Amgen EU Binding Corporate Rules – Controller (EU BCR-ene)

Sist oppdatert: 12. desember 2023

Introduksjon

(A) Amgen er en bioteknologileder som er forpliktet til å betjene pasienter med alvorlig sykdom. Disse EU-bindende konsernreglene – behandlingsansvarlig ("**EU BCR-ene**") uttrykker Amgens forpliktelse til personvern og databeskyttelse ettersom den bestreber seg på å gi tilstrekkelig beskyttelse for overføring og behandling av personopplysninger mellom deltakende selskaper.

(B) Alle deltakende selskaper og alt personell er forpliktet til å respektere, og er juridisk bundet av, disse EU BCR-ene med hensyn til personopplysninger innenfor EU BCR-enes omfang. Manglende overholdelse kan føre til disiplinære sanksjoner, som tillatt av lokale forskrifter. Chief Compliance Officer i samarbeid med personverndirektøren sikrer at EU BCR-ene vil bli håndhevet. En liste over deltakende selskaper finner du her: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. Alle deltakende selskaper kan kontaktes på privacy@amgen.com ved spørsmål som omhandler disse EU BRC-ene.

(C) Disse EU BCR-ene har blitt vedtatt med henvisning til EUs databeskyttelseslover. Amgen Frankrike er ansvarlig for å sikre at de deltakende selskapene overholder disse EU BCR-ene. Enkeltpersoner kan håndheve disse EU BCR-ene mot Amgen Frankrike som en tredjeparts begunstiget som beskrevet nedenfor. Disse EU BCR-ene er tilgjengelige på Amgens nettsted: www.amgen.com/bcr. Du kan også kontakte Amgen på privacy@amgen.com for å be om en kopi.

1. Omfang

1.1. Amgen EU BCR-ene gjelder for overføringer og behandling, automatisert eller manuell, av alle personopplysninger om datasubjekter utført av et deltakende selskap som opererer som datakontrollør eller som opererer som databehandler for et annet deltakende selskap som fungerer som datakontrollør i noen av følgende tilfeller:

1.1.1. det deltakende selskapet som behandler personopplysningene er etablert i EU; eller

1.1.2. det deltakende selskapet som behandler personopplysningene er ikke etablert i EØS og har mottatt personopplysningene fra et deltakende selskap etablert i EØS; eller

1.1.3. til videre overføring av personopplysninger fra dataimportører til dataimportører.

1.2. En oversikt over datastrømmene i henhold til disse EU BCR-ene er tilgjengelig i vedlegg 1.

2. Definisjoner

Vilkår	*Definisjoner*
Amgen Frankrike	Amgen S.A.S., et selskap registrert i Frankrike med hovedkontor på 25 quai du Président Paul Doumer, 92400 Courbevoie.
Gjeldende lov	EUs lovgivning og/eller (hvis aktuelt) nasjonal eller lokal lovgivning i EØS-landene (inkluderer uten begrensning, EUs databeskyttelseslover).
Samsvarsansvarlig	En person i Healthcare Compliance-divisjonen i Worldwide Compliance and Business Ethics-avdelingen i et deltakende selskap som har delegert ansvaret for databeskyttelse og personvern, og der det er differanse fra den lokale databeskyttelsesansvarlige, støtter den lokale databeskyttelsesansvarlige med sine ansvarsområder og oppgaver.
Samtykke	Enhver fritt gitt spesifikk, informert og utvetydig indikasjon på en registrert sine ønsker, der den registrerte, ved en uttalelse eller ved en klar bekreftende handling, betyr enighet om behandling av personopplysninger knyttet til ham/henne.
Datakontrollør	Enhver enhet som tar beslutninger med hensyn til innsamling og behandling av personopplysninger, inkludert beslutninger om formålene med og måten personopplysninger behandles på.
Dataeksportør	Et deltakende selskap som opererer som en datakontrollør etablert i EØS som overfører personopplysninger til en dataimportør.
Dataimportør	Et deltakende selskap som ikke er etablert i EØS som enten (a) mottar personopplysninger fra en dataeksportør eller (b) mottar en videre overføring av personopplysninger i henhold til artikkel 1(c) i disse EU BCR-ene.
Databehandler	En person eller enhet som behandler personopplysninger på vegne av en behandlingsansvarlig.
Datatilsynet (DPA)	En uavhengig offentlig databeskyttelsesmyndighet etablert av et EØS-medlemsland.
Databeskyttelsesansvarlig	En person som er utpekt av Amgens personverndirektør som ansvarlig for tilsyn med personvern og databeskyttelse på lokalt nivå, samt implementering av passende og nødvendige kontroller.
Registrerte personer	En fysisk person som kan identifiseres, direkte eller indirekte, ved henvisning til personopplysninger. En registrert kan være (uten begrensning): • en pasient / klinisk forsøksperson (som kan inkludere et barn under 18 år) • helsepersonell • en ansatt

Vilkår	*Definisjoner*
	• en leverandør eller leverandør
EØS	Medlemslandene i den europeiske union (Østerrike, Belgia, Bulgaria, Kroatia, Republikken Kypros, Tsjekkia, Danmark, Estland, Finland, Frankrike, Tyskland, Hellas, Ungarn, Irland, Italia, Latvia, Litauen, Luxembourg, Malta, Nederland, Polen, Portugal, Romania, Slovakia, Slovenia, Spania og Sverige) og Island, Liechtenstein og Norge (alle er "**EØS-medlemsland**").
EUs databeskyttelseslover	GDPR og (hvis aktuelt) lokal eller nasjonal lovgivning knyttet til databeskyttelse og behandling av personopplysninger og implementering av GDPR i et relevant EØS-medlemsland.
GDPR	Den generelle databeskyttelsesforskriften (EU) 2016/679).
Deltakende selskap	En juridisk enhet fra Amgen-gruppen som er bundet av EUs BCR-ene.
Personopplysninger	Enhver informasjon relatert til en datasubjekt som et navn, et identifikasjonsnummer, stedsdata, en online identifikator eller til en eller flere faktorer som er spesifikke for eller informasjon relatert til den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identiteten til den fysiske personen. Eksempler på personopplysninger kan inkludere følgende: • En registrert persons navn, adresse, personnummer, førerkortnummer, bankkontoinformasjon, familieinformasjon eller medisinske data, • Navn, høyere utdanning og forskrivningspraksis for helsepersonell, • E-postadressen og annen identifiserende informasjon oppgitt av noen som besøker et Amgen-nettsted. Listen ovenfor er kun veiledende og ikke fullstendig.
Brudd på personvern	Ethvert sikkerhetsbrudd som fører til utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert utlevering av eller tilgang til personopplysninger som overføres, lagres eller på annen måte behandles.
Personell	Alle ansatte og kontingentarbeidere (inkludert konsulenter, vikarer og kontraktsarbeidere) i ethvert deltakende selskap.
Behandling	Enhver handling eller handlingssett som utføres på personlig informasjon (eller sett med personlig informasjon), enten det skjer automatisk eller ikke, som innsamling, opptak, organisering, lagring, tilpasning eller endring, henting, konsultasjon, bruk, avsløring ved overføring, videreformidling eller på annen måte gjøre tilgjengelig,

Vilkår	*Definisjoner*
	justere eller kombinasjon, begrense, sletting eller destruksjon.
Sensitive personopplysninger	Personopplysninger som avslører rase eller etnisk opprinnelse, politiske meninger, religiøs eller filosofisk tro, eller fagforeningsmedlemskap, og behandling av genetiske data, biometriske data med det formål å unikt identifisere en fysisk person, helseopplysninger eller data om en fysisk persons sexliv eller seksuelle legning. I tillegg til EUs lover om databeskyttelse, anser Amgen også finansiell informasjon og informasjon som kan brukes til å begå identitetstyveri (f.eks. personnummer, førerkortnummer, kredittkort eller annen bankkontoinformasjon) som sensitive personopplysninger.
Tekniske og organisatoriske sikkerhetstiltak	Teknologiske og organisatoriske tiltak som tar sikte på å beskytte personopplysninger mot utilsiktet eller ulovlig ødeleggelse eller utilsiktet tap, endring, uautorisert utlevering eller tilgang, spesielt der behandlingen innebærer overføring av data over et nettverk, og mot alle andre ulovlige former for behandling.
Tredjepart	En fysisk eller juridisk person, offentlig myndighet, byrå eller ethvert annet organ enn den registrerte, det deltakende selskapet som fungerer som datakontrollør og et deltakende selskap som fungerer som databehandler. Hos Amgen anses en leverandør som en tredjepart. Avhengig av omstendighetene kan en tredjepart fungere som datakontrollør eller databehandler i forhold til behandling av personopplysninger.
Leverandør	Enhver fysisk eller juridisk person, virksomhet eller organisasjon som leverer varer og/eller tjenester til et deltakende selskap under et kontraktsforhold og/eller er en mottaker av personopplysninger fra et slikt deltakende selskap for å yte disse godene og/eller tjenestene.

Amgen skal tolke vilkårene i disse EU BCR-ene i samsvar med EUs databeskyttelseslover.

3. Formålsbegrensning

3.1. Personopplysninger skal behandles for eksplisitte, spesifiserte og legitime formål i henhold til artikkel 5(1)(b) i GDPR.

3.2. Personopplysninger vil ikke bli behandlet på måter som er uforenlige med de legitime formålene som personopplysningene ble samlet inn for eller gjeldende lov. Dataimportører er forpliktet til å overholde opprinnelige formål når de lagrer og/eller viderebehandler personopplysninger eller behandler personopplysninger som overføres til dem av et annet deltakende selskap. Formålet med behandling av personopplysninger kan bare endres med samtykke fra datasubjektet eller i den grad det er tillatt i henhold til gjeldende lov.

3.3. Sensitive personopplysninger vil bli utstyrt med ytterligere sikkerhetstiltak, slik som gitt av EUs databeskyttelseslover.

4. Datakvalitet og proporsjonalitet

4.1. Personopplysninger må være nøyaktige og, der det er nødvendig, holdes oppdatert; alle rimelige skritt må tas for å sikre at personopplysninger som er unøyaktige, med hensyn til formålene de behandles for, slettes eller korrigeres uten forsinkelse.

4.2. Personopplysninger skal være tilstrekkelige, relevante og begrenset til det som er nødvendig i forhold til formålene de behandles for, i henhold til artikkel 5(1)(c) i GDPR.

4.3. Behandling av personopplysninger vil bli styrt av målet om å begrense innsamling, behandling og/eller bruk av personopplysninger til bare det som er nødvendig, dvs så lite personopplysninger som mulig. Muligheten for anonyme eller pseudonyme data må vurderes, forutsatt at kostnadene og innsatsen som er involvert, står i forhold til ønsket formål.

4.4. Personopplysninger som ikke lenger er nødvendige for det forretningsformålet de opprinnelig ble samlet inn og lagret for, må slettes i henhold til Amgens tidsplan for oppbevaring av journalopplysninger. I tilfelle lovbestemte oppbevaringsperioder eller lovlige tilbakeholdinger gjelder, vil dataene bli blokkert i stedet for slettet. Ved slutten av oppbevaringsperioden eller den juridiske tilbakeholdingen vil dataene bli slettet.

5. Rettslig grunnlag for behandling av personopplysninger

5.1. Behandling av personopplysninger er bare tillatt hvis minst én av følgende forutsetninger er oppfylt:

5.1.1. Den registrerte har gitt sitt samtykke til behandling av hans eller hennes personopplysninger for ett eller flere spesifikke formål.

5.1.2. Behandlingen er nødvendig for utførelsen av en kontrakt som den registrerte er part i, eller for å iverksette tiltak på forespørsel fra den registrerte før inngåelse av en kontrakt.

5.1.3. Behandlingen er nødvendig for å overholde en juridisk forpliktelse som den behandlingsansvarlige er underlagt i henhold til gjeldende lov.

5.1.4. Behandlingen er nødvendig for å beskytte de vitale interessene, som liv, helse eller sikkerhet, til den registrerte eller en annen fysisk person.

5.1.5. Behandlingen er nødvendig for å utføre en oppgave utført i allmennhetens interesse eller i utøvelse av offentlig myndighet som er tildelt den behandlingsansvarlige.

5.1.6. Behandlingen er nødvendig for de legitime interessene som forfølges av datakontrolløren eller av en tredjepart, unntatt der slike interesser overstyres av interessene eller grunnleggende rettigheter og friheter til den registrerte.

5.2. Behandling av personopplysninger knyttet til straffedommer og lovbrudd skal bare utføres når behandlingen er autorisert av gjeldende lov som gir passende garantier for de registrertes rettigheter og friheter.

6. Prosessering av sensitiv personlig informasjon.

6.1. Hvis, i henhold til et spesifikt og legitimt formål, det deltakende selskapet trenger å behandle sensitive personopplysninger, vil det deltakende selskapet bare gjøre det hvis:

6.1.1. Den registrerte har gitt uttrykkelig samtykke til behandling av disse sensitive personopplysningene for ett eller flere spesifiserte formål, unntatt der gjeldende lov fastsetter at forbudet i artikkel 9(1) i GDPR ikke kan oppheves av den registrerte.

6.1.2. Behandlingen er nødvendig for å oppfylle forpliktelsene og de spesifikke rettighetene til den behandlingsansvarlige innen lov om sysselsetting og sosial sikkerhet og sosial beskyttelse i den grad det er autorisert av gjeldende lov eller ved en tariffavtale i henhold til gjeldende lov som gir passende garantier for de grunnleggende rettighetene og interessene til den registrerte.

6.1.3. Behandlingen er nødvendig for å beskytte de vitale interessene til den registrerte eller en annen fysisk person der den registrerte er fysisk eller juridisk ute av stand til å gi sitt samtykke.

6.1.4. Behandlingen utføres i løpet av sine legitime aktiviteter med hensiktsmessige garantier av en stiftelse, forening eller et annet non-profit-søkende organ med et politisk, filosofisk, religiøst eller fagforeningsmessig mål og på betingelse av at behandlingen kun gjelder medlemmene av organet eller personer som har regelmessig kontakt med det i forbindelse med dets formål, og at dataene ikke offentliggjøres utenfor dette organet uten samtykke fra de registrerte.

6.1.5. Behandlingen gjelder sensitive personopplysninger som åpenbart offentliggjøres av den registrerte.

6.1.6. Behandlingen av sensitive personopplysninger er nødvendig for etablering, utøvelse eller forsvar av juridiske krav.

6.1.7. Behandlingen er nødvendig av hensyn til vesentlig offentlig interesse, på grunnlag av gjeldende lov som skal være proporsjonal med målet som forfølges, respektere essensen av retten til databeskyttelse og sørge for egnede og spesifikke tiltak for å ivareta de grunnleggende rettighetene og interessene til den registrerte.

6.1.8. Behandlingen av de sensitive personopplysningene er nødvendig for forebyggende formål eller arbeidsmedisin, for vurdering av arbeidskapasiteten til den ansatte, medisinsk diagnose, levering av helse- eller sosialomsorg eller behandling eller styring av helse- eller sosialomsorgssystemer og -tjenester på grunnlag av gjeldende lov eller i henhold til kontrakt med en helsepersonell, og hvor disse sensitive personopplysningene behandles av eller under ansvar av en helsepersonell, må slik profesjonell være underlagt taushetsplikt i henhold til gjeldende lov eller regler fastsatt av kompetente organer i en EØS-medlemsstat eller av en annen person som også er underlagt taushetsplikt i henhold til gjeldende lov eller regler fastsatt av kompetente organer i et EØS-medlemssland.

6.1.9. Behandlingen av sensitive personopplysninger er nødvendig av hensyn til allmennhetens interesse på folkehelseområdet, som for eksempel å beskytte mot

alvorlige grenseoverskridende trusler mot helsen eller sikre høye kvalitets- og sikkerhetsstandarder for helsevesenet og for legemidler eller medisinsk utstyr, på grunnlag av gjeldende lov som gir passende og spesifikke tiltak for å ivareta rettighetene og frihetene til den registrerte, spesielt taushetsplikt.

6.1.10. Behandlingen av sensitive personopplysninger er nødvendig for arkiveringsformål i allmennhetens interesse, vitenskapelige eller historiske forkningsformål eller statistiske formål i samsvar med artikkel 89(1) i GDPR basert på gjeldende lov som skal være proporsjonal med målet som forfølges, respektere essensen av retten til databeskyttelse og sørge for passende og spesifikke tiltak for å ivareta de grunnleggende rettighetene og interessene til den registrerte.

7. Innsyn og informasjonsrettigheter

7.1. Alle deltakende selskaper skal behandle personopplysninger på en gjennomsiktig måte.

Amgen er forpliktet til å gjøre EU BCR-ene, inkludert kontaktinformasjon, lett tilgjengelig for alle registrerte og til å informere registrerte om overføring og behandling av deres personopplysninger. Disse EU BCR-ene er tilgjengelige på Amgens nettsted: www.amgen.com/bcr. Du kan også kontakte Amgen på privacy@amgen.com for å be om en kopi. Amgen vil også bruke ulike kommunikasjonsmidler som bedrifters hjemmesider, inkludert interne nettsteder og nyhetsbrev, kontrakter og spesifikke personvernerklæringer for å oppfylle dette tilgjengelighetskravet. I tillegg vil Amgen informere de registrerte, ved hjelp av disse kommunikasjonsmidlene, om eventuelle oppdateringer eller endringer i EU BCR-ene eller til listen over deltakende selskaper uten unødig forsinkelse.

7.2. Registrerte personer hvis personopplysninger behandles av et deltakende selskap, skal gis informasjonen som er angitt i artikkel 13 og 14 i GDPR.

7.3. Når personopplysningene ikke mottas fra en registrert, gjelder ikke plikten til å informere den registrerte hvis det viser seg umulig eller ville innebære en uforholdsmessig innsats, eller hvis opptak eller utlevering er uttrykkelig fastsatt ved lov.

8. Rett til tilgang, retting, sletting og begrensning av data

8.1. Hver registrerte person har rett til å få fra det deltakende selskapet bekreftelse på hvorvidt personopplysninger om ham eller henne blir behandlet, og, hvis det er tilfelle, tilgang til personopplysningene og informasjonen som kreves i henhold til artikkel 15(1) i GDPR. Oppfølgingen av denne forespørselen, inkludert muligheten til å kreve et gebyr eller tidsrammen for å svare på en slik forespørsel, vil være underlagt gjeldende lov og kommuniseres hensiktsmessig til den registrerte når han/hun sender inn sin forespørsel.

8.2. Hver registrerte har rett til å få retting, sletting eller begrensning av personopplysninger, spesielt der dataene er ufullstendige eller unøyaktige.

8.3. Hver registrerte har rett til når som helst å motsette seg, av begrunnelser knyttet til deres spesielle situasjon, behandling av deres personopplysninger basert på utførelsen av en oppgave utført i allmennhetens interesse eller de legitime interessene til det deltakende selskapet eller en tredjepart (inkludert profilering basert på disse begrunnelsene). Det deltakende selskapet skal ikke lenger behandle personopplysningene med mindre det viser overbevisende legitime begrunnelser for behandlingen som overstyrer interessene,

rettighetene og frihetene til den registrerte eller for etablering, utøvelse eller forsvar av juridiske krav.

8.4. Hver registrerte har rett til å motsette seg (gratis) behandling av personopplysninger knyttet til ham eller henne med henblikk på direkte markedsføring, som inkluderer profilering i den grad det er relatert til slik direkte markedsføring. Når den registrerte utøver sin rett til å motsette seg behandling av personopplysninger knyttet til ham eller henne med henblikk på direkte markedsføring, må det deltakende selskapet avslutte behandlingen av personopplysningene for dette formålet.

8.5. Alle registrerte har rett til å få varsling til tredjeparter som personopplysningene har blitt utlevert til om enhver retting, sletting eller begrensning, i henhold til artikkel 19 i GDPR.

8.6. Alle registrerte har rett til å kjenne til logikken involvert i enhver automatisk behandling av personopplysninger, i henhold til artikkel 13(2)(f) i GDPR.

8.7. Der behandling er basert på samtykke, har alle registrerte rett til å trekke tilbake samtykket når som helst. Tilbaketrekking av samtykke skal ikke påvirke lovligheten av behandling basert på samtykke før tilbaketrekking.

8.8. Hver registrerte har rett til å klage til det deltakende selskapet angående behandling av personopplysninger gjennom den interne klagemekanismen som er gitt i henhold til artikkel 17.

8.9. Eventuelle forespørsler i henhold til denne artikkel 8 (eller artikkel 9 nedenfor) skal sendes til det deltakende selskapet på: privacy@amgen.com. Vi oppfordrer på det sterkeste til å sende forespørsler via e-post, men dette utelukker ikke at en registrert person kan sende en muntlig forespørsel. Det deltakende selskapet skal informere den registrerte uten forsinkelse om utfallet av deres forespørsel og senest innen en måned etter mottak av forespørselen (inkludert, der det er aktuelt, årsakene til ikke å iverksette tiltak og muligheten for å sende inn en klage til den kompetente databeskyttelsesmyndigheten og/eller søke rettsmiddel). Denne perioden på én måned kan forlenges med ytterligere to måneder når det er nødvendig, med tanke på kompleksiteten og antallet forespørsler. Det deltakende selskapet skal informere den registrerte om en slik forlengelse innen en måned etter mottak av forespørselen, sammen med årsakene til forsinkelsen. All kommunikasjon, handling og/eller informasjon som gis i forbindelse med en forespørsel i henhold til denne artikkel 8 (eller artikkel 9 nedenfor) skal gis til den registrerte gratis. Der forespørsler fra en registrert er åpenbart ubegrunnede eller overdrevne, særlig på grunn av deres repeterende karakter, kan det deltakende selskapet enten: (a) kreve et rimelig gebyr som tar hensyn til de administrative kostnadene ved å gi informasjonen eller kommunikasjonen eller iverksette den forespurte handlingen; eller (b) nekte å handle på forespørselen. Det deltakende selskapet skal bære byrden av å demonstrere den åpenbart ubegrunnede eller overdrevne karakteren av forespørselen.

9. Automatiserte individuelle beslutninger

9.1. Den registrerte skal ha rett til ikke å bli gjenstand for en beslutning basert utelukkende på automatisert behandling, inkludert profilering, som gir rettsvirkninger for ham eller henne eller på lignende måte påvirker ham eller henne betydelig, med mindre denne beslutningen:

9.1.1. er nødvendig for å inngå eller utføre en kontrakt mellom den registrerte og det deltakende selskapet;

9.1.2. er pålagt eller autorisert av gjeldende lov som også fastsetter egnede tiltak for å beskytte den registrertes rettigheter og friheter og legitime interesser (inkludert minst retten til å få menneskelig inngripen fra det deltakende selskapets side, for å uttrykke sitt synspunkt og å bestride beslutningen); eller

9.1.3. er basert på den registrertes eksplisitte samtykke.

10. Sikkerhet og konfidensialitet

10.1. Amgen implementerer passende tekniske og organisatoriske sikkerhetstiltak for å beskytte mot og oppdage brudd på personopplysninger. Internasjonale rammeverk, som ISO/IEC 27002, brukes av Amgen til å fastsette disse sikkerhetstiltakene.

10.2. Amgen har prosesser på plass for å sikre at brudd på personopplysninger er gjenstand for rapportering, sporing og passende korrigerende tiltak, etter behov. Ethvert brudd på personopplysninger skal dokumenteres (inkludert fakta knyttet til brudd på personopplysninger, dens virkninger og de utbedrende tiltakene som er iverksatt), og dokumentasjonen skal gjøres tilgjengelig for den kompetente DPA på forespørsel. Deltakende selskaper skal varsle uten unødig forsinkelse ethvert brudd på personopplysninger til Amgen Frankrike, personverndirektøren og den andre relevante personvernansvarlige/-funksjonen, og (der det deltakende selskapet som lider av et brudd på personopplysninger, fungerer som databehandler) til det deltakende selskapet som fungerer som datakontrollør. Brudd på personopplysninger skal, i forbindelse med personverndirektøren, varsles til den kompetente DPA uten unødig forsinkelse (og der det er mulig senest 72 timer etter å ha blitt oppmerksom på brudd på personopplysninger) med mindre det er usannsynlig at det vil føre til en risiko for de registrertes rettigheter og friheter. Der brudd på personopplysninger sannsynligvis vil føre til en høy risiko for rettighetene og frihetene til registrerte, skal det også varsles til registrerte uten unødig forsinkelse.

10.3. Informasjonssikkerhets risikovurderinger brukes til å identifisere potensielle trusler mot sensitive personopplysninger og implementering av ytterligere sikkerhetskontroller etter behov.

10.4. Gjennomføringen av tiltakene vil ta hensyn til den nyeste teknologien, i henhold til artikkel 32 i GDPR.

10.5. Informasjonssikkerhetsdirektøren samarbeider med personverndirektøren for å sikre sikkerheten og konfidensialiteten til personopplysninger.

10.6. De tekniske og organisatoriske sikkerhetstiltakene skal utformes for å implementere databeskyttelsesprinsippene i henhold til artikkel 5 i GDPR, databeskyttelse ved design og standardprinsipper i henhold til artikkel 25 i GDPR og for å tilrettelegge overholdelse av kravene fastsatt av disse EU BCR-ene i praksis.

11. Forhold til databehandlere (Amgen Dataimportør eller Leverandør)

11.1. Det deltakende selskapet (som fungerer som datakontrollør) vil nøye velge en databehandler som kan være enten et annet deltakende selskap eller en leverandør. Databehandleren må gi tilstrekkelige garantier vedrørende sine tekniske og organisatoriske sikkerhetstiltak som styrer behandlingen som skal utføres, og må sikre overholdelse av disse tiltakene.

11.2. Når utkontraktering anses nødvendig etter å ha vurdert forretningsbehovene og risikoene ved en slik utkontraktering, vil prosessen med å velge databehandler inkludere en evaluering av personvernrisikofaktorer og balansere forretningsbehov mot potensielle risikoer.

11.3. Det deltakende selskapet som fungerer som datakontrollør, ved bruk av skriftlige kontraktsmessige midler, vil i samsvar med gjeldende lov (og spesielt kravene i artikkel 28(3) i GDPR) instruere databehandleren, blant annet:

11.3.1. databehandleren skal kun handle etter instruksjoner fra det deltakende selskapet som opptrer som datakontrollør, og at behandling av personopplysninger for databehandlerens egne formål eller for en tredjeparts formål er forbudt;

11.3.2. om reglene om sikkerheten og konfidensialiteten som påhviler databehandleren og å implementere passende tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er passende for risikoen for behandlingen;

11.3.3. personer som er autorisert til å behandle personopplysningene har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt;

11.3.4. databehandleren skal ikke engasjere en annen databehandler uten forutgående spesifikk eller generell skriftlig tillatelse fra det deltakende selskapet som opptrer som datakontrollør, og der slik tillatelse er gitt, skal de samme forpliktelsene til databeskyttelse som er fastsatt i kontrakten eller annen juridisk handling mellom det deltakende selskapet som opptrer som datakontrollør og databehandleren pålegges den andre databehandleren;

11.3.5. tar hensyn til arten av behandlingen, må den bistå det deltakende selskapet som fungerer som datakontrollør ved hensiktsmessige tekniske og organisatoriske tiltak, så langt dette er mulig, for oppfyllelse av det deltakende selskapets forpliktelse til å svare på forespørsler om utøvelse av den registrertes rettigheter;

11.3.6. det må bistå det deltakende selskapet som fungerer som datakontrollør for å sikre overholdelse av forpliktelsene knyttet til sikkerhet for behandling, melding om et brudd på personopplysninger til den kompetente DPA, kommunikasjon av et brudd på personopplysninger til den registrerte, vurderinger av innvirkning på databeskyttelse og forutgående konsultasjon med den kompetente DPA, mens det tas hensyn til arten av behandling og informasjonen som er tilgjengelig for databehandleren;

11.3.7. etter valg av det deltakende selskapet som fungerer som datakontrollør, må det slette eller returnere alle personopplysningene til det deltakende selskapet som fungerer som datakontrollør etter slutten av leveringen av tjenester knyttet til behandlingen, og slette eksisterende kopier med mindre EUs databeskyttelseslov krever lagring av personopplysningene;

11.3.8. det må gjøre tilgjengelig for det deltakende selskapet som fungerer som datakontrollør all informasjon som er nødvendig for å demonstrere overholdelse av forpliktelsene fastsatt i denne artikkelen 11 og tillate og bidra til revisjoner, inkludert inspeksjoner, utført av det deltakende selskapet som fungerer som datakontrollør eller en annen revisor som er bemyndiget av den.

11.4. Det deltakende selskapet som fungerer som datakontrollør, skal sikre at databehandleren forblir i full overensstemmelse med de avtalte tekniske og organisatoriske sikkerhetstiltakene.

11.5. Det deltakende selskapet som fungerer som datakontrollør, beholder ansvaret for legitimiteten til behandlingen og er fortsatt ansvarlig for den registrertes rettigheter. I den grad databehandleren er underlagt EUs databeskyttelseslover, skal den også være ansvarlig for sine forpliktelser og ansvar som databehandler i henhold til slike lover.

11.6. For å sørge for de kontraktsmessige forpliktelsene som er fastsatt i denne artikkelen om databehandlere, er en kontraktsmal med tittelen Data Privacy Schedule gitt for bruk av deltakende selskaper som fungerer som datakontrollør. Det deltakende selskapet som fungerer som datakontrollør, kan, avhengig av de spesifikke omstendighetene for hver kontraktsordning, forhandle andre bestemmelser enn de som er fastsatt i datapersonvernplanen, men kontraktsbestemmelsene må fortsatt dekke, som et minimum, forpliktelsene som er angitt ovenfor i denne artikkelen 11.

11.7. Hvert deltakende selskap som fungerer som en databehandler som er underlagt EUs databeskyttelseslover, må føre en oversikt over alle kategorier av behandlingsaktiviteter utført på vegne av et deltakende selskap som fungerer som datakontrollør. Denne registreringen skal gjøres skriftlig, inkludert i elektronisk form, skal gjøres tilgjengelig for personverndirektøren og den kompetente DPA på forespørsel, og skal inneholde følgende informasjon: (a) navn og kontaktinformasjon for det deltakende selskapet som opptrer som databehandler og for hvert deltakende selskap som opptrer som datakontrollør på vegne av hvilket det opptrer, og, der det er aktuelt, dets representant og DPO; (b) kategoriene av behandling utført på vegne av hvert deltakende selskap som opptrer som datakontrollør; og (c) der det er aktuelt, overføringer av personopplysninger til et tredjeland eller en internasjonal organisasjon, inkludert identifisering av det tredjelandet eller den internasjonale organisasjonen, og, i tilfelle overføringer som er avhengig av et unntak i henhold til artikkel 49 hvis GDPR, dokumentasjon av passende sikkerhetstiltak; og (d) der det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene.

12. Restriksjoner på overføringer og videreoverføringer

12.1. Alle overføringer av personopplysninger som er underlagt disse EU BCR-ene til tredjeparter som befinner seg utenfor EØS, skal respektere EUs databeskyttelseslover om overføringer og videre overføringer av personopplysninger, enten ved å bruke standard kontraktsklausuler autorisert i henhold til kommisjonens gjennomføringsbeslutning (EU) av 4. juni 2021 om standard kontraktsklausuler for overføring av personopplysninger til tredjeland i henhold til GDPR eller ved andre tilstrekkelige midler i henhold til kapittel V i GDPR (inkludert, unntaksvis, hvis et unntak gjelder for en bestemt situasjon i samsvar med artikkel 49 i GDPR).

12.2. Alle overføringer av personopplysninger som er underlagt disse EU BCR-ene til databehandlere som befinner seg utenfor EØS, skal overholde EUs databeskyttelseslover knyttet til databehandlere (og kravene fastsatt i artikkel 11 ovenfor) i tillegg til reglene om overføringer og videre overføringer av personopplysninger fastsatt i denne artikkelen 12 og i EUs databeskyttelseslover.

12.3. Før overføring av personopplysninger til en dataimportør eller (med hensyn til pågående overføringer) før en oppdatert lokal nasjonal lov trer i kraft, skal dataeksportøren, sammen med Personvernsjefen og Amgen Frankrike, med hjelp av dataimportøren og med hensyn til omstendighetene ved overføringen, vurdere om lokal nasjonal lov vil hindre dataimportøren i

å oppfylle sine forpliktelser i henhold til EU BCR-ene og avgjøre om eventuelle nødvendige tilleggstiltak skal implementeres. En slik vurdering vil ta hensyn til:

12.3.1. de spesifikke omstendighetene ved overføringen (inkludert formålene som personopplysningene overføres og behandles for, hvilke typer enheter som er involvert i behandlingen, den økonomiske sektoren der overføringen skjer, kategoriene og formatet til de overførte personopplysningene, plasseringen av behandlingen (inkludert lagring) og overføringskanalene som brukes);

12.3.2. lovene og praksisen i destinasjonstredjelandet som er relevant i lys av de spesifikke omstendighetene ved overføringen (inkludert de som krever utlevering av data til offentlige myndigheter eller autorisering av tilgang av slike myndigheter) og gjeldende begrensninger og garantier; og

12.3.3. alle relevante kontraktsmessige, tekniske eller organisatoriske sikkerhetstiltak som er på plass med hensyn til overføringen, inkludert tiltak som brukes under overføringen og til behandling av personopplysningene i destinasjonslandet.

Videre skal en slik vurdering være basert på forståelsen av at lover og praksis i bestemmelseslandet respekterer de grunnleggende rettighetene og frihetene til den registrerte og ikke overskrider det som er nødvendig og forholdsmessig i et demokratisk samfunn for å ivareta ett av følgende mål: (a) nasjonal sikkerhet; (b) forsvar; (c) offentlig sikkerhet; (d) forebygging, etterforskning, oppdagelse eller rettsforfølgelse av straffbare handlinger eller gjennomføring av strafferettslige sanksjoner, inkludert beskyttelse mot og forebygging av trusler mot offentlig sikkerhet; (e) andre viktige mål av allmenn interesse, spesielt viktige økonomiske eller finansielle interesser, inkludert monetære, budsjettmessige og skattemessige forhold, folkehelse og sosial sikkerhet; (f) beskyttelse av rettslig uavhengighet og rettssaker; (g) forebygging, etterforskning, oppdagelse og rettsforfølgelse av brudd på etikk for regulerte yrker; (h) overvåking, inspeksjon eller regulatoriske funksjoner knyttet til utøvelse av offentlig myndighet i tilfellene nevnt i de foregående målene; (i) beskyttelse av den registrerte eller andres rettigheter og friheter; og/eller (j) håndhevelse av sivilrettslige krav.

Personvernsjefen skal gjennomgå og godkjenne den dokumenterte vurderingen og eventuelle foreslåtte tilleggstiltak. Der utfallet av vurderingen viser behovet for å implementere tilleggstiltak, skal dataeksportøren implementere disse tiltakene. Hvis ingen supplerende tiltak kan iverksettes (eller hvis instruert av personverndirektøren eller en kompetent DPA), skal dataeksportøren suspendere overføringen. Utfallet av vurderingen og foreslåtte tilleggstiltak skal registreres og leveres til den kompetente databeskyttelsesmyndigheten der det er nødvendig.

Personvernsjefen og Amgen Frankrike vil informere alle deltakende selskaper om vurderingen som er utført og om resultatene, slik at de identifiserte tilleggstiltakene kan brukes der samme type overføringer utføres av andre deltakende selskaper, eller der effektive tilleggstiltak ikke kan settes på plass, blir slike overføringer suspendert eller avsluttet.

12.4. Dataimportøren skal umiddelbart varsle dataeksportøren, Amgen Frankrike og personverndirektøren hvis den har grunn til å tro at den er eller har blitt underlagt lover eller praksis som vil hindre den i å oppfylle sine forpliktelser i henhold til disse EU BCR-ene, inkludert etter en endring i de lokale nasjonale lovene i tredjelandet som beskrevet i artikkel 12.3 eller et tiltak som en opplysningsforespørsel som beskrevet i artikkel 16.3. I tillegg skal

dataeksportørene (i samarbeid med personverndirektøren) kontinuerlig overvåke, og der det er hensiktsmessig med bistand fra dataimportørene, utviklingen i tredjelandene som dataeksportørene har overført personopplysninger til, som kan påvirke den første vurderingen av beskyttelsesnivået for personopplysninger og beslutningene som tas med hensyn til slike overføringer.

12.5. Etter en suspensjon av en overføring, må dataeksportøren avslutte overføringen eller settet med overføringer hvis dataimportøren ikke er i stand til å overholde EU BCR-ene og/eller overholdelse ikke gjenopprettes innen en måned etter suspensjonen. I slike tilfeller må dataimportøren, etter dataeksportørens valg, enten returnere eller ødelegge alle personopplysninger som har blitt overført før suspensjonen, og eventuelle kopier derav.

12.6. Enhver flyt av personopplysninger som ikke er underlagt disse EU BCR-ene og/eller ikke stammer fra et deltakende selskap etablert i et EØS-medlemssland, anses ikke som en overføring av personopplysninger i henhold til disse EU BCR-ene og er følgelig ikke underlagt kravene i disse EU BCR-ene.

13. Opplæringsprogram

13.1. Som beskrevet i vedlegg 2, gir Amgen hensiktsmessig og oppdatert opplæring om personvernprinsipper og mer spesifikt om EUs BCR-ene til alt personell. Denne opplæringen inkluderer også informasjon om konsekvensene i henhold til straffe- og arbeidsrett og/eller deres kontrakt for tjenester for personell som bryter EU BCR-ene.

13.2. Opplæringen er obligatorisk og gjentas årlig. Vellykket deltakelse i opplæring vil bli dokumentert.

13.3. Spesifikke opplæringer vil bli gitt fra sak til sak til personell som har permanent eller regelmessig tilgang til personopplysninger, eller som er involvert i innsamling av personopplysninger eller i utviklingen av verktøy som brukes til å behandle personopplysninger.

13.4. I tillegg gir Amgens Global Privacy Compliance Team passende informasjon og ressurser relatert til personvern, inkludert på Amgens intranettportal.

14. Revisjons- og overvåkingsprogram

14.1. Personverndirektøren sikrer at alle deltakende selskaper (og deres overholdelse av disse EU BCR-ene) er inkludert i revisjons- og overvåkingsprogrammet fra et personvern- og databeskyttelsesperspektiv. Omfattende revisjoner utføres regelmessig, ikke sjeldnere enn hvert 2. til 3. år (for deltakende selskaper med en middels til høy risikoprofil basert på revisjonsavdelingens risikovurderingsmetodikk) og hvert 4. til 5. år (for deltakende selskaper med en lav risikoprofil basert på revisjonsavdelingens risikovurderingsmetodikk), av internrevisjonsteamet eller uavhengige, eksterne sertifiserte revisorer. Omfattende revisjoner inkluderer databeskyttelse og personvernspørsmål innenfor deres omfang (inkludert overholdelse av disse EU BCR-ene, der det er aktuelt for og brukt av et deltakende selskap). I tillegg til omfattende revisjoner, og uten at det berører tidsrammene som er angitt ovenfor, utføres andre revisjonsomfang, inkludert tverrfunksjonelle eller problemspesifikke revisjoner (f.eks. overholdelse av EU BCR-ene), en begrenset revisjon av ett eller flere systemer for behandling av personopplysninger og/eller en begrenset revisjon av én eller flere funksjonelle avdelinger (f.eks. Global Privacy Compliance Team). Revisjonsprogrammet er utviklet og godkjent i samarbeid med revisjonssjefen og Chief Compliance Officer som er

Senior Visepresident. Personverndirektøren, Chief Compliance Officer og Chief Information Officer kan starte ad hoc EUs BCR-relaterte revisjoner når som helst. For eksempel, som svar på et identifisert samsvarsproblem eller en rapport om vesentlig manglende overholdelse, et brudd på personopplysninger og/eller en vesentlig endring i EUs databeskyttelseslover. Revisjonsprogrammet dekker alle aspekter av EU BCR-ene, inkludert metoder for å sikre at korrigerende tiltak vil finne sted.

14.2. Alle EU BCR-enes revisjonsrapporter kommuniseres til Chief Compliance Officer og til personverndirektøren i tide. EU BCR-enes revisjonsoppsummeringer og funn, samt annen relevant informasjon, rapporteres også regelmessig til styret i Amgen Inc. via relevante komiteer (f.eks. Corporate Responsibility and Compliance Committee og/eller revisjonskomiteen til styret), til styret i Amgen Frankrike og (der det er hensiktsmessig, for eksempel i forhold til et funn som krever rettsmiddel) til det relevante deltakende selskapet. Samfunnsansvars- og samsvarskomiteen til styret i Amgen, Inc. møtes fem ganger i året. Personvern og databeskyttelse dekkes årlig, vanligvis i oktobermøtet.

14.3. Den kompetente DPA kan motta en kopi av EU BCR-relaterte revisjonsrapporter på forespørsel.

14.4. Hvert deltakende selskap skal samarbeide med og skal akseptere, uten begrensninger, å bli revidert av den kompetente DPA. Hver revidert enhet må informere personverndirektøren umiddelbart hvis den mottar varsel om slik revisjon eller en slik revisjon finner sted.

15. Samsvar og tilsyn med samsvar

15.1. Amgen utnevner passende personell, inkludert der det er aktuelt et nettverk av ansvarlige for databeskyttelse, med toppledelsesstøtte for å overvåke og sikre overholdelse av databeskyttelsesregler. Personverndirektøren er ansvarlig for Global Privacy Compliance Team som er et globalt team som gir ekspertstøtte over hele verden for Amgen-enheter (inkludert deltakende selskaper).

15.2. I Amgen omfatter personverndirektøren ansvar blant annet:

15.2.1. gi råd til styret;

15.2.2. sikre overholdelse av databeskyttelse på globalt nivå (inkludert å ha det overordnede ansvaret for EU BCR-ene);

15.2.3. regelmessig rapportering om overholdelse av databeskyttelse (inkludert til personverndirektøren); og

15.2.4. arbeide med den kompetente DPAs undersøkelser.

15.3. Global Privacy Compliance Team inkluderer personverndirektøren (som, i tillegg til ansvaret nevnt ovenfor, fører tilsyn med det globale nettverket av databeskyttelsesansvarlige), den europeiske databeskyttelsesansvarlige og andre lokale databeskyttelsesansvarlige. Global Privacy Compliance Team har det overordnede ansvaret for databeskyttelse og personvernsamsvar over hele verden hos Amgen.

15.4. Den europeiske databeskyttelsesansvarlige er utnevnt av Amgen som databeskyttelsesansvarlig for EØS, Storbritannia og Sveits. Den europeiske databeskyttelsesansvarlige har oppgavene som er fastsatt i artikkel 39 i GDPR. Amgen vil

sørge for at oppgavene og pliktene til den europeiske databeskyttelsesansvarlige ikke resulterer i en interessekonflikt med slike oppgaver. Den europeiske databeskyttelsesansvarlige har en direkte rapporteringslinje til personverndirektøren (som er en del av det høyeste ledelsesnivået for Amgen) og støttes av den lokale Compliance Lead i Frankrike. Den europeiske databeskyttelsesansvarlige kan kontakte personverndirektøren hvis det oppstår spørsmål eller problemer under utførelsen av sine oppgaver. Den europeiske databeskyttelsesansvarlige kan kontaktes på: privacy@amgen.com

15.5. På lokalt nivå er databeskyttelsesansvarlige ansvarlige for å håndtere lokale personvernforespørsler fra registrerte, for å sikre overholdelse på lokalt nivå med støtte fra Global Privacy Compliance Team og for å rapportere store personvernproblemer til personverndirektøren. Amgen opprettholder et databeskyttelsesansvarlig nettverk og sikrer at en DPO er utnevnt eller tildelt for hvert land der Amgen har en bedriftsenhet (det deltakende selskapet), og gjeldende lov i jurisdiksjonen til et slikt deltakende selskap krever slik utnevnelse.

15.6. Vanligvis er databeskyttelsesansvarlige enten, eller støttes av, de lokale Compliance Leads som rapporterer til Worldwide Compliance and Business Ethics-avdelingen. Global Privacy Compliance Team er en del av, og rapporterer til, Worldwide Compliance and Business Ethics-avdelingen som ledes av Chief Compliance Officer. Chief Compliance Officer har det overordnede ansvaret for Amgen-konsernets juridiske og regulatoriske overholdelse over hele verden. Sjelden, på grunn av de spesifikke omstendighetene til et deltakende selskap eller andre spesielle omstendigheter, kan databeskyttelsesansvarlig komme fra en annen funksjon, for eksempel Regulatory. Under alle omstendigheter sikrer Global Privacy Compliance Team at databeskyttelsesansvarlige og Compliance Leads er opplært på riktig måte og har et tilstrekkelig nivå av ledelse og kompetanse til å oppfylle hans eller hennes rolle. I tillegg har databeskyttelsesansvarlige en direkte rapporteringslinje til personverndirektøren og støttes av Global Privacy Compliance Team Personnel i tilfelle de trenger ytterligere veiledning.

15.7. Hvert deltakende selskap som fungerer som datakontrollør, skal være ansvarlig for og kunne demonstrere overholdelse av EU BCR-ene. Som en del av dette kravet skal alle deltakende selskaper:

15.7.1. må opprettholde en oversikt over alle kategorier av behandlingsaktiviteter utført i tråd med kravene som er fastsatt i artikkel 30(1) i GDPR. Denne registreringen skal gjøres skriftlig, inkludert i elektronisk form, skal gjøres tilgjengelig for personverndirektøren og den kompetente DPA på forespørsel, og skal inneholde følgende informasjon: (a) navnet og kontaktopplysningene til det deltakende selskapet som fungerer som datakontrollør, dets representant og DPO; (b) formålene med behandlingen; (c) en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger; (d) kategoriene av mottakere som personopplysningene har blitt eller vil bli avslørt for, inkludert mottakere i tredjeland eller internasjonale organisasjoner; (e) der det er aktuelt, overføringer av personopplysninger til et tredjeland eller en internasjonal organisasjon, inkludert identifisering av det tredjelandet eller den internasjonale organisasjonen, og, i tilfelle overføringer som er avhengig av et unntak, dokumentasjon av passende sikkerhetstiltak; (f) der det er mulig, de planlagte tidsgrensene for sletting av de ulike kategoriene av personopplysninger; og (g) der det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene.

15.7.2. utføre konsekvensutredninger for databeskyttelse for behandlingsoperasjoner som sannsynligvis vil resultere i en høy risiko for fysiske personers rettigheter og friheter i samsvar med artikkel 35 i GDPR. Når en vurdering av personvernkonsekvenser i henhold til artikkel 35 indikerer at behandlingen vil resultere i en høy risiko i fravær av tiltak som er iverksatt av det deltakende selskapet for å redusere risikoen, må personverndirektøren konsulteres før behandling, som deretter skal konsultere den kompetente DPA i samsvar med artikkel 36 i GDPR.

16. Tiltak i tilfelle nasjonal lovgivning hindrer overholdelse av EU BCR-ene

16.1. Der et deltakende selskap har grunn til å tro at lovene som gjelder for det, hindrer det deltakende selskapet i å oppfylle sine forpliktelser i henhold til EU BCR-ene eller har en betydelig innvirkning på garantiene gitt av reglene, vil det umiddelbart informere Personvernsjefen (unntatt der det er forbudt av en rettshåndhevende myndighet, for eksempel et forbud i henhold til strafferetten for å bevare konfidensialiteten til en rettshåndhevende etterforskning) og Amgen Frankrike.

16.2. Der det er konflikt mellom lokal nasjonal lovgivning og forpliktelsene i EU BCR-ene, vil personverndirektøren i samarbeid med lokal juridisk rådgiver og den lokale databeskyttelsesansvarlige avgjøre hvilke juridisk passende tiltak som kreves. Ved behov vil personverndirektøren også rådføre seg med den kompetente databeskyttelsesmyndigheten.

16.3. Der eventuelle juridiske krav som et deltakende selskap er underlagt i et tredjeland, sannsynligvis vil ha en betydelig negativ effekt på garantiene gitt av EU BCR-ene, skal Personvernsjefen, Amgen Frankrike, og dataeksportøren umiddelbart varsles av dataimportøren, og personverndirektøren skal varsle den kompetente DPA og (der det er mulig) de registrerte. Dette inkluderer (a) enhver juridisk bindende forespørsel om utlevering av personopplysninger av en rettshåndhevende myndighet eller statlig sikkerhetsorgan, og i et slikt tilfelle bør den kompetente DPA være tydelig informert om forespørselen, inkludert informasjon om dataene som er forespurt, det forespørrende organet og det juridiske grunnlaget for utleveringen og svaret som er gitt (med mindre annet er forbudt, for eksempel et forbud i henhold til straffeloven for å bevare konfidensialiteten til en rettshåndhevende etterforskning), og (b) enhver direkte tilgang fra offentlige myndigheter til personopplysninger overført i henhold til disse EU BCR-ene i samsvar med lovene i bestemmelseslandet, og i slike tilfeller skal slik melding inkludere all informasjon som er tilgjengelig for et slikt deltakende selskap (med mindre annet er forbudt, for eksempel et forbud i henhold til straffeloven for å bevare konfidensialiteten til en rettshåndhevende etterforskning).

16.4. Hvis suspensjonen og/eller varslingen i spesielle tilfeller er forbudt, vil det deltakende selskapet som mottar forespørselen, gjøre sitt beste for å få rett til å frafalle dette forbudet for å kommunisere så mye informasjon som mulig og så snart som mulig og kunne demonstrere (på forespørsel fra dataeksportøren) at det gjorde det.

16.5. Dataimportøren vil med jevne mellomrom gi dataeksportøren så mye relevant informasjon som mulig om de mottatte forespørslene (spesielt antall forespørsler, hvilken type personopplysninger som er forespurt, identiteten til de forespørrende myndighetene, om forespørsler har blitt utfordret og utfallet av slike utfordringer). Dataimportøren vil beholde slik informasjon så lenge personopplysningene er underlagt sikkerhetstiltakene som er gitt av EU BCR-ene, og vil gjøre den tilgjengelig for den kompetente DPA på forespørsel. Hvis dataimportøren er eller blir helt eller delvis forhindret fra å gi dataeksportøren den

foregående informasjonen, vil dataimportøren, uten unødig forsinkelse, informere dataeksportøren om dette.

16.6. Dataimportøren vil, i samarbeid med personverndirektøren, gjennomgå lovligheten av en forespørsel om offentliggjøring fra en offentlig myndighet for å avgjøre om det faller innenfor de myndighetene som er gitt til den anmodende offentlige myndigheten. Dataimportøren vil bestride forespørselen hvis, etter en slik vurdering, den konkluderer (sammen med personverndirektøren) det er rimelig grunn til å vurdere at forespørselen er ulovlig i henhold til lovene i bestemmelseslandet, gjeldende forpliktelser i henhold til folkeretten, og/eller prinsipper for internasjonal høflighet. Hvis dataimportøren mener at det er slike rimelige grunner til å anse forespørselen som ulovlig, vil den forfølge klagemuligheter. Når du utfordrer en forespørsel, vil dataimportøren søke midlertidige tiltak med sikte på å suspendere effektene av forespørselen til den kompetente rettsmyndigheten har bestemt seg for sine fordeler. Dataimportøren vil ikke avsløre de forespurte personopplysningene før det er påkrevd å gjøre det i henhold til gjeldende lov og prosedyreregler i destinasjonslandet. Dataimportøren vil dokumentere sin juridiske vurdering og eventuelle utfordringer mot forespørselen om offentliggjøring og, i den grad det er tillatt i henhold til lovene i bestemmelseslandet, gjøre dokumentasjonen tilgjengelig for dataeksportøren og, på forespørsel, til den kompetente DPA.

16.7. Dataimportøren vil gi et minimum av informasjon som er tillatt når han svarer på en forespørsel om offentliggjøring, basert på en rimelig tolkning av forespørselen.

16.8. Under alle omstendigheter skal overføring av personopplysninger av et deltakende selskap til enhver offentlig myndighet ikke være massiv, uforholdsmessig og vilkårlig på en måte som vil gå utover det som er nødvendig i et demokratisk samfunn.

16.9. For deltakende selskaper som befinner seg i EØS, kan enhver dom fra en domstol eller et tribunal og enhver avgjørelse fra en administrativ myndighet i et tredjeland som krever at en datakontrollør eller databehandler overfører eller utleverer personopplysninger, bare anerkjennes eller håndheves på noen måte hvis den er basert på en internasjonal avtale, for eksempel en avtale om gjensidig juridisk bistand, som er i kraft mellom det anmodende tredjelandet og EU eller et EØS-medlemsland, uten at det berører andre grunner for overføring i henhold til kapittel V GDPR.

17. Interne klagemekanismer

17.1. Amgen vil benytte sin eksisterende klagehåndteringsprosess for å innlemme håndtering av eventuelle EU BCR-relaterte klager eller bekymringer.

17.2. Enhver registrert kan når som helst klage på at ethvert deltakende selskap ikke overholder EU BCR-ene. Slike klager vil bli behandlet av Global Privacy Compliance Team under ledelse av personverndirektøren og i samarbeid med den relevante lokale databeskyttelsesansvarlige.

17.3. Amgen anbefaler at slike klager leveres skriftlig enten via post eller e-post direkte til Global Privacy Compliance Team eller til det deltakende selskapet. Global Privacy Compliance Team kan kontaktes ved hjelp av kontaktinformasjonen nedenfor:

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

E-post: privacy@amgen.com

17.4. Amgen-personell kan l, når det er akseptabelt i henhold til lovene som gjelder for det deltakende selskapet, bruke Hotline for forretningsadferd til å rapportere en EU BCR-klage.

17.5. Hvis klagen mottas lokalt av det deltakende selskapet, vil DPO oversette om nødvendig og videresende den uten unødig forsinkelse til Global Privacy Compliance Team.

17.6. Et første svar vil bli gitt til den registrerte innen ti (10) virkedager som informerer han/henne om at deres klage er under behandling, og at han/hun vil motta substansielt svar uten unødig forsinkelse og under alle omstendigheter innen en måned etter mottak av forespørselen. Tatt i betraktning kompleksiteten og antallet forespørsler, kan perioden på én måned forlenges med maksimalt to ytterligere måneder, i hvilket tilfelle den registrerte skal informeres om dette. Det substansielle svaret vil inkludere detaljer om funnene våre og eventuelle tiltak Amgen har eller foreslår å iverksette. Hvis Amgen fastslår at ingen tiltak skal iverksettes, skal dette forklares for den registrerte sammen med årsakene til denne fastsettelsen.

17.7. Hvis klagen opprettholdes av Amgen, vil Amgen iverksette egnede korrigerende tiltak. Disse tiltakene vil bli avgjort fra sak til sak av personverndirektøren og Global Privacy Compliance Team, den lokale DPO og, der det er aktuelt, enhver annen relevant avdeling. Videre, hvis Global Privacy Compliance Team oppdager individuelle forseelser, vil passende disiplinære tiltak bli iverksatt, opp til og inkludert oppsigelse av ansettelse eller engasjement, i den grad det er tillatt i henhold til gjeldende lov.

17.8. Den registrerte vil motta et svar som informerer han/henne om utfallet av klagen. Dette skal være uten unødig forsinkelse og under alle omstendigheter innen en måned etter mottak av klagen (med tilstrekkelige detaljer til at Amgen kan identifisere arten av klagen og, bare der det er rimelig nødvendig, med all informasjon som kreves for å bekrefte klagerens identitet). Tatt i betraktning kompleksiteten og antallet forespørsler, kan perioden på én måned forlenges med maksimalt to ytterligere måneder, i hvilket tilfelle den registrerte skal informeres om dette.

17.9. Den registrerte vil bli informert om at hvis han/hun ikke er fornøyd med Amgens svar, kan han/hun fremme et krav for domstolene i et EØS-medlemsland eller den kompetente databeskyttelsesmyndigheten. Det er imidlertid ikke et krav at en registrert først går gjennom Amgens klagebehandlingsprosess før han eller hun kan klage til den kompetente databeskyttelsesmyndigheten eller fremme et krav for domstolene i et EØS-medlemsland.

17.10. Denne klagebehandlingsprosessen vil bli offentliggjort gjennom publiseringen av EU BCR-ene som nevnt i artikkel 7 ovenfor.

18. Tredjepartsmottakers rettigheter og ansvar

18.1. En registrert hvis personopplysninger stammer fra EØS eller er beskyttet av EUs databeskyttelseslover og overføres til deltakende selskaper utenfor EØS, skal ha rett til å håndheve EU BCR-ene som en tredjepartsbegunstiget og skal ha rett til å søke rettslig oppreisning, få rettsmidler og, der det er hensiktsmessig, kompensasjon for faktisk skade som følge av brudd på disse EU BCR-ene. Eventuelle slike krav kan fremmes av den registrerte for en kompetent DPA (som kan være DPA i EØS-medlemslandet der den registrerte vanligvis bor, eller DPA på hans/hennes arbeidssted eller DPA på stedet for den påståtte overtredelsen). Registrerte kan også fremme et krav for en kompetent domstol i et EØS-medlemsland (som kan være domstolene i EØS-medlemslandet der det relevante deltakende selskapet har et driftssted eller domstolene i EØS-medlemslandet der den

registrerte har sitt vanlige bosted). En registrert kan være representert i utøvelsen av sin rett til et effektivt rettsmiddel mot et deltakende selskap av et ikke-for-profitt-organ, organisasjon eller forening, forutsatt at et slikt organ, organisasjon eller forening har blitt riktig konstituert i samsvar med gjeldende lov, har lovbestemte mål som er i allmennhetens interesse, og er aktiv innen beskyttelse av registrerte rettigheter og friheter knyttet til beskyttelse av deres personopplysninger. Den registrerte skal kunne håndheve følgende artikler som en tredjepartsbegunstiget:

18.1.1. Artikkel 1 (Omfang), 2 (Definisjoner), 3 (Formålsbegrensning), 4 (Datakvalitet og proporsjonalitet), 5 (Rettslig grunnlag for behandling av personopplysninger) og 6 (Behandling av sensitive personopplysninger);

18.1.2. Artikkel 7 (Innsyn og informasjonsrettigheter);

18.1.3. Artikkel 8 (Rett til tilgang, retting, sletting og begrensning av data) og 9 (Automatiserte individuelle beslutninger);

18.1.4. Artikkel 10 (Sikkerhet og konfidensialitet), 11 (Forhold til databehandlere (Amgen Dataimportør eller Leverandør) og 12 (Begrensning av overføringer og videreoverføringer);

18.1.5. Artikkel 16 (Handlinger i tilfelle av nasjonal lovgivning som hindrer overholdelse av EU BCR-ene) og 21 (Forholdet mellom nasjonale lover og EU BCR-ene);

18.1.6. Artikkel 18 (Tredjepartsrettigheter og -ansvar); og

18.1.7. Artikkel 19 (Gjensidig bistand og samarbeid med databeskyttelsesmyndighetene).

18.2. For å unngå tvil, omfatter tredjepartsrettighetene ikke de artiklene og elementene i disse EU BCR-ene som gjelder interne mekanismer implementert i deltakende selskaper eller Amgen-gruppen, slik som detaljer om opplæring (inkludert vedlegg 2), revisjonsprogrammer, interne samsvarsnettverk og struktur og mekanismen for oppdatering av EU BCR-ene.

18.3. Amgen Frankrike påtar seg ansvaret for og samtykker i å iverksette slike tiltak som er rimelig nødvendige for å rette opp handlingene til deltakende selskaper etablert utenfor EØS. Amgen Frankrike skal betale erstatning for materielle eller ikke-materielle skader som følge av brudd på disse EU BCR-ene, med mindre det kan påvise at det deltakende selskapet etablert utenfor EØS ikke er ansvarlig for hendelsen som forårsaket skaden. Amgen Frankrike har tilstrekkelige økonomiske midler og forsikringsdekning til å dekke skader i henhold til EU BCR-ene.

18.4. Alle registrerte som har lidd skade som følge av brudd på disse EU BCR-ene av et deltakende selskap som ikke er etablert i EØS, har rett til, der det er hensiktsmessig, å motta kompensasjon fra Amgen Frankrike for skaden de har lidd, og domstolene eller andre kompetente myndigheter i EØS skal ha jurisdiksjon. Den registrerte skal ha rettighetene og rettsmidlene mot Amgen Frankrike som om overtredelsen hadde blitt forårsaket av Amgen Frankrike i EU i stedet for det deltakende selskapet som ikke er etablert i EØS. Hvis det deltakende selskapet som ikke er etablert i EØS, er ansvarlig eller holdes ansvarlig for et slikt brudd, vil det i den grad det er ansvarlig eller erstatningspliktig, holde Amgen Frankrike skadesløs for enhver kostnad, utlegg, skade, utgift eller tap Amgen Frankrike pådrar seg i forbindelse med et slikt brudd.

18.5. I tilfelle et krav fra en registrert om at han/hun har lidd skade og har fastslått at det er sannsynlig at slik skade oppstod på grunn av brudd på disse EU BCR-ene, skal bevisbyrden for å vise at skadene som den registrerte har lidd på grunn av brudd på disse EU BCR-ene, ikke kan tilskrives relevant deltakende selskap, ligge hos Amgen Frankrike. Hvis Amgen Frankrike kan påvise at det deltakende selskapet etablert utenfor EØS ikke er ansvarlig for hendelsen som forårsaket skaden, skal det ikke være ansvarlig eller belastbar for skaden.

19. Gjensidig bistand og samarbeid med databeskyttelsesmyndighetene

19.1. Deltakende selskaper skal samarbeide og hjelpe hverandre med å håndtere en forespørsel eller klage fra en registrert eller en undersøkelse eller forespørsel fra den kompetente databeskyttelsesmyndigheten.

19.2. Deltakende selskaper vil, i samarbeid med personverndirektøren, svare på EU BCR-relaterte forespørsler fra den kompetente DPA innen en passende tidsramme i lys av omstendighetene rundt forespørselen (og i alle fall ikke senere enn en frist pålagt av den kompetente DPA) og i en passende detalj basert på informasjonen som er rimelig tilgjengelig for det deltakende selskapet. I forhold til implementering og kontinuerlig anvendelse av EU BCR-ene, skal deltakende selskaper ta behørig hensyn til kommunikasjon og anbefalinger fra den kompetente DPA og skal overholde eventuelle formelle beslutninger eller merknader utstedt av den kompetente DPA.

19.3. Eventuelle tvister knyttet til en kompetent DPAs utøvelse av tilsyn med overholdelse av disse EU BCR-ene vil bli løst av domstolene i medlemslandet til den DPA, i samsvar med gjeldende lov i det aktuelle medlemslandet.

20. EU BCR-ene oppdatering og endringer

20.1. Amgen forbeholder seg retten til å endre og/eller oppdatere disse EU BCR-ene når som helst. En slik oppdatering av EU BCR-ene kan være nødvendig spesielt som følge av nye juridiske krav, betydelige endringer i Amgen-konsernets struktur eller offisielle krav pålagt av den kompetente DPA.

20.2. Amgen vil umiddelbart og uten unødig forsinkelse rapportere vesentlige endringer i EU BCR-ene eller i listen over deltakende selskaper til alle andre deltakende selskaper og til den kompetente DPA for å ta hensyn til endringer i gjeldende lov, regelverket og/eller Amgen-konsernets struktur. Spesielt der en endring vil påvirke beskyttelsesnivået som tilbys av EU BCR-ene, vil personverndirektøren umiddelbart kommunisere slik endring på forhånd til den kompetente DPA med en kort forklaring på årsakene til endringen. Noen endringer kan kreve en ny godkjenning fra den kompetente DPA.

20.3. Personverndirektøren vil holde en fullstendig oppdatert liste over de deltakende selskapene i EU BCR-ene og spore eventuelle oppdateringer av reglene, samt gi den nødvendige informasjonen til de registrerte eller den kompetente databeskyttelsesmyndigheten ved forespørsel. Eventuelle administrative endringer i EU BCR-ene vil bli rapportert til deltakende selskaper med jevne mellomrom.

20.4. Ingen overføring av personopplysninger vil bli gjort til et nytt deltakende selskap under garantiene i EU BCR-ene før det nye deltakende selskapet er effektivt bundet av EU BCR-ene og i samsvar med EU BCR-ene.

20.5. Eventuelle administrative endringer i EU BCR-ene eller til listen over deltakende selskaper vil bli rapportert til de deltakende selskapene regelmessig og rapportert minst en gang i året til den kompetente DPA med en kort forklaring om årsakene til oppdateringen.

20.6. Vesentlige endringer i EU BCR-ene vil også bli kommunisert til de registrerte på en hvilken som helst måte i henhold til artikkel 7 i EU BCR-ene.

21. Forholdet mellom nasjonale lover og EU BCR-ene

21.1. Der de lokale nasjonale lovene som gjelder for et deltakende selskap krever et høyere beskyttelsesnivå for personopplysninger, vil det ha forrang over EU BCR-ene. Hvis de lokale nasjonale lovene som gjelder for et deltakende selskap, gir et lavere beskyttelsesnivå for personopplysninger enn EU BCR-ene, vil EU BCR-ene bli brukt.

21.2. I tilfelle forpliktelser som følger av de lokale nasjonale lovene som gjelder for et deltakende selskap, er i konflikt med EU BCR-ene, skal det deltakende selskapet informere personverndirektøren uten unødig forsinkelse og skal overholde tilleggskravene fastsatt i artikkel 16 ovenfor.

21.3. Under alle omstendigheter skal personopplysninger behandles i samsvar med artikkel 5 i GDPR og relevant lokal lovgivning.

22. Avsluttende bestemmelser

22.1. EU BCR-ene skal tre i kraft etter godkjenning av den kompetente databeskyttelsesmyndigheten og gjelde for de deltakende selskapene ved signering av EUs BCR-adopsjonsavtale.

22.2. Ingen overføring skal gjøres til et deltakende selskap med mindre det er bundet av disse EU BCR-ene. Når en dataimportør slutter å være bundet av EU BCR-ene, må den umiddelbart returnere eller slette alle personopplysninger (inkludert kopier av disse) som er overført i henhold til disse EU BCR-ene, bortsett fra at forutsatt at dataimportøren gir juridisk bindende forpliktelser til å opprettholde beskyttelse av personopplysningene i samsvar med kapittel V i GDPR, kan den beholde personopplysninger som er overført i henhold til disse EU BCR-ene.

22.3. Dataimportøren må umiddelbart informere dataeksportøren, Amgen Frankrike og personverndirektøren hvis de av en eller annen grunn ikke er i stand til å overholde disse EU BCR-ene (inkludert situasjonene beskrevet i artikkel 12.3 ovenfor). Hvis dataimportøren bryter disse EU BCR-ene, eller ikke er i stand til å overholde dem, må dataeksportøren varsle personverndirektøren og suspendere overføringen av personopplysninger.

22.4. Etter dataeksportørens valg må dataimportøren umiddelbart returnere eller slette alle personopplysninger (inkludert kopier av disse) som er overført i henhold til disse EU BCR-ene, og skal sertifisere det samme til dataeksportøren, der:

22.4.1. dataeksportøren har suspendert overføringen av personopplysninger, og overholdelsen av disse EU BCR-ene ikke gjenopprettes innen rimelig tid, og under alle omstendigheter innen en måned etter suspensjonen; eller

22.4.2. dataimportøren er i vesentlig brudd på disse EU BCR-ene; eller

22.4.3. dataimportøren unnlater å overholde en bindende beslutning fra en kompetent domstol eller kompetent DPA om sine forpliktelser i henhold til disse EU BCR-ene.

Inntil personopplysningene er slettet eller returnert, må dataimportøren fortsette å sikre overholdelse av disse EU BCR-ene. Hvis lokale nasjonale lover som gjelder for dataimportøren, forbyr retur eller sletting av personopplysningene som overføres i henhold til disse EU BCR-ene, må dataimportøren fortsette å sikre overholdelse av disse EU BCR-ene og bare behandle personopplysningene i den grad og så lenge det kreves i henhold til slike lokale nasjonale lover.

23. Vedlegg

Vedlagte vedlegg er en integrert del av EU BCR-ene.

Vedlegg 1: Oversikt over Amgen-datastrømmer

Vedlegg 2: Oversikt over Amgens opplæringsprogram

Vedlegg 1: Oversikt over Amgen-datastrømmer

Registrerte personer	Datakategorier	Formål	Overfør
Ansatt	Identifikasjonsdata som navn, adresse, fødselsdato og fødested, ansettelsesdato, personnummer, kredittkortnummer, bankkonto og finansiell informasjon, og førerkort og offentlig utstedte identifikasjonskortnumre Ferier og fordeler, klager, bonuser, forfremmelser, anmeldelser og evalueringer, arbeidsjournaler, informasjon relatert til helse- og velferdsdekning, pensjonsplan og aksjeopsjonsdetaljer Personopplysninger om skatt og økonomi Sensitive data som nasjonal opprinnelse, når det er tillatt i henhold til lokal lovgivning	Personaladministrasjon, informasjonsteknologistøtte og administrasjonsformål i forbindelse med ansettelsesforholdet og ytelser, eller administrasjon av ytelser etter ansettelse, samt for å overholde Amgens juridiske, administrative og bedriftsmessige forpliktelser	Amgens globale databaser er lokalisert i USA der Amgen Inc., hovedkontoret, har sin base. Data flyter fra Amgen Frankrike (eller den relevante dataeksportøren) til Amgen Inc. i USA eller til deltakende selskaper i Sveits. Deretter kan dataene: - bare lagres og vedlikeholdes der - analyseres for å gi global statistikk og rapporter - deles videre innenfor Amgen-konsernet til andre deltakende selskaper der det er et forretningsbehov for slik tilgang av spesifikt personell eller forretningsfunksjoner i de deltakende selskapene (f.eks. en ansatt som søker på en jobb utenfor sitt land eller må rapportere til en leder med base utenfor sitt land). I de fleste tilfeller vil slike deltakende selskaper fungere som datakontrollører, men avhengig av forretningsbehovet kan
Helsepersonell	Navn, forretningskontaktinformasjon, inkludert telefonnummer og e-postadresse, fagfelt Profesjonell bakgrunn (CV) Deltakelse i annen forskning Finansiell informasjon (fakturerings- og betalingsinformasjon)	Administrasjon og styring av Amgens faglige og vitenskapelige aktiviteter – Forskning og utvikling (for eksempel deltakelse i medisinsk forskning, kliniske studier, faglige møter eller kongresser) Markedsføring av Amgens produkter og tjenester Offentliggjøring av finansiell informasjon når det kreves av gjeldende lov eller overholdelse av bransjeregler Overholdelse av forskrifter som sikkerhetsovervåking og rapportering av uønskede hendelser	

Leverandører	Individuelt navn, organisasjonsnavn, forretningskontaktinformasjon Fakturerings- og betalingsinformasjon	Behandling av betalinger til leverandører og underleverandører Overholdelse av forskrifter som skatterett	deltakende selskaper også fungere som databehandlere (f.eks. ved å gi IT-helpdesk-støtte eller gi støtte knyttet til HR Connect servicesenter).
Pasienter i kliniske studier (som kan inkludere barn under 18 år hvor det er en pediatrisk pasient involvert i en klinisk studie sponset av Amgen).	Kodede data – pasientnavn og kontaktinformasjon erstattes med et internt generert identifikasjonsnummer. Kun det kliniske utprøvingsstedet (sykehus/forskningssted) beholder listen for å knytte identifikasjonsnummeret tilbake til pasientens navn. Indirekte identifikatorer som fødselsår eller fødselsdato (full fødselsdato samles bare inn for pediatriske studier), kjønn, vekt, høyde. Nødvendige helsedata som skissert i forskningsstudieprotokollen. Andre data relatert til pasienten som er nødvendige for gjennomføringen av forskningen, inkludert etnisitet, familiesituasjon (for eksempel antall barn), forbruk av narkotika, alkohol, narkotika, generelle vaner eller atferd, yrkessituasjon som jobb, arbeidsledighet, deltakelse i annen forskning.	Administrasjon og styring av biomedisinsk forskning (kliniske studier, observatoriestudier)	
Pasienter (som kan inkludere barn under 18 år hvor det er en bivirkning som involverer bruk av et Amgen-produkt med en pediatrisk	Indirekte identifikatorer for pasienten som alder, fødselsår eller fødselsdato, pasientinitialer (som tillatt av lokal lov), kjønn, vekt / høyde eller identifikasjonsnummer for pasienten (unntatt nasjonale helseidentifikatorer).	Overholdelse av forskrifter og legemiddelovervåking, som sikkerhetsovervåking og bivirkningsrapportering (når det er tillatt i henhold til lokale lover)	

indikasjon).	Data relatert til identifikasjon av Amgen-produktet, slik som produktet eller enheten som brukes, serienummer på enheter, leveringsmetode eller dosering av produktet, produktets parti-/ batchnummer. Helsedata, inkludert administrerte behandlinger, resultater av undersøkelser, type uønsket (e) effekt(er), personlig eller familiær sykehistorie, tilknyttede sykdommer eller hendelser, risikofaktorer, informasjon knyttet til forskrivning og bruk av legemidler og til den terapeutiske atferden til helsepersonell som er involvert i behandlingen av pasientens sykdom. Andre data relatert til pasienten som er nødvendige for vurderingen av den negative helsetilstanden i samsvar med lovpålagte forpliktelser som etnisitet, yrkesliv, forbruk av narkotika, alkohol, narkotika og/eller generelle vaner eller atferd.		

Vedlegg 2: Oversikt over Amgens opplæringsprogram

Opplæring i personvern og databeskyttelse/bevissthetsprogram

Opplæringsprogrammet for personvern og databeskyttelse bestreber seg på å sikre at alt Amgen-personell er riktig opplært om Amgen EU BCR-ene, samt eventuelle juridiske forpliktelser som påvirker behandling av personopplysninger. Dette programmet inneholder ulike elementer.

Generell opplæring for alt Amgen-personell

Alt Amgen-personell må gjennomføre en årlig nettbasert opplæring i databeskyttelse som en del av opplæring i etiske retningslinjer. Denne opplæringen er obligatorisk og overvåket og tar vanligvis rundt 75 minutter å fullføre. Denne opplæringen inkluderer EU BCR-ene og informasjon om konsekvensene i henhold til straffe- og arbeidsrett og/eller deres kontrakt for tjenester for personell som bryter EU BCR-ene.

Spesifikk opplæring til DPO-er

Alle Amgen DPO-er blir regelmessig opplært i nye prosesser gjennom regelmessige DPO-samtaler utført av Global Privacy Compliance Team og personvern-workshops på stedet og/eller online etter behov. Alle databeskyttelsesansvarlige har tilgang til en wikiside som besvarer de vanligste spørsmålene og gir veiledning samt koblinger til eksterne ressurser.

Spesifikk opplæring til personell

Spesifikk opplæring kan leveres etter behov, enten online eller på stedet, eller ved å legge ut informasjon på Amgens intranett. Denne opplæringen kan være fokusert på bestemte grupper som enten kan behandle personopplysninger på daglig basis eller støtte andre grupper som behandler personopplysninger. For eksempel blir revisjonsgruppen, FoU-funksjoner og juridisk avdeling regelmessig opplært. Dette inkluderer informasjon om prosedyrer for å administrere forespørsler om tilgang til personopplysninger fra offentlige myndigheter, der det er relevant for spesifikt personell. Denne opplæringen kan skje enten på regionalt nivå eller på landsnivå. Ytterligere spesifikk EU BCR-opplæring kan utvikles ved behov.

Bevissthet

Amgen har en dedikert side på sitt intranett om personvern og databeskyttelse som gir koblinger til andre ressurser enten internt eller eksternt.

Amgens Global Privacy Compliance Team samarbeider med informasjonssikkerhetsavdelingen om Sentinel-programmet som er et globalt program for å øke bevisstheten til Amgen-personell om informasjonssikkerhet.

Opplæringsstøtte

Alle personvernrelaterte opplæringer er utviklet av Global Privacy Compliance Team og godkjent av personverndirektøren. Opplæringen kan enten utføres direkte av et medlem av Global Privacy Compliance Team eller av en lokal DPO på en "lær opp opplæreren" -modell.