Amgen Binding Corporate Rules (BCR) offentlig dokument

Innledning:

Amgen er en leder innen bioteknologi som forplikter seg til å betjene pasienter med alvorlig sykdom.

BCR (Binding Corporate Rules)-reglene uttrykker Amgens forpliktelse til fortrolighet og personvern, fordi selskapet forsøker å sørge for tilstrekkelig beskyttelse av overføring og behandling av personlig informasjon mellom Amgen-enheter.

Alle juridiske enheter i Amgen og alle ansatte forplikter seg til å respektere BCR-reglene. Manglende overholdelse kan føre til disiplinære tiltak, slik stedets lover tillater.

Complianceansvarlig (Chief Compliance Officer) i samarbeid med personvernsansvarlig (Chief Privacy Officer) sørger for at disse reglene blir håndhevet.

BCR-reglene er blitt vedtatt i henhold til de gjeldende EU-bestemmelsene om beskyttelse av personopplysninger, som EU-direktiv 95/46/EF og 2002/58/EF.

1 - Omfang

Amgens BCR-regler gjelder for automatisk eller manuell overføring og håndtering av all personlig informasjon om ansatte, kunder, leverandører, aksjonærer, pasienter og alle andre dataemner som er utført av et av Amgens selskaper som fungerer som kontrollør i et hvilket som helst av følgende tilfeller:

a) Amgen-selskapet som behandler personopplysninger og er etablert i et regulert land; eller

b) Amgen-selskapet som behandler personopplysninger, men er ikke etablert i et regulert land ("dataimportør") og har mottatt personopplysninger fra et Amgen-selskap etablert i et regulert land som definert i artikkel 2 ("dataeksportør").

Disse BCR-reglene gjelder også for videreoverføring av personopplysninger fra dataimportører til dataimportører.

2 - Definisjoner

Vilkår	Definisjoner
Personopplysninger	Informasjon om en person hvis identitet er tydelig eller kan fastslås av informasjonen, ved direkte eller indirekte metoder. Alternativt kan personopplysninger betraktes som informasjon som kan, enten alene eller i kombinasjon med annen informasjon, identifisere eller bli brukt til å kontakte eller finne en enkeltperson. Eksempler på personopplysninger kan inkludere følgende, avhengig av lokale personopplysningslover: • En persons navn, adresse, personnummer, førerkortnummer, finansiell kontoinformasjon, familieinformasjon eller medisinske opplysninger, • Navnet, faglig utdanningen og forskriftspraksisen til en lege, • E-postadressen og annen identifiserende informasjon levert av besøkende på en Amgen-nettside. Ovenstående liste er kun ment å være et eksempel og ikke uttømmende.
Sensitive personopplysninger	Informasjon om et dataemne: • Medisinske eller helsemessige forhold (fysisk eller psykisk) • Finansiell informasjon • Rase eller etnisk opprinnelse • Politiske meninger • Religiøs eller filosofisk overbevisning • Medlemskap i fagforening • Seksuell preferanse • Domfelt for kriminelle handlinger eller arrestasjonshistorie Amgen anser sensitiv informasjon å være informasjon som kan brukes til å begå identitetstyveri, for eksempel personnummer, førerkortnummer, kredittkort- eller annen bankkontoinformasjon.
Dataemne	Personen informasjonen gjelder. Et dataemne kan (blant annet) være en: • Pasient/forbruker/klinisk studiekandidat • Helsepersonell (for eksempel lege eller klinisk sykepleier) • Ansatt (nåværende, tidligere eller pensjonert) • Entreprenør/innehaver/leverandør/konsulent
Kontrollør (datakontrollør)	Enhver enhet som tar beslutninger med hensyn til innsamling og behandling av personopplysninger, herunder beslutninger om formålene med og hvordan personopplysninger behandles.
Databehandler	En person eller enhet som behandler personopplysninger på vegne av en kontrollør.

Behandling	Enhver handling eller gruppe handlinger som er utført på personopplysninger, også ved hjelp av automatiske midler, slik som oppsamling, se på, ha tilgang til, lagre, registrere, organisere, tilpasse eller endre, hente ut, gi råd om, bruke, fremlegge ved overføring, spre eller ellers gjøre tilgjengelig, justere eller kombinere, blokkere, slette eller destruere.
Tredjepart	Fysisk eller juridisk person, offentlig myndighet, byrå eller annen enhet enn dataemnet, kontrolløren og de personene som, under kontrollørens direkte myndighet, har fullmakt til å behandle. Hos Amgen anses en leverandør å være en tredjepart.
Leverandør	Enhver person, bedrift eller organisasjon som leverer varer og/eller tjenester til Amgen, er under et kontraktsforhold, og/eller er mottaker av personopplysninger fra Amgen som er pålagt å levere disse varer og/eller tjenester.
Datatilsyn	En eller flere offentlige myndigheter som er ansvarlige for å overvåke innenfor sitt territorium overholdelse av de bestemmelser som er vedtatt av medlemsstatene i henhold til direktiv 95/46. Disse myndighetene handler med fullstendig uavhengighet når de utøver de oppgavene som de er betrodd.
Regulert land	Et land i det europeiske økonomiske samarbeidsområde (EØS) eller et land med tilstrekkelig grad av personvern som bekreftet ved en beslutning fra EU-kommisjonen eller andre land som anerkjenner BCR-reglene som legitime måter å overføre personopplysninger utenfor sin jurisdiksjon, er land som Andorra, Argentina, Canada, Færøyene, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Sveits, Uruguay.
Dataeksportør	En Amgen-enhet som fungerer som en datakontrollør og er etablert i et regulert land som overfører personopplysninger til en annen Amgen-enhet som ikke er etablert i et regulert land (dataimportør)
Dataimportør	En Amgen-enhet som ikke er etablert i et regulert land som mottar personopplysninger fra en dataeksportør
Tekniske og organisatoriske sikkerhetsforanstaltninger	Tiltak som har til formål å beskytte personopplysninger mot utilsiktet eller ulovlig destruksjon eller utilsiktet tap, endring, uautorisert avsløring eller tilgang, spesielt når prosessen omfatter overføring av informasjon over et nettverk og mot alle andre ulovlige former for behandling.
Deltakende selskap	En juridisk enhet i Amgen-gruppen som er bundet av BCR-reglene.
Samtykke	Eventuelle spesifikke og informerte indikasjoner på dataemnets ønsker, hvorved dataemnet indikerer samtykke til innsamling og behandling av personopplysninger om vedkommende.
Data Protection Officer	Bedriftsmedarbeider som har blitt identifisert og nominert av ledelsen i et søsterselskap eller forretningsenhet som ansvarlig for tilsynet med personvern og databeskyttelse på lokalt nivå, samt implementering av hensiktsmessige og nødvendige kontroller.

Amgen tolker vilkårene i BCR-reglene i henhold til EU-direktivene 95/46/EF og 2002/58/EF, som er nevnt nedenfor som EU-direktivene.

3 – Formålsbegrensninger

Personopplysninger skal behandles for eksplisitte, spesifikke og legitime formål i henhold til artikkel 6.1 (b) i direktiv 95/46.

Personopplyninger skal ikke behandles på måter som er uforenlige med de legitime formålene som personopplysninger ble samlet inn på. Dataimportører er forpliktet til å overholde opprinnelige formål når informasjonen lagres og/eller viderebehandles eller bruker informasjon som er overført til dem fra et annet søsterselskap. Formålet med databehandlingen kan kun endres med samtykke fra dataemnet eller i den utstrekning det er tillatt i lokal lovgivning, som dataeksportøren overfører opplysningene til.

Sensitiv data vil bli gitt ytterligere sikkerhetstiltak som følger av EU-direktiv 95/46/EF.

4 - Datakvalitet og forholdsmessighet

Personopplysninger må være faktisk korrekt, og der det er nødvendig, holdes oppdatert. Passende tiltak må tas for å sikre at feilaktige eller ufullstendige opplysninger korrigeres eller slettes.

Personopplysninger skal være tilstrekkelige og relevante, i henhold til artikkel 6.1 (c) i direktiv 95/46.

Databehandling vil bli styrt av målet om å begrense innsamling, behandling og/eller bruk av personopplysninger til bare det som er nødvendig, dvs. så få personopplysninger som mulig. Muligheten for anonym eller pseudonym data må benyttes, forutsatt at kostnaden og innsatsen involvert står i forhold til ønsket formål.

Personopplysninger som ikke lenger er nødvendige for virksomhetsformålet som de opprinnelig ble samlet inn og lagret for, må slettes i henhold til Amgen Record Retention Schedule. I tilfelle lovbestemte oppbevaringsperioder eller juridisk ventetid gjelder, blir opplysningene blokkert i stedet for slettet. Ved slutten av oppbevaringsperioden eller juridisk ventetid vil opplysningene bli slettet.

5 - Juridisk grunnlag for behandling av personopplysninger

Behandling av personopplysninger er bare tillatt dersom minst en av følgende forutsetninger er oppfylt:

- Dataemnet har fritt og entydig gitt sitt informerte samtykke
- Behandlingen er nødvendig for utførelsen av en kontrakt som dataemnet er en del av eller har et lignende tillitsforhold til, eller for å iverksette tiltak etter anmodning fra dataemnet før inngåelse av en kontrakt
- Behandlingen er nødvendig for å overholde en juridisk forpliktelse som kontrolløren er underlagt eller er fastsatt eller tillagt ved gjeldende lover eller forskrifter
- Behandlingen er nødvendig for å beskytte dataemnets vitale interesser, for eksempel liv, helse eller sikkerhet
- Behandlingen er nødvendig for utførelsen av en oppgave utført i offentlighetens interesse eller i utøvelse av offentlig myndighet gitt til kontrollør eller en tredjepart, som har mottatt og fått opplysningene
- Behandlingen er nødvendig for legitime interesser av kontrolløren eller tredjepart eller de partene der opplysningene blir formidlet til, med unntak av når slike interesser blir tilsidesatt av de legitime interessene for dataemnets grunnleggende rettigheter og selvstendighet.

6 – Behandling av sensitive opplysninger

Hvis Amgen ifølge et bestemt og legitimt formål må behandle sensitive opplysninger, vil Amgen kun gjøre det hvis:

- Dataemnet har gitt sitt eksplisitte samtykke til behandling av slike sensitive opplysninger, unntatt der gjeldende lover forbyr databehandling
- Behandlingen er nødvendig for å utføre forpliktelser og spesifikke rettigheter til kontrolløren innenfor arbeidsrettens område i den utstrekning det er tillatt etter nasjonal lovgivning hvor det gis tilstrekkelige garantier
- Behandlingen er nødvendig for å beskytte dataemnets interesser eller interessene til en annen person når dataemnet er fysisk eller juridisk ute av stand til å gi sitt samtykke
- Behandlingen utføres i henhold til den legitime virksomheten til en stiftelse, forening eller enhver annen ideell organisasjon med et politisk, filosofisk, religiøst eller fagforeningsmål, sammen med hensiktsmessige garantier og under forutsetning av at behandlingen bare gjelder medlemmene eller personer som har regelmessig kontakt med den i forbindelse med formålene, og at opplysningene ikke blir gitt videre til en tredjepart uten samtykke fra dataemnene
- Behandlingen relaterer til sensitive opplysninger som åpenbart er publisert av dataemnet
- Behandlingen av sensitive opplysninger er nødvendig for å etablere, utøve eller forsvare juridiske krav
- Behandlingen av sensitive opplysninger er nødvendig for formålet for forebyggende medisin, medisinsk diagnose, omsorg eller behandling eller forvaltning av helsetjenester, og hvor sensitive opplysninger behandles av helsefaglig personale i henhold til nasjonal lovgivning eller regler etablert av nasjonale kompetente organer med hensyn til taushetsplikt, eller av en annen person som også er underlagt en tilsvarende taushetsplikt

7 - Åpenhet og informasjonsrettighet

Alle søsterselskaper skal behandle personopplysninger på en gjennomsiktig måte. Amgen er forpliktet til å gjøre BCR-reglene, inkludert kontaktinformasjon, lett tilgjengelig for alle dataemner, og dessuten informere dataemner om eventuell overføring og behandling av deres personopplysninger.

For å gjøre dette vil Amgen bruke ulike kommunikasjonsmidler, som bedriftens nettsteder, inkludert interne nettsteder og nyhetsbrev, kontrakter og ytterlige spesifikke personvernerklæringer.

Dataemner hvis personopplysninger behandles av et søsterselskap skal gis følgende opplysninger:

- Identiteten til kontrolløren(e) og eventuelt dens/deres representant,
- Formålet med behandlingen som opplysningene er ment for,
- Opprinnelsen til opplysningen (med mindre dette er personopplyninger samlet inn direkte fra dataemnet)
- Ytterligere informasjon som:

  i) mottakere eller kategorier av datamottakere,

  ii) eksistensen av retten til tilgang til, og retten til å rette opp opplysningene om ham eller henne så langt som slik ytterligere informasjon er nødvendig, med hensyn til de spesielle forholdene der opplysninger samles inn, for å sikre en rettferdig behandling med hensyn til dataemnet.

Når opplysningene ikke er mottatt fra et dataemne, gjelder ikke forpliktelsen til å informere dataemnet dersom tilgjengeligheten av slik informasjon ikke er mulig eller vil innebære en uforholdsmessig innsats, eller om registrering eller opplysning er uttrykkelig fastsatt ved lov.

8 – Rett til tilgang, rettelse, sletting og blokkering av opplysninger

Hvert dataemne har rett til å motta, uten begrensning med rimelig mellomrom, en kommunikasjon av opplysningene som behandles i en forståelig form, samt av all tilgjengelig informasjon om opplysningenes kilde. Oppfølgingen av denne forespørselen, inkludert muligheten til å kreve gebyr eller tidsramme for å svare på en slik forespørsel, vil være underlagt gjeldende lover og formidles hensiktsmessig til dataemnet når vedkommende sender inn sin forespørsel.

Hvert dataemne har rett til å få opplysningene korrigert, slettet eller blokkert, særlig når opplysningene er ufullstendige eller unøyaktige.

Hvert dataemne har rett til å nekte når som helst på grunnlag av overbevisende legitime grunner knyttet til sin spesielle situasjon, behandling av sine personopplysninger, med mindre behandlingen kreves av loven eller forskrifter. Hvor innvendingen er berettiget, må behandlingen avbrytes.

Hvert dataemne har rett til å nekte (gratis) behandling av personopplysninger knyttet til ham eller henne ment for for direkte markedsføring.

Hvert dataemne har rett til å innhente kopi av varslingen sendt til tredjeparter som har mottatt opplysninger om eventuelle rettelser, sletting eller blokkering i henhold til artikkel 12 (c) i direktiv 95/46.

Hvert dataemne har rett til å kjenne grunnene som er involvert i automatisk behandling av opplysningene, i henhold til artikkel 12 (a) i direktiv 95/46.

9 - Automatiserte individuelle beslutninger

Automatiserte prosedyrer brukes kun som et verktøy i beslutningsprosessen. Ingen evaluering eller avgjørelse om et dataemne som påvirker ham eller henne betydelig, er utelukkende basert på automatisk behandling av hans eller hennes opplysninger med mindre avgjørelsen:

- Er tatt i forbindelse med inngåelse eller gjennomføring av en kontrakt, forutsatt at anmodningen om inngåelse eller gjennomføring av kontrakten, innlevert av dataemnet, er oppfylt eller at det er tatt hensiktsmessige tiltak for å beskytte vedkommendes legitime interesser, slik som ordninger som gjør at vedkommende kan tilføye sitt synspunkt, eller
- Er godkjent av en lov som også krever tiltak for å beskytte dataemnets legitime interesser.

10 - Sikkerhet og konfidensialitet

Amgen implementerer hensiktsmessige tekniske og organisatoriske sikkerhetsforanstaltninger, for å beskytte mot, og å finne utilsiktet eller ulovlig destruksjon, tap, endring, uautorisert avsløring eller tilgang til personopplysninger, spesielt hvor prosessen innebærer overføring av opplysninger over et offentlig nettverk, og mot alle andre potensielle former for ulovlig behandling. Amgen bruker et internasjonalt rammeverk som ISO/IEC 27002 til å bestemme disse sikkerhetsforanstaltningene.

Amgen har prosesser på plass for å sikre at potensielle personvernhendelser blir rapportert, sporet og at det tas passende korrigerende tiltak, etter behov.

Risikoanalyser for informasjonssikkerhet brukes til å identifisere potensielle trusler mot sensitiv

personsopplysninger og implementering av ekstra sikkerhetstiltak etter behov.

Gjennomføringen av tiltakene vil bli gjort med hensyn til den nyeste teknologien, i henhold til artikkel 17.1 i direktiv 95/46.

Informasjonssikkerhetsleder (Chief Information Security Officer) arbeider sammen med personvernsansvarlig (Chief Privacy Officer) for å forsikre sikkerheten og konfidensialiteten til personopplysning.

11 - Forhold til databehandlere (Amgens dataimportør eller leverandør)

Kontrolløren vil nøye velge en databehandler som kan være enten et Amgen-selskap eller en tjenesteleverandør. Behandleren må gi tilstrekkelige garantier for sine tekniske sikkerhetstiltak og organisatoriske tiltak som styrer behandlingen som skal gjennomføres, og må sikre at disse tiltakene overholdes.

Når outsourcing anses nødvendig etter vurdering av forretningsbehov og risiko forbundet med slik outsourcing, vil prosessen med å velge leverandør omfatte en vurdering av personvernrisikofaktorer og balansere forretningsbehov mot potensielle farer.

Ved bruk av skriftlige kontraktsmessige midler vil kontrollør i henhold til gjeldende lov instruere leverandøren om at blant annet:

i) Behandleren skal bare handle på instruksjoner fra kontrolløren, og at behandling av opplysninger for behandlerens egne formål eller med hensyn til en tredjepart er forbudt, og

ii) reglene knyttet til sikkerheten og konfidensialiteten til behandleren.

Kontrolløren skal sørge for at behandleren alltid overholder og møter avtalt tekniske og organisatoriske sikkerhetsforanstaltninger.

Kontrolløren beholder ansvaret for legitimiteten av behandlingen og er fortsatt ansvarlig for dataemnets rettigheter.

For å levere slike kontraktsforpliktelser er det gitt en kontraktsmal med navnet Data Privacy Schedule. Når det gjelder situasjonen for en bestemt kontrakt, kan datakontrolløren forhandle om en annen bestemmelse, men den skal fortsatt dekke forpliktelsene som er nevnt ovenfor.

12 - Begrensninger av overføringer og videreoverføringer

Leverandører som fungerer som databehandlere er bundet av skriftlige avtaler som fastsetter at leverandøren kun skal handle på instruks fra kontrolløren og skal være ansvarlig for gjennomføringen av tilstrekkelige sikkerhets- og konfidensialitetsforanstaltninger.

All overføring av opplysninger til leverandører utenfor EU skal overholde de europeiske reglene for datastrømmer over landegrenser, enten ved å benytte EUs standard kontraktsklausuler godkjent av EU-kommisjonen, eller andre tilstrekkelige kontraktsmessige midler i henhold til artikkel 25 og 26 i EU-direktivet.

All overføring av opplysninger til leverandører som fungerer som databehandlere utenfor EU, skal overholde EU-direktivets regler knyttet til behandlerne i tillegg til reglene for datastrømmer over landegrenser.

13 - Opplæringsprogram

Amgen sørger for passende opplæring av alle medarbeiderne om personvernprinsipper og BCR-reglene. Denne opplæringen inneholder også opplysninger om konsekvensene ifølge både straffe- og ansettelsesrett, for ansatte som bryter med BCR-reglene.

Opplæringen er obligatorisk og gjentas årlig. Deltakelse i opplæring må dokumenteres.

Spesifikke opplæringer vil i hvert enkelt tilfelle gis til ansatte som har permanent eller vanlig tilgang til personopplysninger, eller som er involvert i innsamling av personopplysninger eller i utviklingen av verktøy som brukes til å behandle personopplysninger.

I tillegg gir Amgens personvernkontor relevant informasjon og ressurser knyttet til personvern på Amgens intranettportal, samt via andre metoder.

14 - Revisjons- og overvåkingsprogram

Idet Amgen initierer Binding Corporate Rules (BCR-reglene), vil revisjonskontroll av personvernet opprettholdes og Amgens complianceprogram vil bli oppdatert for å innlemme BCR-reglene. I tillegg vil Amgen fortsette regelmessig personvernovervåkning som utføres lokalt av personvernsansvarlige (Data Protection Officer) i deres egenskap av sin rolle som complianceansvarlig (Compliance Lead).

Revisjonsprogrammet dekker alle aspekter av BCR-reglene, inkludert metoder for å sikre at korrigerende tiltak av rutiner finner sted.

Slike revisjoner utføres regelmessig av det interne krediterte revisjonslaget.

Revisjonsprogrammet er utviklet og avtalt i samarbeid av Chief Audit Executive og Chief Compliance Officer.

Chief Privacy Officer, Chief Compliance Officer og Chief Information Officer kan når som helst iverksette ad hoc-revisjoner basert på BCR-reglene.

Alle BCR-revisjonsrapporter kommuniseres til Chief Compliance Officer og til Chief Privacy Officer på en betimelig måte. BCR-reglenes revisjonsoppsummeringer og funn, samt annen relevant informasjon, rapporteres regelmessig til styret via egnede komiteer (for eksempel selskapsansvars- og compliancekomité og/eller revisjonsutvalg).

Datatilsynet kan motta en kopi av BCR-relaterte revisjonsrapporter på forespørsel.

Alle søsterselskapene forstår at de kan revideres av datatilsynet, og de vil overholde pålegg fra datatilsynet om et hvilket som helst problem relatert til BCR-reglene. Hver reviderte enhet må informere Chief Privacy Officer umiddelbart etter varsel om revisjon.

15 - Overholdelse og overvåking av compliance

Amgen utpeker passende medarbeiderne, inkludert et nettverk av personvernsansvarlige, med støtte fra toppledelsen for å overvåke og sikre overholdelse av reglene.

Hos Amgen omfatter den personvernsansvarlige sine oppgaver blant annet:

- rådgivning til styret,
- sikre overholdelse av personvern på globalt nivå
- rapportere regelmessig om personvernsoverholdelse (compliance), og
- jobber med datatilsynets etterforskninger

Chief Privacy Officer har ansvaret for Global Privacy Office som er et team som tilbyr ekspertstøtte over hele verden til Amgen-enheter.

På lokalt nivå er personvernsledere (Data Protection Officer) ansvarlige for håndtering av lokale personvernforespørsler fra dataemner, for å sikre compliance på lokalt nivå med støtte fra personvernskontoret og for å rapportere viktige personvernsproblemer til personvernsansvarlig (Chief Privacy Officer). Amgen opprettholder et nettverk av datavernsledere og sikrer at en DPO er utnevnt eller tildelt for hvert land der Amgen (deltakende selskap) har en bedriftsenhet. Denne betegnelsen er laget i samråd med den lokale lederen av DPO og den lokale personalavdelingen.

Vanligvis er personvernsledere (Data Protection Officer) lokale helsepersonell somarbeider som complianceansvarlig og som rapporterer til Worldwide Compliance and Business Ethics-avdeling. Personvernkontoret rapporterer også til avdelingen Global Compliance and Business Ethics. Sjelden, på grunn av spesifikkheten til en Amgen-enhet eller spesielle omstendigheter, kan Data Protection Officeren komme fra en annen funksjon, for eksempel Regulatory. Personvernskontoret sikrer under alle omstendigheter at personvernsleder er hensiktsmessig opplært og har tilstrekkelig grad av lederskap og kompetanse for å oppfylle sin rolle som personvernsleder. I tillegg har personvernslederen (Data Protection Officer) en direkte linje til Chief Privacy Officer samt personvernskontorpersonale, dersom det er behov for ytterligere veiledning.

16 - Tiltak der nasjonal lovgivning forhindrer overholdelse av BCR-reglene

Dersom et medlem av konsernet har grunn til å tro at lovgivningen som gjelder for ham eller henne, forhindrer selskapet i å oppfylle sine forpliktelser under BCR-reglene, og har en vesentlig innvirkning på garantiene som reglene gir, vil han/hun straks informere Chief Privacy Offiser (unntatt der det er forbudt av en rettshåndhevende myndighet, for eksempel et forbud i straffelov for å bevare konfidensialiteten til en etterforskning av rettshåndhevende myndighet).

Når det er konflikt mellom nasjonal lovgivning og forpliktelsene i BCR-reglene, vil Chief Privacy Officer i samråd med lokal juridisk rådgiver og lokalt datatilsyn avgjøre hvilken juridisk hensiktsmessig handling som kreves. Om nødvendig, vil personvernsansvarlig (Chief Privacy Officer) også rådføre seg med det relevante datatilsynet.

17 - Interne klagemekanismer

Amgen vil utvide og utnytte sin eksisterende klagehåndteringsprosess for å inkludere håndtering av eventuelle BCR-relaterte klager eller bekymringer.

Ethvert dataemne kan til enhver tid sende inn en klage over at et deltakende selskap ikke overholder BCR-

reglene. Slike klager vil bli håndtert av personvernskontoret under ledelse av personvernsansvarlig (Chief Privacy Officer) og i samarbeid med den relevante lokale personvernslederen (Data Protection Officer).

Amgen anbefaler at slike klager leveres skriftlig enten via post eller e-post direkte til personvernskontoret eller til daterselskapet. Dataemner kan også, når dette er akseptabelt i henhold til gjeldende lover, bruke Business Conduct Hotline til å rapportere en BCR-klage.

Hvis klagen mottas lokalt, vil DPO oversette om nødvendig, og videresender den uten forsimkelse til personvernskontoret.

Et første svar vil bli gitt til dataemnet som informerer vedkommende om at klagen er under vurdering, og at han eller hun vil få svar innen maksimalt to måneder.

Dersom personvernskontoret oppdager feil utført av et bestemt individ, vil det bli truffet hensiktsmessige disiplinære tiltak, inntil og med øyeblikkelig oppsigelse av ansettelse, i den utstrekning det er tillatt etter gjeldende lov.

Innen maksimalt to måneder skal dataemnet motta et svar som informerer ham eller henne om resultatet av klagen.

Dataemnet vil bli informert om at dersom han eller hun ikke er fornøyd med Amgens svar, kan han eller hun innkreve et krav fra den relevante domstolen eller datatilsynet.

Denne klagehåndteringsprosessen vil bli offentliggjort ved offentliggjøring av BCR-reglene som nevnt i § 7.

18 - Rettigheter og ansvar til tredjepartsmottaker

Der dataemnets personopplysninger stammer fra et regulert land og hevder brudd på eventuelle forpliktelser som er referert til i BCR-reglene, har det rett til å håndheve reglene som tredjepartsmottaker. Disse rettighetene dekker rettsmidler for brudd på de garanterte rettighetene og retten til å motta kompensasjon. Hvis det er aktuelt, er ansvaret begrenset til den faktiske skaden.

I den utstrekning det er tillatt av gjeldende jurisdiksjon, kan dataemner velge å innlevere krav til:

- Dataeksportørens jurisdiksjon, og hvis dataemnets personopplysninger stammer fra en EØS-dataeksportør, skal den kompetente jurisdiksjonen være stedet der EØS-dataeksportøren er registrert, eller
- Det gjeldende datatilsynet.

Ethvert dataemne som har vært utsatt for et brudd utført av dataeksportøren eller dataimportøren på de forpliktelsene som er nevnt i BCR-reglene, har rett til å motta kompensasjon fra dataeksportøren for skaden. Hvis dataeksportøren eller dataimportøren er ansvarlig for brudd, vil det i den utstrekning det er ansvarlig, holde den andre parten fri for eventuelle kostnader, økonomiske belastninger, skader, utgifter eller tap det har pådratt seg.

Både dataeksportør og dataimportør kan være unntatt fra ansvar i henhold til BCR-reglene, hvis det viser seg at medlemmet i gruppen utenfor EU ikke har krenket BCR-reglene eller ikke er ansvarlig for skadene dataemnet er utsatt for. Imidlertid forblir bevisbyrden hos dataeksportøren og dataimportøren.

Dataimportøren som fungerer som databehandler, kan ikke påberope at en underbehandler har overtrådt

sine forpliktelser, for å unngå egne forpliktelser. Hvis et dataemne ønsker å fremsette en fordring mot dataeksportøren, men ikke kan oppnå dette som følge av brudd på BCR-reglene, fordi dataeksportøren faktisk har forsvunnet eller opphørt å eksistere etter loven, eller ble insolvent, kan dataemnet håndheve sine fordringer mot dataimportøren direkte. Hvis en etterfølgende forretningsenhet har overtatt alle juridiske forpliktelser fra dataeksportøren eller dataimportøren ved kontrakt eller etter loven, kan dataemnet håndheve sine rettigheter mot en slik enhet. Dataimportørens ansvar skal begrenses til egne behandlingsoperasjoner etter BCR-reglene.

19 - Fellesskap og samarbeid med datatilsyn

Deltakende selskaper er pålagt å samarbeide og bistå hverandre med å håndtere en forespørsel eller klage fra et dataemne eller en undersøkelse eller forespørsel fra datatilsynet.

Deltakende selskaper vil i samarbeid med Chief Privacy Officer svare på BCR-relaterte henvendelser fra datatilsynet innen en passende tidsramme og på passende måte og følge råd og beslutninger fra den kompetente datatilsynet med hensyn til gjennomføring av BCR-reglene.

20 - BCRs oppdatering og endringer

Amgen forbeholder seg retten til å endre og/eller oppdatere disse BCR-reglene når som helst. En slik oppdatering av BCR-reglene kan være nødvendig spesielt som et resultat av endrede lovkrav, betydelige endringer i Amgen-gruppens struktur eller offisielle krav pålagt av datatilsynene.

Amgen vil rapportere eventuelle vesentlige endringer i BCR-reglene eller listen over deltakende selskaper til alle andre deltakende bedrifter og til datatilsynene som tar hensyn til endringer i regelverket og selskapsstrukturen.

Noen endringer kan kreve en ny autorisasjon fra datatilsynene.

Chief Privacy Officer vil opprettholde en fullstendig oppdatert liste over selskapene som deltar i BCR-reglene, de regulerte landene som kan være beskyttet under BCR-reglene, og følge opp eventuelle oppdateringer av reglene, samt gi nødvendig informasjonen til dataemnene eller datatilsynene på forespørsel.

Amgen forplikter seg til at ingen nye overføringer sendes til deltakende selskaper med garantiene til BCR-reglene før det nye deltakende selskapet er effektivt bundet av BCR-reglene og overholder BCR-reglene.

Eventuelle endringer i BCR-reglene eller listen over deltakende selskaper vil bli rapportert en gang i året til datatilsynet som usteder godkjennelsene sammen med en kort forklaring om årsakene til oppdateringen.

Vesentlige endringer av reglene vil også bli formidlet til dataemnene i henhold til artikkel 7 i BCR-reglene.

21 - Forholdet mellom nasjonale lover og BCR-reglene

Når lokale lover krever et høyere beskyttelsesnivå av personlig informasjon, vil de ha prioritet over BCR-reglene. Hvis gjeldende lokal lov gir et lavere beskyttelsesnivå av personopplysninger enn BCR-reglene, vil BCR-reglene bli brukt.

Ved eventuelle forpliktelser som følge av at gjeldende lokal lovgivning er i konflikt med BCR-reglene, skal

det deltakende selskapet informere personvernsansvarlig (Chief Privacy Officer) uten unødig forsinkelse.

Personopplysninger skal under alle omstendigheter behandles i samsvar med gjeldende lovgivning, som fastsatt i artikkel 4 i direktiv 95/46/EF og relevant lokal lovgivning.