



## **Amgenin konsernin sisäiset sitovat tietosuojasäännöt (Binding Corporate Rules, BCR) – julkinen asiakirja**

### **Johdanto:**

Amgen on johtava bioteknologiayritys, joka on sitoutunut palvelemaan vakavasti sairaita potilaita.

Konsernin sisäisissä sitovissa tietosuojasäännöissä (Binding Corporate Rules, BCR) ilmaistaan Amgenin sitoumus yksityisyyden suojaan ja tietosuojaan sen pyrkiessä suojelemaan riittävästi henkilötietojen siirtoa ja käsittelyä Amgenin yksiköiden välillä.

Kaikki Amgeniin kuuluvat oikeushenkilöt ja kaikki henkilöstön jäsenet ovat sitoutuneet noudattamaan sitovia tietosuojasääntöjä. Niiden noudattamatta jättäminen voi johtaa paikallisten lakien sallimiin kurinpidollisiin toimenpiteisiin.

Säännönmukaisuudesta vastaava johtaja (Chief Compliance Officer) varmistaa yhteistyössä yksityisyyden suojasta vastaavan johtajan (Chief Privacy Officer) kanssa, että esitetyt säännöt pannaan täytäntöön.

Sitovat tietosuojasäännöt on hyväksytty viitaten nykyisiin sovellettavissa oleviin Euroopan unionin tietosuojadirektiiveihin 95/46/EY ja 2002/58/EY.

### **1 – Laajuus**

Amgenin sitovat tietosuojasäännöt koskevat työntekijöiden, asiakkaiden, tavarantoimittajien, osakkeenomistajien, potilaiden ja kaikkien muiden rekisteröityjen henkilöiden kaikenlaisten henkilötietojen automaattista tai manuaalista siirtoa ja käsittelyä, joka tapahtuu Amgenissa mukana olevan yrityksen toimiessa rekisterinpitäjänä seuraavissa tapauksissa:

- a) Amgenissa mukana oleva henkilötietoja käsittelevä yritys sijaitsee säännellyssä maassa
- b) Amgenissa mukana oleva henkilötietoja käsittelevä yritys ei sijaitse säännellyssä maassa ("tietojen tuoja") ja on saanut henkilötiedot säännellyssä maassa sijaitsevalta Amgenissa mukana olevalta yritykseltä kohdan 2 määritelmän mukaan ("tietojen viejä").

Nämä sitovat tietosuojasäännöt koskevat myös henkilötietojen siirtoa eteenpäin tietojen tuojilta toisille tietojen tuojille.

## 2 – Määritelmät

Termit	Määritelmät
Henkilötiedot	<p>Henkilöä koskevat tiedot, joista käy selvästi ilmi tai joista voidaan todeta henkilöllisyys joko suoraan tai epäsuorasti. Vaihtoehtoisesti henkilötietoja voidaan ajatella tietoina, joita voidaan joko yksinään tai yhdessä muiden tietojen kanssa käyttää tunnistamaan yksittäinen henkilö, ottamaan häneen yhteyttä tai paikallistamaan hänet. Esimerkkejä henkilötiedoista voivat olla seuraavat, riippuen paikallisista yksityisyyden suojaa ja tietosuojaa koskevista laeista:</p> <ul style="list-style-type: none"> <li>• henkilön nimi, osoite, henkilötunnus, ajokortin numero, tilitiedot, perhe- tai potilastiedot</li> <li>• lääkärin nimi, koulutustiedot ja lääkemääräyskäytännöt</li> <li>• Amgen-sivustolla vierailevan henkilön antama sähköpostiosoite ja muut henkilötiedot.</li> </ul> <p>Nämä ovat vain esimerkkejä, eikä kyseessä ole täydellinen luettelo.</p>
Arkaluonteiset henkilötiedot	<p>Seuraavat rekisteröityä henkilöä koskevat tiedot:</p> <ul style="list-style-type: none"> <li>• terveydentilaan (fyysiseen tai psyykkiseen) liittyvät tiedot</li> <li>• taloudelliset tiedot</li> <li>• rotu tai etninen alkuperä</li> <li>• poliittiset mielipiteet</li> <li>• uskonnollinen tai filosofinen vakaumus</li> <li>• ammattiliiton jäsenyys</li> <li>• sukupuolinen suuntautuminen</li> <li>• rikostuomiot tai pidätykset.</li> </ul> <p>Amgen pitää arkaluonteisena tietona tietoja, joita voitaisiin käyttää identiteettivarkaudessa, esim. henkilötunnusta, ajokortin numeroa, luottokortti- ja pankkitilitietoja.</p>
Rekisteröity henkilö	<p>Henkilö, johon henkilötiedot liittyvät. Rekisteröity henkilö voi olla esimerkiksi</p> <ul style="list-style-type: none"> <li>• potilas/kuluttaja/tutkimushenkilö</li> <li>• terveydenhuollon ammattilainen (esim. lääkäri tai terveydenhoitaja)</li> <li>• työntekijä (nykyinen, entinen tai eläkkeellä oleva)</li> <li>• urakoitsija/yksityisrittäjä/hankkija/konsultti.</li> </ul>
Rekisterinpitäjä (tietojen hallinnoija)	<p>Taho, joka tekee henkilötietojen keräämistä ja käsittelyä koskevat päätökset, mukaan lukien päätökset siitä, mihin tarkoituksiin ja millä tavalla henkilötietoja käsitellään.</p>
Tiedonkäsittelijä	<p>Henkilö tai yritys, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.</p>

Käsittely	Kaikki niin manuaaliset kuin automaattisetkin tietojenkäsittelytoimet, joissa käsitellään henkilötietoja. Näihin lukeutuvat mm. tietojen kerääminen ja katselu, tietoihin pääsy, tietojen varastointi, tallennus, järjestäminen, muokkaaminen tai muuttaminen, haku, hyödyntäminen, käyttö, paljastaminen siirtämällä, välittämällä edelleen tai asettamalla muutoin saataville, ryhmittely tai yhdistäminen, suojaaminen, poistaminen tai tuhoaminen.
Kolmas osapuoli	Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai mikä tahansa muu taho kuin rekisteröity henkilö itse, rekisterinpitäjä tai henkilöt, jotka rekisterinpitäjä on suoraan valtuuttanut käsittelemään tietoja. Amgenilla hankkijoita pidetään kolmansina osapuolina.
Hankkija	Henkilö, yritys tai organisaatio, joka tarjoaa tavaroita tai palveluja Amgenille, on sopimussuhteessa sen kanssa ja/tai on saanut Amgenilta henkilötietoja, jotka vaaditaan kyseisten tavaroiden tai palvelujen toimittamiseksi.
Tietosuojaviranomaiset	Yksi tai useampi julkinen viranomainen, joka on vastuussa jäsenvaltioiden hyväksymien säännösten soveltamisen valvonnasta omalla alueellaan direktiivin 95/46 mukaisesti.  Nämä viranomaiset hoitavat vastuullaan olevat tehtävät täysin itsenäisesti.
Säännelty maa	Euroopan talousalueella (ETA) oleva maa tai maa, jonka tietosuojan Euroopan komissio on todennut asianmukaiseksi, tai muut maat, jotka noudattavat sitovia tietosuojasääntöjä siirtäessään henkilötietoja lainkäyttövaltansa ulkopuolella oleville alueille. Tällaisia maita ovat Andorra, Argentiina, Kanada, Färösaaret, Guernsey, Mansaari, Israel, Jersey, Uusi-Seelanti, Sveitsi ja Uruguay.
Tietojen viejä	Säännellyssä maassa sijaitseva Amgenin yksikkö, joka toimii rekisterinpitäjänä ja siirtää henkilötietoja sellaiseen Amgenin yksikköön, joka ei sijaitse säännellyssä maassa (tietojen tuoja).
Tietojen tuoja	Amgenin yksikkö, joka ei sijaitse säännellyssä maassa ja joka vastaanottaa henkilötietoja tietojen viejältä.
Tekniset ja organisatoriset turvatoimet	Toimenpiteet, joiden tavoitteena on suojata henkilötietoja tahattomalta tai laittomalta tuhoamiselta, tahattomalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai niihin pääsylvä erityisesti silloin, kun tiedonkäsittelyyn liittyy tietojen siirtäminen verkossa, sekä muulta laittomalta käsittelyltä.
Mukana oleva yritys	Amgen-konserniin kuuluva oikeushenkilö, joka on velvollinen noudattamaan sitovia tietosuojasääntöjä.
Suostumus	Vapaaehtoisesti annettu täsmällinen ja tietoinen ilmaus rekisteröidyn henkilön toiveista, joiden mukaisesti rekisteröity henkilö ilmaisee suostumuksensa itseään koskevien henkilötietojen keräämiseen ja käsittelyyn.
Tietosuojavastaava (Data Protection Officer)	Yhtiön työntekijä, jonka tytäryhtiön tai liiketoimintayksikön johto on nimennyt vastuuseen yksityisyyden suojan ja tietosuojan valvonnasta paikallistasolla sekä asianmukaisten ja vaadittavien valvontatoimenpiteiden toteuttamisesta.

Amgen tulkitsee sitovissa tietosuojasäännöissä olevat termit Euroopan unionin direktiivien 95/46/EY ja 2002/58/EY mukaisesti. Jäljempänä näitä kutsutaan EU-direktiiveiksi.

### 3 – Käyttötarkoituksen rajaaminen

Henkilötietoja tulee käsitellä tiettyä nimenomaista ja laillista tarkoitusta varten direktiivin 95/46 artiklan 6.1(b) mukaisesti.

Henkilötietoja ei käsitellä niiden laillisten tarkoitusten kanssa yhteensopimattomalla tavalla, joita varten henkilötiedot kerättiin. Tietojen tuojat ovat velvollisia pitämään kiinni alkuperäisistä tarkoituksista tallentaessaan tai käsitellessään tietoja tai käyttäessään jonkun muun mukana olevan yrityksen niille siirtämiä tietoja. Tiedonkäsittelyn tarkoitusta voidaan muuttaa vain rekisteröidyn suostumuksella tai tietoja siirtävää tietojen viejää koskevien paikallisten lakien sallimissa rajoissa.

Arkaluonteisia tietoja suojataan EU-direktiivissä 95/46/EY mainituin erityissuojatoimenpitein.

### 4 – Tietojen laatu ja suhteellisuus

Henkilötietojen on oltava paikkansapitäviä, ja ne on tarvittaessa pidettävä ajan tasalla. On varmistettava asianmukaisin toimenpitein, että virheelliset tai puutteelliset tiedot korjataan tai poistetaan.

Henkilötietojen on oltava riittäviä ja olennaisia direktiivin 95/46 artiklan 6.1(c) mukaisesti.

Tiedonkäsittelyn ohjenuorana on rajata henkilötietojen kerääminen, käsittely ja/tai käyttö vain välttämättömään eli henkilötietojen mahdollisimman vähäiseen määrään. Mahdollisuus nimettömänä tai nimimerkillä annettuihin tietoihin täytyy hyödyntää, mikäli siihen liittyvät kustannukset ja vaivannäkö ovat oikeassa suhteessa haluttuun tarkoitukseen.

Ne henkilötiedot, joita ei enää tarvita siihen liiketoimintatarkoitukseen, jota varten ne on alun perin kerätty ja tallennettu, on poistettava Amgenin tietojen säilyttämistä koskevan aikataulun mukaisesti (Amgen Record Retention Schedule). Lakisäateisten säilytysaikojen tai säilyttämismääräyksen niin vaatiessa tietojen hävittämisen sijasta estetään niihin pääsy. Lakisäateisen säilytysajan tai säilyttämismääräyksen päättyessä tiedot hävitetään.

### 5 – Henkilötietojen käsittelyn laillinen perusta

Henkilötietojen käsittely on sallittua vain, jos vähintään yksi seuraavista edellytyksistä täyttyy:

- rekisteröity on vapaaehtoisesti ja yksiselitteisesti antanut tietoisensa suostumuksensa
- käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on joko osapuolena tai siihen vastaavassa suhteessa, tai sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn henkilön pyynnöstä
- käsittely on tarpeen rekisterinpitäjän lakiin perustuvan veloitteen täyttämiseksi tai jos soveltuvat lait tai säännökset sitä vaativat tai sen sallivat
- käsittely on tarpeen rekisteröidylle henkilölle elintärkeästä syystä kuten hänen henkensä, terveytensä tai turvallisuutensa turvaamiseksi
- käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai sellaisen julkisen vallan käyttämiseksi, joka kuuluu rekisterinpitäjälle tai kolmannelle osapuolelle, jolle tiedot luovutetaan
- käsittely on tarpeen rekisterinpitäjän tai tiedot saavan kolmannen osapuolen oikeutetun intressin toteuttamiseksi, paitsi silloin, kun rekisteröidyn perusoikeuksiin ja -vapauksiin perustuvat oikeutetut intressit syrjäyttävät tämän intressin.

## 6 – Arkaluonteisten tietojen käsittely

Mikäli Amgenin täytyy käsitellä arkaluonteisia tietoja jostain erityisestä, oikeutetusta syystä, Amgen käsittelee niitä vain, jos

- rekisteröity henkilö on antanut nimenomaisen suostumuksensa kyseisten arkaluonteisten tietojen käsittelyyn, elleivät soveltuvat lait kiellä käsittelyä
- käsittely on tarpeen rekisterinpitäjän erityisten oikeuksien ja velvoitteiden noudattamiseksi työoikeuden alalla, siltä osin kuin se sallitaan kansallisessa lainsäädännössä, jolla säädetään riittävästä suojatoimista
- käsittely on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi, jos rekisteröity henkilö on fyysisesti tai juridisesti estynyt antamasta suostumustaan
- käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä ja asianmukaisin suojatoimin sillä edellytyksellä, että käsittely koskee ainoastaan näiden yhteisöjen jäseniä tai henkilöitä, joilla on yhteisöihin säännölliset, yhteisöjen tarkoituksiin liittyvät yhteydet, eikä tietoja luovuteta kolmannelle osapuolelle ilman rekisteröityjen henkilöiden suostumusta
- käsittely koskee arkaluonteisia tietoja, jotka rekisteröity henkilö on nimenomaisesti saattanut julkisiksi
- arkaluonteisten tietojen käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- arkaluonteisten tietojen käsittely on tarpeen ennalta ehkäisevää lääketiedettä tai lääketieteellisiä diagnooseja koskevia tarkoituksia, hoitoa tai terveydenhuollon palvelujen hallintoa varten ja jos näitä arkaluonteisia tietoja käsittelee terveydenhuollon ammattikoulutuksen saanut henkilö, jota kansallinen lainsäädäntö tai toimivaltaisten kansallisten viranomaisten asettama ammatillinen salassapitovelvollisuus koskee, tai jos tietoja käsittelee muu henkilö, jolla on vastaava salassapitovelvoite.

## 7 – Läpinäkyvyys ja oikeus informointiin

Kaikkien mukana olevien yritysten tulee käsitellä henkilötietoja läpinäkyvällä tavalla. Amgen on sitoutunut huolehtimaan siitä, että sitovat tietosuojasäännöt, mukaan lukien yhteystiedot, ovat kaikkien rekisteröityjen henkilöiden käytettävissä, ja tiedottamaan rekisteröidyille henkilöille heidän henkilötietojensa siirrosta ja käsittelystä.

Tätä varten Amgen käyttää erilaisia viestintätapoja, kuten yrityksen verkkosivuja (mukaan lukien sisäiset sivustot ja uutiskirjeet), sopimuksia ja tiettyjä asianmukaisiin tukimateriaaleihin liitettyjä tietosuojailmoituksia.

Rekisteröidyille henkilöille, joiden henkilötietoja käsittelee mukana oleva yritys, tulee antaa seuraavat tiedot:

- rekisterinpitäjän (ja tämän edustajan) henkilöllisyys
- mitä tarkoitusta varten tietoja käsitellään
- tietojen alkuperä (elleivät kyseessä ole suoraan rekisteröidyltä henkilöltä kerätyt henkilötiedot)
- kaikenlaiset lisätiedot, kuten
  - i) tietojen vastaanottajat tai vastaanottajaryhmät
  - ii) tieto, onko rekisteröidyllä henkilöllä rekisteröidyn henkilön kannalta asianmukaisen tietojenkäsittelyn takaamiseksi oikeus saada itseään koskevat tiedot ja oikeus niiden oikaisuun siltä osin, kuin nämä lisätiedot ovat tarpeen, ottaen huomioon erityiset olosuhteet, joissa tiedot kerätään.

Mikäli tietoja ei saada rekisteröidyltä, velvoitetta rekisteröidyn henkilön informoimisesta ei sovelleta, jos

tietojen toimittaminen rekisteröidylle henkilölle osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa tai jos lainsäädännössä nimenomaisesti säädetään tietojen tallentamisesta tai luovuttamisesta.

#### 8 – Oikeus tietojen oikaisuun tai poistamiseen ja oikeus päästä tietoihin käsiksi tai estää pääsy niihin

Jokaisella rekisteröidyllä henkilöllä on oikeus saada kohtuullisin väliajoin ja ilman rajoitteita ymmärrettävässä muodossa oleva tiedote käsiteltävänä olevista tiedoista sekä kaikki saatavilla olevat tiedot niiden alkuperästä. Soveltuvissa laeissa määrätään tätä pyyntöä seuraavista toimista, mukaan lukien mahdollisuudesta periä maksu ja aikarajasta, jolloin pyyntöön on vastattava. Näistä tiedotetaan rekisteröidylle henkilölle asianmukaisesti pyynnön yhteydessä.

Jokaisella rekisteröidyllä henkilöllä on oikeus saada tiedot oikaistua tai poistettua tai estettyä niihin pääsy erityisesti siinä tapauksessa, että tiedot ovat puutteellisia tai virheellisiä.

Jokaisella rekisteröidyllä henkilöllä on oikeus vastustaa henkilötietojensa käsittelyä milloin tahansa erityistilanteeseensa liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi, paitsi milloin lait tai säännökset edellyttävät käsittelyä. Mikäli käsittelyn vastustaminen on oikeutettua, käsittely on lopetettava.

Jokaisella rekisteröidyllä henkilöllä on oikeus vastustaa (korvauksetta) henkilötietojensa käsittelyä suoramarkkinointitarkoituksissa.

Direktiivin 95/46 artiklan 12(c) mukaisesti jokaisella rekisteröidyllä on oikeus siihen, että tehdyistä oikaisuista, poistamisista tai suojaamisista ilmoitetaan kolmansille osapuolille, joille tietoja on luovutettu.

Direktiivin 95/46 artiklan 12(a) mukaisesti jokaisella rekisteröidyllä henkilöllä on oikeus saada tietää tietojen automaattiseen käsittelyyn liittyvästä logiikasta.

#### 9 – Automatisoidut yksittäispäätökset

Automatisoituja menetelmiä käytetään vain päätöksentekoprosessin työkaluna. Sellaisia rekisteröityä henkilöä koskevia arviointeja tai päätöksiä, jotka vaikuttavat häneen merkittävästi, ei tehdä ainoastaan automaattisen tietojenkäsittelyn perusteella, ellei

- tällaista päätöstä tehdä tietyn sopimuksen tekemisen tai täytäntöönpanon yhteydessä, sillä edellytyksellä, että rekisteröidyn henkilön tekemä sopimuksen tekemistä tai täytäntöönpanoa koskeva pyyntö on täytetty tai että asianmukaisilla toimenpiteillä, kuten antamalla hänelle mahdollisuus ilmaista kantansa, voidaan taata hänen oikeutetun etunsa suojaaminen
- tällainen päätös perustuu lakiin, jolla myös määritellään rekisteröidyn henkilön oikeutetun edun turvaavat toimenpiteet.

#### 10 – Turvallisuus ja luottamuksellisuus

Amgenilla on käytössä tarpeelliset tekniset ja organisatoriset turvatoimenpiteet henkilötietojen suojaamiseksi vahingossa tapahtuvalta tai laittomalta tuhoamiselta, häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta ja tietoihin pääsylvä (samoin kuin tällaisen toiminnan havaitsemiseksi) erityisesti, jos käsittely käsittää tietojen siirtämisen julkisessa verkossa, sekä kaikelta muulta laittomalta käsittelyltä. Amgen käyttää näiden turvatoimenpiteiden määrittelyyn kansainvälisiä standardeja, kuten ISO/IEC 27002.

Amgenilla on käytössä menetelmiä, joilla varmistetaan, että mahdollisista tietosuojan liittyvistä

vaaratilanteista ilmoitetaan, niitä seurataan ja niistä on tarvittaessa asianmukaiset seuraamukset.

Tiedon turvallisuuden riskiarvioiteja (Information Security Risk Assessment) käytetään mahdollisten arkaluonteisia henkilötietoja koskevien uhkien tunnistamiseen ja lisäturvatoimenpiteiden käyttöönottoon tarvittaessa.

Toimenpiteet otetaan käyttöön direktiivin 95/46 artiklan 17.1 mukaisesti ottaen huomioon kehityksen taso.

Tietoturvaohjaaja (Chief Information Security Officer) varmistaa yhteistyössä yksityisyyden suojasta vastaavan johtajan (Chief Privacy Officer) kanssa henkilötietojen turvallisuuden ja luottamuksellisuuden.

## 11 – Suhteet tiedonkäsittelijöihin (Amgenin tietojen tuoja tai hankkija)

Rekisterinpitäjä valitsee huolellisesti tiedonkäsittelijän, joka voi olla joko Amgenissa mukana oleva yritys tai hankkija. Käsittelijän on annettava riittävät takeet teknisistä turvatoimistaan ja organisatorisista menetelmistään koskien käsittelyä ja varmistettava niiden noudattaminen.

Mikäli ulkoistamisen aiheuttamien riskien ja liiketoimintatarpeiden määrittämisen jälkeen ulkoistaminen todetaan välttämättömäksi, hankkijan valinta käsittää yksityisyyden suojaa koskevien riskitekijöiden arvioinnin ja liiketoimintatarpeiden punnitsemisen mahdollisia riskejä vastaan.

Soveltuvien lakien mukaisesti rekisterinpitäjä ilmoittaa hankkijalle kirjallisen sopimuksen välityksellä, että

i) käsittelijän tulee toimia ainoastaan rekisterinpitäjän ohjeiden mukaisesti ja tiedonkäsittely käsittelijän omiin tai kolmannen osapuolen tarkoituksiin on kielletty

ii) käsittelijän velvollisuutena on noudattaa turvallisuutta ja luottamuksellisuutta koskevia sääntöjä.

Rekisterinpitäjän on varmistettava, että käsittelijä noudattaa sovittuja teknisiä ja organisatorisia turvatoimia.

Rekisterinpitäjä pysyy vastuullisena käsittelyn laillisuudesta ja on yhä vastuussa rekisteröidyn oikeuksista.

Sopimusvelvoitteiden ilmoittamista varten on käytössä tietosuojaa koskeva sopimusmalli nimeltä Data Privacy Schedule. Sopimustilanteesta riippuen rekisterinpitäjä voi neuvotella eri järjestelyistä, mutta niiden täytyy siitä huolimatta täyttää yllä mainitut velvoitteet.

## 12 – Siirtoja ja eteenpäinsiirtoja koskevat rajoitukset

Tiedonkäsittelijöinä toimivia hankkijoita sitovat kirjalliset sopimukset, joissa säädetään, että hankkijan tulee toimia ainoastaan rekisterinpitäjän ohjeiden mukaisesti ja että hankkija on vastuussa riittävien turvatoimenpiteiden ja luottamuksellisuuden säilyttävien toimenpiteiden toteutumisesta.

Kaikki EU:n ulkopuolella sijaitseville hankkijoille tehdyt tiedonsiirrot noudattavat eurooppalaisia sääntöjä rajojen yli tapahtuvasta tiedonsiirrosta joko käyttämällä Euroopan komission hyväksymiä EU:n mallisopimuslausekkeita tai muita riittäviä sopimusmuotoja EU-direktiivin artiklan 25 ja 26 mukaisesti.

Kaikki tiedonsiirrot tiedonkäsittelijöinä toimiville hankkijoille, jotka sijaitsevat EU:n ulkopuolella, noudattavat

käsittelijöitä koskevia EU-direktiivin sääntöjä sen lisäksi, että ne noudattavat rajojen yli tapahtuvaa tiedonsiirtoa koskevia sääntöjä.

### 13 – Koulutusohjelma

Amgen tarjoaa asianmukaista koulutusta tietosuojaperiaatteista ja sitovista tietosuojasäännöistä koko henkilöstölle. Tässä koulutuksessa kerrotaan myös sekä rikos- että työoikeudelliseen lakiin nojautuvista seurauksista työntekijöille, jotka rikkovat sitovia tietosuojasääntöjä.

Koulutus on pakollinen ja toistetaan vuosittain. Menestyksekkäs osallistuminen koulutukseen dokumentoidaan.

Eryityskoulutusta annetaan tapauskohtaisesti työntekijöille, joilla on pysyvä tai säännöllinen pääsy henkilötietoihin tai jotka ovat mukana henkilötietojen keräämisessä tai henkilötietoja käsittelevien työkalujen kehittämisessä.

Lisäksi Amgenin tietosuojaosasto (Privacy Office) tarjoaa tarkoituksenmukaisia tietosuojaan liittyviä tietoja ja resursseja mm. Amgenin intranet-portaalissa.

### 14 – Tarkastus- ja seurantaohjelma

Amgenin ottaessa sitovat tietosuojasäännöt käyttöön tietosuojatarkastukset jatkuvat ja Amgenin sääntöjennoudattamisohjelma päivitetään niin, että se käsittää myös sitovat tietosuojasäännöt. Lisäksi Amgen jatkaa säännöllistä tietosuojavalvontaa paikallisten tietosuojavastaavien eli säännönmukaisuudesta vastaavien henkilöiden toimesta.

Tarkastusohjelma kattaa kaikki sitovien tietosuojasääntöjen aspektit, mukaan lukien menetelmät, joilla varmistetaan, että korjaavat toimet otetaan käyttöön.

Sisäinen valtuutettu tarkastustiimi suorittaa tarkastukset säännöllisin väliajoin.

Tarkastuksista vastaava johtaja (Chief Audit Executive) yhdessä säännönmukaisuudesta vastaavan johtajan (Chief Compliance Officer) kanssa kehittää tarkastusohjelman ja sopii siitä.

Yksityisyyden suojasta vastaava johtaja (Chief Privacy Officer), säännönmukaisuudesta vastaava johtaja (Chief Compliance Officer) ja tietohallintojohtaja (Chief Information Officer) voivat suorittaa sitovia tietosuojasääntöjä koskevia tarkastuksia satunnaisesti milloin vain.

Kaikki sitovia tietosuojasääntöjä koskevat tarkastusraportit välitetään säännönmukaisuudesta vastaavalle johtajalle (Chief Compliance Officer) ja yksityisyyden suojasta vastaavalle johtajalle (Chief Privacy Officer) pikimmiten. Sitovia tietosuojasääntöjä koskevat tarkastusyhteenvedot ja tulokset samoin kuin muut tarpeelliset tiedot raportoidaan säännöllisesti hallitukselle asianmukaisten komiteoiden välityksellä (esim. yhtiön vastuullisuus- ja säännöstenmukaisuuskomitea [Corporate Responsibility and Compliance Committee] tai hallituksen auditointikomitea [Audit Committee of the Board]).

Tietosuojaviranomaiset voivat saada pyynnöstä kopion sitovia tietosuojasääntöjä koskevista tarkastusraporteista.

Kukin mukana oleva yritys ymmärtää, että tietosuojaviranomaiset voivat tarkastaa sen toiminnan, ja



hyväksyy tietosuojaviranomaisten ohjeet kaikissa sitovia tietosuojasääntöjä koskevissa tapauksissa. Kunkin tarkastettavan yksikön täytyy kertoa tarkastusta koskevasta ilmoituksesta yksityisyyden suojasta vastaavalle johtajalle (Chief Privacy Officer) heti sen saatuaan.

#### 15 – Noudattaminen ja noudattamisen valvonta

Ylimmän johdon tuella Amgen nimittää sopivia henkilöstön jäseniä, mukaan lukien joukon tietosuojavastaavia, valvomaan sääntöjen noudattamista ja varmistamaan sen.

Amgenin yksityisyyden suojasta vastaavan johtajan (Chief Privacy Officer) vastuulla ovat mm. seuraavat:

- johtokunnan neuvominen
- tietosuojan noudattamisen varmistaminen maailmanlaajuisella tasolla
- tietosuojan noudattamisesta raportointi säännöllisesti
- yhteistyö tietosuojaviranomaisten kanssa tutkinnoissa.

Yksityisyyden suojasta vastaava johtaja (Chief Privacy Officer) on vastuussa globaalista tietosuojaosastosta (Global Privacy Office), jonka tiimi antaa asiantuntijatukea Amgenin yksiköille maailmanlaajuisesti.

Paikallisella tasolla tietosuojavastaavat ovat vastuussa paikallisten rekisteröityjen henkilöiden tietosuojapyyntöjen käsittelemisestä, sääntöjen noudattamisesta paikallisella tasolla tietosuojaosaston (Privacy Office) tuella sekä vakavien tietosuojuongelmien raportoimisesta yksityisyyden suojasta vastaavalle johtajalle (Chief Privacy Officer). Amgen pitää yllä tietosuojavastaavaverkostoa ja varmistaa, että jokaiselle maalle, jossa Amgenilla (mukana olevalla yrityksellä) on yritysyksikkö, valitaan tai nimitetään tietosuojavastaava. Tämä nimitys tehdään yhteistyössä tietosuojavastaavan paikallisen esimiehen ja paikallisen henkilöstöosaston kanssa.

Yleensä tietosuojavastaavat ovat paikallisia terveydenhuollon säännöksistä vastaavia esimiehiä, jotka raportoivat maailmanlaajuiselle säännönmukaisuus- ja liiketoimintaetiikkaosastolle (Worldwide Compliance and Business Ethics). Myös tietosuojaosasto (Privacy Office) raportoi maailmanlaajuiselle säännönmukaisuus- ja liiketoimintaetiikkaosastolle (Worldwide Compliance and Business Ethics). Joissain harvoissa tapauksissa johtuen Amgenin yksikön erityispiirteistä tai erityisolosuhteista tietosuojavastaava voi tulla jostain toisesta toiminnosta, esimerkiksi sääntelytehtävistä (Regulatory). Joka tapauksessa tietosuojaosasto (Privacy Office) takaa, että tietosuojavastaavat koulutetaan asianmukaisesti ja heillä on riittävä esimieskokemus ja asiantuntemus hoitaakseen tietosuojavastaavan tehtävät. Lisäksi tietosuojavastaavilla on suora yhteys yksityisyyden suojasta vastaavaan johtajaan (Chief Privacy Officer) samoin kuin tietosuojaosaston (Privacy Office) henkilökuntaan siltä varalta, että he tarvitsevat lisäapua.

#### 16 – Toimet siinä tapauksessa, että kansallinen lainsäädäntö estää sitovien tietosuojasääntöjen noudattamisen

Jos konserniin kuuluvalla taholla on syytä uskoa siihen sovellettavan lainsäädännön estävän yhtiötä täyttämästä sitovien tietosuojasääntöjen asettamia velvoitteita ja lainsäädännöllä on merkittävä vaikutus säännöissä luvattujen takuiden osalta, asiasta tulee ilmoittaa välittömästi yksityisyyden suojasta vastaavalle johtajalle (Chief Privacy Officer) (ellei lainvalvontaviranomainen kiellä sitä esimerkiksi rikoslain mukaisesti lainvalvontaviranomaisen tekemän tutkimuksen salassapitovelvollisuuden nojalla).

Mikäli kansallisen lainsäädännön ja sitovien tietosuojasääntöjen asettamien velvoitteiden välillä on ristiriita, yksityisyyden suojasta vastaava johtaja (Chief Privacy Officer) päättää yhdessä paikallisen lakimiehen ja paikallisen tietosuojavastaavan kanssa, millaisia oikeudellisesti asianmukaisia toimia tarvitaan. Tarvittaessa yksityisyyden suojasta vastaava johtaja (Chief Privacy Officer) neuvottelee asiaankuuluvien tietosuojaviranomaisten kanssa.

#### 17 – Sisäiset valitusmekanismit

Amgen laajentaa ja hyödyntää olemassa olevia valitusten käsittelyprosessejaan niin, että ne kattavat sitoviin

tietosuojasääntöihin liittyvät valitukset ja huolenaiheet.

Kuka tahansa rekisteröity henkilö voi valittaa milloin tahansa siitä, että mukana oleva yritys ei noudata sitovia tietosuojasääntöjä. Nämä valitukset käsitellään tietosuojaosastossa (Privacy Office) yksityisyyden suojasta vastaavan johtajan (Chief Privacy Officer) johdolla yhteistyössä asiaankuuluvan paikallisen tietosuojavastaavan kanssa.

Amgen suosittelee, että tällaiset valitukset toimitetaan kirjallisesti joko postitse tai sähköpostitse suoraan tietosuojaosastolle (Privacy Office) tai tytäryhtiölle. Rekisteröidyt henkilöt voivat myös sovellettavien lakien niin salliessa soittaa Business Conduct Hotlineen sitovia tietosuojasääntöjä koskevista valituksista.

Jos valitus tehdään paikallisesti, tietosuojavaltuutettu kääntää sen tarvittaessa ja lähettää sen viipymättä tietosuojaosastolle (Privacy Office).

Rekisteröity henkilö saa ensimmäisen vastauksen, jossa hänelle kerrotaan, että valitus on tarkastelun alla ja että hän saa vastauksen kahden kuukauden sisällä.

Jos tietosuojaosasto (Privacy Office) havaitsee yksittäisen henkilön väärinkäytöksen, otetaan käyttöön asianmukaiset kurinpitotoimenpiteet, mukaan lukien välitön työsuhteen päättäminen, siinä määrin kuin sovellettava laki sallii.

Kahden kuukauden sisällä rekisteröity henkilö saa vastauksen, jossa hänelle kerrotaan valituksen tuloksesta.

Rekisteröidylle henkilölle ilmoitetaan, että jos Amgenin vastaus ei tyydytä häntä, hän voi tehdä kantelun asiaankuuluvassa tuomioistuimessa tai tietosuojaviranomaiselle.

Tämä valitusten käsittelyprosessi julkistetaan yhdessä sitovien tietosuojasääntöjen kanssa kappaleessa 7 mainitulla tavalla.

#### 18 – Kolmannen osapuolen edunsaajan oikeudet ja vastuut

Rekisteröidyllä henkilöllä, jonka henkilötiedot ovat lähtöisin säännelystä maasta ja joka väittää, että sitovissa tietosuojasäännöissä mainittuja velvoitteita on rikottu, on oikeus panna säännöt täytäntöön kolmannen osapuolen edunsaajana. Nämä oikeudet käsittävät taattujen oikeuksien rikkomiseen liittyvät oikeuskeinot sekä oikeuden saada korvaus. Mahdollinen vastuu rajoittuu todellisiin kärsittyihin vahinkoihin.

Sovellettavan lainkäyttöalueen sallimissa rajoissa rekisteröidyt henkilöt voivat tehdä kantelun jommassakummassa seuraavista:

- tietojen viejän lainkäyttöalueella; mikäli rekisteröidyn henkilön henkilötietojen alkuperä on ETA-maassa sijaitseva tietojen viejä, toimivaltainen lainkäyttöalue on ETA-maassa sijaitsevan tietojen viejän sijaintipaikka
- toimivaltaisille tietosuojaviranomaisille.

Rekisteröidyllä henkilöllä, joka on kärsinyt sitovissa tietosuojasäännöissä mainittujen velvoitteiden rikkomuksesta tietojen viejän tai tietojen tuojan taholta, on oikeus saada tietojen viejältä korvaus kärsityistä vahingoista. Jos tietojen viejän tai tietojen tuojan katsotaan olevan vastuussa rikkomuksesta, se korvaa toiselle osapuolelle kaikki tälle aiheutuneet kulut, maksut, vahingot, kustannukset ja menetykset siinä määrin, kuin sen katsotaan olevan vastuussa niistä.

Tietojen viejä ja tietojen tuoja voidaan vapauttaa vahingonkorvausvastuusta sitovien tietosuojasääntöjen perusteella, jos osoitetaan, että EU:n ulkopuolinen konserniin kuuluva yritys ei ole rikkonut sitovia tietosuojasääntöjä vastaan tai ei ole vastuussa rekisteröidylle henkilölle aiheutuneista vahingoista. Todistustaakka on kuitenkin tietojen viejällä ja tietojen tuojalla.

Tiedonkäsittelijänä toimiva tietojen tuoja ei voi vetäytyä vastuustaan vetoamalla siihen, että alihankkijana toimiva taho ei täyttänyt veloitteitaan. Jos rekisteröity henkilö haluaa nostaa kanteen tietojen viejää vastaan sitovien tietosuojasääntöjen rikkomuksen perusteella muttei pysty, koska tietojen viejä on todenperäisesti kadonnut tai lakannut oikeudellisesti olemasta tai tullut maksukyvyttömäksi, rekisteröity henkilö voi panna oikeutensa täytäntöön suoraan tietojen tuojaa vastaan. Jos jokin toinen yritys on ottanut hoitaakseen tietojen viejän tai tietojen tuojan kaikki oikeudelliset veloitteet sopimuksella tai lain perusteella, rekisteröity henkilö voi panna oikeutensa täytäntöön tätä seuraajaa vastaan. Tietojen tuojan vastuu koskee ainoastaan sen omaa sitoviin tietosuojasääntöihin liittyvää käsittelytoimintaa.

#### 19 – Yhteistyö tietosuojaviranomaisten kanssa ja keskinäinen avunanto

Mukana olevien yritysten tulee toimia yhteistyössä ja avustaa toisiaan käsiteltäessä rekisteröidyltä henkilöltä tullutta pyyntöä tai valitusta tai tietosuojaviranomaisten tutkimusta tai tiedustelua.

Mukana olevat yritykset vastaavat yhdessä yksityisyyden suojasta vastaavan johtajan (Chief Privacy Officer) kanssa tietosuojaviranomaisten sitoviin tietosuojasääntöihin liittyviin pyyntöihin kohtuullisen ajan sisällä ja asianmukaisesti, ja noudattavat toimivaltaisen tietosuojaviranomaisen neuvoja ja päätöksiä sitovien tietosuojasääntöjen täytäntöönpanosta.

#### 20 – Sitovien tietosuojasääntöjen päivitys ja muutokset

Amgen pidättää oikeuden muuttaa ja päivittää näitä sitovia tietosuojasääntöjä milloin tahansa. Sitovien tietosuojasääntöjen päivitys saattaa olla tarpeen erityisesti muuttuneiden oikeudellisten vaatimusten, Amgen-konsernin merkittävien rakennemuutosten tai toimivaltaisten tietosuojaviranomaisten virallisten vaatimusten vuoksi.

Amgen raportoi kaikista sitovia tietosuojasääntöjä tai mukana olevien yritysten luetteloa koskevista merkittävistä muutoksista kaikille muille mukana oleville yrityksille ja tietosuojaviranomaisille, jotta huomioidaan sääntely-ympäristön ja yhtiön rakenteen muutokset.

Jotkut muutokset saattavat vaatia uuden luvan tietosuojaviranomaisilta.

Yksityisyyden suojasta vastaava johtaja (Chief Privacy Officer) pitää yllä ajan tasalla olevaa luetteloa sitovissa tietosuojasäännöissä mukana olevista yrityksistä ja sitovien tietosuojasääntöjen mahdollisesti suojaamista säännellyistä maista, seuraa sääntöjen mahdollisia päivityksiä ja välittää pyydettyä tarvittavat tiedot rekisteröidylle henkilöille ja tietosuojaviranomaisille.

Amgen on sitoutunut siihen, ettei mitään siirtoja tehdä uusille mukana oleville yrityksille ennen kuin uusi mukana oleva yritys on täysin sitoutunut sitoviin tietosuojasääntöihin ja noudattaa niitä.

Kaikki sitoviin tietosuojasääntöihin ja mukana olevien yritysten luetteloon tehdyt muutokset raportoidaan kerran vuodessa luvat myöntäville tietosuojaviranomaisille. Mukaan liitetään lyhyt selvitys päivityksen syistä.

Olenaisista sääntömuutoksista tiedotetaan myös rekisteröidyille henkilöille jollakin sitovien tietosuojasääntöjen kohdassa 7 mainitulla tavalla.

#### 21 – Kansallisen lainsäädännön ja sitovien tietosuojasääntöjen suhde

Paikallinen lainsäädäntö syrjäyttää sitovat tietosuojasäännöt, mikäli se vaatii korkeatasoisempaa henkilötietojen suojelua. Mikäli soveltuva paikallinen lainsäädäntö tarjoaa henkilötiedoille sitovia tietosuojasääntöjä alhaisemman suojan, sovelletaan sitovia tietosuojasääntöjä.

Mikäli soveltuvan paikallisen lainsäädännön aiheuttamat velvoitteet ovat ristiriidassa sitovien tietosuojasääntöjen kanssa, mukana olevan yrityksen tulee ilmoittaa tästä viipymättä yksityisyyden suojasta vastaavalle johtajalle (Chief Privacy Officer).

Joka tapauksessa direktiivin 95/46/EY artiklassa 4 ja asiaankuuluvissa paikallisissa laeissa määrätään, että henkilötiedot tulee käsitellä soveltuvan lainsäädännön mukaisesti.