behandlinger, resultater af undersøgelser, arten af eventuelle uønskede virkninger, personlig eller familiemæssig sygehistorie, tilknyttede sygdomme eller hændelser, risikofaktorer, information vedrørende ordination og brug af lægemidler og til den terapeutiske adfærd af helbredet fagfolk involveret i behandlingen af patientens sygdom. Andre data vedrørende patienten, der er nødvendige for vurderingen af den uønskede helbredshændelse i overensstemmelse med lovmæssige overholdelsesforpligtelser såsom etnicitet, arbejdsliv, forbrug af stoffer, alkohol, stoffer og/eller generelle vaner eller adfærd.		

Bilag 2: Oversigt over Amgen træningsprogram

Oplysningsprogram om privatliv og databeskyttelse

Uddannelsesprogrammet for privatliv og databeskyttelse bestræber sig på at sikre, at alt Amgen-personale er ordentligt uddannet i Amgen EU BCR'er samt eventuelle juridiske forpligtelser, der påvirker behandlingen af personoplysninger. Dette program indeholder forskellige elementer.

Generel træning for alt Amgen personale

Alt Amgen-personale skal udføre en årlig onlineuddannelse i databeskyttelse som en del af adfærdskodeksuddannelsen. Denne træning er obligatorisk og overvåget og tager normalt omkring 75 minutter at gennemføre. Denne uddannelse omfatter EU's BCR'er og information om konsekvenserne i henhold til straffe- og ansættelseslovgivningen og/eller deres kontrakt for tjenester til personale, der bryder EU's BCR'er.

Specifik uddannelse til DPO'er

Alle Amgen DPO'er trænes regelmæssigt i nye processer gennem regelmæssige DPO-opkald udført af Global Privacy Compliance Team og privatlivsworkshops på stedet og/eller online efter behov. Alle DPO'er har adgang til en wiki-side, der besvarer de oftest stillede spørgsmål og giver vejledning samt links til eksterne ressourcer.

Specifik uddannelse til personale

Specifik træning kan leveres på behov-to-know-basis enten online eller onsite eller ved at offentliggøre oplysninger på Amgens intranet. Denne uddannelse kan være fokuseret på specifikke grupper, som enten behandler personoplysninger på daglig basis eller støtter andre grupper, der behandler personoplysninger. For eksempel uddannes revisionsgruppen, R&D-funktioner og den juridiske afdeling løbende. Dette omfatter oplysninger om procedurer for håndtering af anmodninger om adgang til personoplysninger fra offentlige myndigheder, hvor det er relevant for specifikt personale. Denne uddannelse kan foregå enten på regionalt niveau eller på landeniveau. Yderligere specifik EU-BCR-uddannelse kan udvikles efter behov.

Opmærksomhed

Amgen har en dedikeret side på sit intranet om privatliv og databeskyttelse, der giver links til andre ressourcer enten internt eller eksternt.

Amgens Global Privacy Compliance Team samarbejder med Information Security-afdelingen om Sentinel-programmet, som er et globalt program, der skal øge bevidstheden hos Amgen Personale om informationssikkerhed.

Træningsstøtte

Alle privatlivsrelaterede træninger er udviklet af Global Privacy Compliance Team og godkendt af Chief Privacy Officer. Træningen kan enten udføres direkte af et Global Privacy Compliance Team-medlem eller af en lokal DPO efter en "train the trainer"-model.