



## Amgen ES saistošie korporatīvie noteikumi — kontrolieris (ES BCR)

Pēdējo reizi atjaunināts: 2023. gada 12. decembrī

### Ievads

- (A) Amgen ir biotehnoloģiju līderis, kas apņēmieš sniegt pakalpojumus pacientiem ar smagām slimībām. Šie ES saistošie korporatīvie noteikumi — pārzinis (" ES BCR ") pauž Amgen apņemšanos nodrošināt privātumu un datu aizsardzību, jo tā cenšas nodrošināt atbilstošu aizsardzību personas datu pārsūtīšanai un apstrādei starp iesaistītajiem uzņēmumiem.
- (B) Visi iesaistītie uzņēmumi un viss personāls ir apņēmieš ievērot šos ES BCR un tiem ir juridiskas saistības attiecībā uz personas datiem ES BCR darbības jomā. Par noteikumu neievērošanu var tikt piemērots disciplinārsods, kā to pieļauj vietējie tiesību akti. Galvenais atbilstības speciālists sadarbībā ar galveno privātuma amatpersonu nodrošina ES BCR izpildi. Iesaistīto uzņēmumu sarakstu var atrast šeit: <https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf>. Ar visiem iesaistītajiem uzņēmumiem var sazināties, izmantojot e-pasta adresi [privacy@amgen.com](mailto:privacy@amgen.com), ja rodas jautājumi par šiem ES BCR.
- (C) Šie ES BCR ir pieņemti, atsaucoties uz ES datu aizsardzības likumiem. Amgen France ir atbildīga par to, lai nodrošinātu, ka iesaistītie uzņēmumi ievēro šos ES BCR. Privātpersonas var īstenot šos ES BCR pret Amgen France kā trešās puses saņēmēju, kā aprakstīts tālāk. Šie ES BCR ir pieejami Amgen tīmekļa vietnē: [www.amgen.com/bcr](http://www.amgen.com/bcr). Lai pieprasītu kopiju, lūdzu, sazinieties ar Amgen pa e-pastu [privacy@amgen.com](mailto:privacy@amgen.com).

### 1. Darbības joma

- 1.1. Amgen EU BCR attiecas uz visu datu subjektu personas datu automatizētu vai manuālu pārsūtīšanu un apstrādi, ko veic iesaistītais uzņēmums, kas darbojas kā datu pārzinis vai darbojas kā datu apstrādātājs citai iesaistītajai sabiedrībai, kas darbojas kā datu pārzinis, jebkurā no šiem gadījumiem:
- 1.1.1. Iesaistītā sabiedrība, kas apstrādā personas datus, ir reģistrēta ES; vai
  - 1.1.2. Iesaistītā sabiedrība, kas apstrādā personas datus, nav reģistrēta EEZ un ir saņēmusi personas datus no EEZ reģistrēta iesaistītā uzņēmuma; vai
  - 1.1.3. personas datu tālākai pārsūtīšanai no datu importētājiem datu importētājiem.
- 1.2. Pārskats par datu plūsmām saskaņā ar šiem ES BCR ir pieejams 1. pielikumā.

### 2. Definīcijas

<b>Noteikumi</b>	<b>Definīcijas</b>
<b>Amgen Francija</b>	Amgen SAS, Francijā reģistrēts uzņēmums, kura juridiskā adrese ir 25 quai du Président Paul Doumer, 92400 Courbevoie.
<b>Piemērojamiem tiesību aktiem</b>	ES tiesību akti un/vai (attiecīgā gadījumā) EEZ dalībvalstu nacionālie vai vietējie tiesību akti (tostarp bez ierobežojuma ES datu aizsardzības tiesību akti).
<b>Atbilstības vadītājs</b>	Persona, kas ir iesaistītā uzņēmuma vispasaules atbilstības un biznesa ētikas departamenta veselības aprūpes atbilstības nodaļā, kam ir deleģēta atbildība par datu aizsardzību un privātumu un, ja tā ir atšķirta no vietējā datu aizsardzības speciālista, atbalsta vietējo datu aizsardzības inspektoru tā pienākumu un uzdevumu veikšanā.
<b>Piekrišana</b>	Jebkura brīvi dota konkrēta, informēta un nepārprotama norāde uz datu subjekta vēlmēm, ar kuru datu subjekts ar paziņojumu vai nepārprotamu apstiprinošu darbību apliecina piekrišanu ar viņu saistīto personas datu apstrādei.
<b>Datu pārzinis</b>	Jebkura struktūra, kas pieņem lēmumus par personas datu vākšanu un apstrādi, tostarp lēmumus par personas datu apstrādes mērķiem un veidu.
<b>Datu eksportētājs</b>	Iesaistītais uzņēmums, kas darbojas kā datu pārzinis, kas reģistrēts EEZ un nodod personas datus datu importētājam.
<b>Datu importētājs</b>	Iesaistītā sabiedrība, kas nav reģistrēta EEZ un kas (a) saņem personas datus no datu eksportētāja vai (b) saņem tālāku personas datu pārsūtīšanu saskaņā ar šo ES BCR 1. panta c) apakšpunktu.
<b>Datu apstrādātājs</b>	Persona vai juridiska persona, kas apstrādā personas datus datu pārziņa vārdā.
<b>Datu aizsardzības iestāde (DPA)</b>	Neatkarīga publiska datu aizsardzības iestāde, ko izveidojusi EEZ dalībvalsts.
<b>Datu aizsardzības inspektors</b>	Persona, kuru Amgen galvenais privātuma speciālists ir iecēlis par atbildīgo par privātuma un datu aizsardzības uzraudzību vietējā līmenī, kā arī par atbilstošu un nepieciešamo kontroles pasākumu ieviešanu.
<b>Datu subjekts</b>	Fiziska persona, kuru var tieši vai netieši identificēt, atsaucoties uz Personas datiem. Datu subjekts var būt (bez ierobežojuma): <ul style="list-style-type: none"> <li>• pacients/klīniskā pētījuma datu subjekts (kurā var būt bērns, kas jaunāks par 18 gadiem)</li> <li>• veselības aprūpes speciālists</li> <li>• darbinieks</li> <li>• pārdevējs vai piegādātājs</li> </ul>

<b>Noteikumi</b>	<b>Definīcijas</b>
<b>EEZ</b>	Eiropas Savienības dalībvalstis (Austrija, Beļģija, Bulgārija, Horvātija, Kipras Republika, Čehija, Dānija, Igaunija, Somija, Francija, Vācija, Grieķija, Ungārija, Īrija, Itālija, Latvija, Lietuva, Luksemburga, Malta, Nīderlande, Polija, Portugāle, Rumānija, Slovākija, Slovēnija, Spānija un Zviedrija) un Islande, Lihtenšteina un Norvēģija (visas ir “ <b>EEZ dalībvalstis</b> ”).
<b>ES datu aizsardzības likumi</b>	VDAR un (ja piemērojams) vietējie vai valsts tiesību akti, kas attiecas uz datu aizsardzību un personas datu apstrādi, kā arī attiecīgās EEZ dalībvalsts GDPR ieviešanu.
<b>GDPR</b>	Vispārīgā datu aizsardzības regula ((ES) 2016/679).
<b>Iesaistītais uzņēmums</b>	Amgen grupas juridiska persona, kurai ir saistoši ES BCR.
<b>Personas dati</b>	Jebkura informācija, kas attiecas uz datu subjektu, piemēram, vārds, identifikācijas numurs, atrašanās vietas dati, tiešsaistes identifikators vai viens vai vairāki faktori, kas raksturīgi vai informācija, kas attiecas uz šīs personas fizisko, fizioloģisko, ģenētisko, garīgo, ekonomisko, kultūras vai sociālo identitāti.. Personas datu piemēri var ietvert: <ul style="list-style-type: none"> <li>• Datu subjekta vārds, adrese, sociālās apdrošināšanas numurs, autovadītāja apliecības numurs, finanšu konta informācija, ģimenes informācija vai medicīniskie dati,</li> <li>• Veselības aprūpes speciālista vārds, uzvārds, profesionālā izglītība un zāļu izrakstīšanas prakse,</li> <li>• E-pasta adrese un cita identificējoša informācija, ko sniedz kāds, kas apmeklē Amgen vietni.</li> </ul> Iepriekš minētais saraksts ir tikai orientējošs un nav pilnīgs.
<b>Personas datu pārkāpums</b>	Jebkurš drošības pārkāpums, kas izraisa nejaušu vai nelikumīgu pārsūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšanu, nozaudēšanu, pārveidošanu, neatļautu izpaušanu vai piekļuvi tiem.
<b>Personāls</b>	Visi jebkuras iesaistītās sabiedrības darbinieki un kontingenti darbinieki (tostarp konsultanti, pagaidu aģentūru darbinieki un līgumstrādnieki).
<b>Apstrāde</b>	Jebkura darbība vai darbību kopums, kas tiek veikts ar personas datiem (vai personas datu kopām), neatkarīgi no tā, vai tiek izmantots automatizēts līdzeklis, piemēram, vākšana, ierakstīšana, organizēšana, strukturēšana, uzglabāšana, pielāgošana vai pārveidošana, izguve, konsultēšana, izmantošana, izpaušana nosūtot, izplatot vai citādi padarot pieejamu, saskaņojot vai kombinējot, ierobežojot, dzēšot vai iznīcinot .
<b>Jūtīgi personas dati</b>	Personas dati, kas atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai piederību arodbiedrībām, un

<b>Noteikumi</b>	<b>Definīcijas</b>
	<p>ģenētisko datu, biometrisku datu apstrāde nolūkā unikāli identificēt fizisku personu, datus par veselību vai datus par fiziskās personas dzimumdzīvi vai seksuālo orientāciju.</p> <p>Atsevišķi ES datu aizsardzības likumiem, Amgen par <b>jūtīgiem</b> personas datiem uzskata arī finanšu informāciju un informāciju, ko varētu izmantot, lai veiktu identitātes zādzību (piemēram, sociālās apdrošināšanas numuru, autovadītāja apliecības numuru, kredītkarti vai citu bankas konta informāciju).</p>
<b>Tehniskie un organizatoriskie drošības pasākumi</b>	Tehnoloģiskie un organizatoriski pasākumi, kuru mērķis ir aizsargāt personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu nozaudēšanu, pārveidošanu, neatļautu izpaušanu vai piekļuvi, jo īpaši, ja apstrāde ietver datu pārsūtīšanu tīklā, un pret visiem citiem nelikumīgiem apstrādes veidiem.
<b>Trešā puse</b>	<p>Fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita struktūra, kas nav datu subjekts, iesaistītais uzņēmums, kas darbojas kā datu pārzinis, un iesaistītais uzņēmums, kas darbojas kā datu apstrādātājs.</p> <p>Amgen pārdevējs tiek uzskatīts par trešo pusi. Atkarībā no apstākļiem trešā puse var darboties kā datu pārzinis vai datu apstrādātājs saistībā ar personas datu apstrādi.</p>
<b>Pārdevējs</b>	Jebkura fiziska vai juridiska persona, uzņēmums vai organizācija, kas nodrošina preces un/vai pakalpojumus iesaistītajam uzņēmumam saskaņā ar līgumattiecībām un/vai ir personas datu saņēmējs no šādas iesaistītās sabiedrības, lai sniegtu šīs preces un/vai pakalpojumus.

Amgen interpretē noteikumus šajos ES BCR saskaņā ar ES datu aizsardzības likumiem.

### 3. Mērķa ierobežojums

- 3.1. Personas datus apstrādā skaidriem, konkrētiem un likumīgiem mērķiem saskaņā ar VDAR 5. panta 1. punkta b) apakšpunktu.
- 3.2. Personas dati netiks apstrādāti veidā, kas nav savienojams ar likumīgiem mērķiem, kādiem personas dati tika vākti, vai ar piemērojamajiem tiesību aktiem. Datu importētājiem ir pienākums ievērot sākotnējos mērķus, glabājot un/vai turpmāk apstrādājot personas datus vai apstrādājot personas datus, ko tiem pārsūtījis cits iesaistītais uzņēmums. Personas datu apstrādes mērķi var mainīt tikai ar datu subjekta piekrišanu vai tiktāl, cik to atļauj piemērojamie tiesību akti.
- 3.3. Jūtīgiem personas datiem tiks nodrošināti papildu aizsardzības pasākumi, piemēram, ES datu aizsardzības likumi.

### 4. Datu kvalitāte un proporcionalitāte

- 4.1. Personas datiem jābūt precīziem un, ja nepieciešams, atjauninātiem; ir jāveic visi saprātīgie pasākumi, lai nodrošinātu, ka personas dati, kas ir neprecīzi, ņemot vērā to apstrādes mērķus, tiek nekavējoties dzēsti vai laboti.
- 4.2. apakšpunktu personas datiem ir jābūt adekvātiem, atbilstošiem un ierobežotiem ar to, kas ir nepieciešams saistībā ar nolūkiem, kādiem tie tiek apstrādāti.
- 4.3. Personas datu apstrāde tiks vadīta ar mērķi ierobežot personas datu vākšanu, apstrādi un/vai izmantošanu tikai tiktāl, cik tas ir nepieciešams, t.i., pēc iespējas mazāk personas datu. Ir jāapsver anonīmu vai pseidonīmu datu iespēja, ja izmaksas un pūles ir samērīgas ar vēlamo mērķi.
- 4.4. Personas dati, kas vairs nav nepieciešami uzņēmējdarbības mērķim, kuram tie sākotnēji tika vākti un glabāti, ir jādzēš saskaņā ar Amgen ierakstu saglabāšanas grafiku. Gadījumā, ja tiek piemēroti likumā noteiktie glabāšanas periodi vai juridiskā aizturēšana, dati tiks bloķēti, nevis dzēsti. Beidzoties glabāšanas periodam vai likumīgai aizturēšanai, dati tiks dzēsti.

## **5. Personas datu apstrādes juridiskais pamats**

- 5.1. Personas datu apstrāde ir pieļaujama tikai tad, ja ir izpildīts vismaz viens no šiem priekšnoteikumiem:
  - 5.1.1. Datu subjekts ir devis savu piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem mērķiem.
  - 5.1.2. Apstrāde ir nepieciešama, lai izpildītu līgumu, kura puse ir datu subjekts, vai lai veiktu darbības pēc datu subjekta pieprasījuma pirms līguma noslēgšanas.
  - 5.1.3. Apstrāde ir nepieciešama, lai izpildītu juridisko pienākumu, kas uz datu pārzini attiecas saskaņā ar piemērojamiem tiesību aktiem.
  - 5.1.4. Apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas svarīgas intereses, piemēram, dzīvību, veselību vai drošību.
  - 5.1.5. Apstrāde ir nepieciešama, lai veiktu uzdevumu, kas tiek veikts sabiedrības interesēs vai datu pārzinim piešķirto oficiālo pilnvaru īstenošanai.
  - 5.1.6. Apstrāde ir nepieciešama datu pārziņa vai trešās puses likumīgo interešu īstenošanai, izņemot gadījumus, kad šīs intereses ir svarīgākas par datu subjekta interesēm vai pamattiesībām un brīvībām.
- 5.2. Personas datu apstrāde saistībā ar sodāmību un noziedzīgiem nodarījumiem tiek veikta tikai tad, ja apstrādi atļauj piemērojami tiesību akti, kas paredz atbilstošus datu subjektu tiesību un brīvību aizsardzības pasākumus.

## **6. Jūtīgu personas datu apstrāde**

- 6.1. Ja saskaņā ar konkrētu un likumīgu mērķi iesaistītajam uzņēmumam ir jāapstrādā jūtīgi personas dati, iesaistītais uzņēmums to darīs tikai tad, ja:

- 6.1.1. Datu subjekts ir devis nepārprotamu piekrišanu šo jūtīgo personas datu apstrādei vienam vai vairākiem noteiktiem mērķiem, izņemot gadījumus, kad piemērojamie tiesību akti paredz, ka datu subjekts nevar atcelt VDAR 9. panta 1. punktā noteikto aizliegumu.
- 6.1.2. Apstrāde ir nepieciešama, lai izpildītu datu pārziņa pienākumus un īpašās tiesības nodarbinātības un sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā, ciktāl to atļauj piemērojamie tiesību akti vai koplīgums saskaņā ar piemērojamajiem tiesību aktiem paredzot atbilstošus datu subjekta pamattiesību un interešu aizsardzības pasākumus.
- 6.1.3. Apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālās intereses, ja datu subjekts fiziski vai juridiski nav spējīgs dot savu piekrišanu.
- 6.1.4. Apstrādi veic, veicot tās likumīgās darbības ar atbilstošām garantijām, ko nodrošina fonds, asociācija vai jebkura cita bezpeļņas organizācija ar politisku, filozofisku, reliģisku vai arodbiedrību mērķi, un ar nosacījumu, ka apstrāde attiecas tikai uz struktūras locekļiem vai personām, kuras regulāri sazinās ar to saistībā ar tās mērķiem un, ka dati netiek izpausti ārpus šīs struktūras bez datu subjektu piekrišanas.
- 6.1.5. Apstrāde attiecas uz jūtīgiem personas datiem, kurus datu subjekts ir acīmredzami publiskojis.
- 6.1.6. Jūtīgu personas datu apstrāde ir nepieciešama, lai izvirzītu, īstenotu vai aizstāvētu juridiskas prasības.
- 6.1.7. Apstrāde ir nepieciešama būtisku sabiedrības interešu dēļ, pamatojoties uz piemērojamiem tiesību aktiem, kas ir samērīgi ar izvirzīto mērķi, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un īpašus pasākumus, lai aizsargātu datu subjekta pamattiesības un intereses. .
- 6.1.8. Jūtīgo personas datu apstrāde ir nepieciešama profilaktiskās vai arodmedicīnas nolūkos, darbinieka darbības novērtēšanai, medicīniskās diagnozes noteikšanai, veselības vai sociālās aprūpes, vai ārstēšanas nodrošināšanai, vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldībai, pamatojoties uz piemērojamiem tiesību aktiem vai saskaņā ar līgumu ar veselības aprūpes speciālistu, un ja šos jūtīgos personas datus apstrādā veselības aprūpes speciālists vai par to ir atbildīgs veselības aprūpes speciālists, uz šādu speciālistu ir jāattiecinā dienesta noslēpuma pienākums saskaņā ar piemērojamiem tiesību aktiem vai noteikumiem, ko noteikušas EEZ dalībvalsts kompetentās iestādes vai cita persona, uz kuru arī attiecas pienākums glabāt noslēpumu saskaņā ar piemērojamiem tiesību aktiem vai noteikumiem, ko izstrādājušas kompetentās iestādes EEZ dalībvalstī.
- 6.1.9. Jūtīgu personas datu apstrāde sabiedrības veselības jomā ir nepieciešama sabiedrības interešu dēļ, piemēram, lai aizsargātu pret nopietniem pārrobežu veselības apdraudējumiem vai nodrošinātu augstus veselības aprūpes un zāļu vai medicīnas ierīču kvalitātes un drošības standartus, pamatojoties uz piemērojamiem tiesību aktiem, kas paredz piemērotus un konkrētus pasākumus datu subjekta tiesību un brīvību, jo īpaši dienesta noslēpuma, aizsardzībai.

- 6.1.10. Jūtīgu personas datu apstrāde ir nepieciešama arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēsturiskās pētniecības nolūkos vai statistikas nolūkos saskaņā ar GDPR 89. panta 1. punktu, pamatojoties uz piemērojamiem tiesību aktiem, kas ir samērīgi ar izvirzīto mērķi, ievērojot tiesību uz datu aizsardzību būtību un paredzēt piemērotus un konkrētus pasākumus, lai aizsargātu datu subjekta pamattiesības un intereses.

## **7. Pārredzamība un tiesības uz informāciju**

- 7.1. Visi iesaistītie uzņēmumi apstrādā personas datus pārredzamā veidā. Amgen ir apņēmusies padarīt ES BCR, tostarp kontaktinformāciju, viegli pieejamus un viegli pieejamus ikvienam datu subjektam un informēt datu subjektus par viņu personas datu pārsūtīšanu un apstrādi. Šie ES BCR ir pieejami Amgen tīmekļa vietnē: [www.amgen.com/bcr](http://www.amgen.com/bcr). Lai pieprasītu kopiju, lūdzu, sazinieties ar Amgen pa e -[pastu\\_privacy@amgen.com](mailto:pastu_privacy@amgen.com). Amgen izmantos arī dažādus saziņas līdzekļus, piemēram, korporatīvās vietnes, tostarp iekšējās tīmekļa vietnes un biļetenus, līgumus un īpašus paziņojumus par konfidencialitāti, lai izpildītu šo pieejamības prasību. Turklāt Amgen bez nepamatotas kavēšanās informēs datu subjektus, izmantojot šos saziņas līdzekļus, par visiem ES BCR vai iesaistīto uzņēmumu saraksta atjauninājumiem vai izmaiņām.
- 7.2. Datu subjektiem, kuru personas datus apstrādā iesaistītais uzņēmums, jāsniedz GDPR 13. un 14. pantā noteiktā informācija.
- 7.3. Ja personas dati netiek saņemti no datu subjekta, pienākums informēt datu subjektu nav spēkā, ja šādas informācijas sniegšana izrādās neiespējama vai būtu saistīta ar nesamērīgām pūlēm, vai, ja ierakstīšana vai izpaušana ir skaidri noteikta likumā.

## **8. Tiesības piekļūt datiem, labot, dzēst un ierobežot datus**

- 8.1. Ikvienam datu subjektam ir tiesības saņemt no iesaistītā uzņēmuma apstiprinājumu par to, vai personas dati par viņu tiek apstrādāti, un, ja tas notiek, piekļuvi personas datiem un informācijai, kas jāsniedz saskaņā ar pantu. VDAR 15. panta 1. punkts. Šā pieprasījuma turpmākie pasākumi, tostarp iespēja iekasēt maksu vai termiņu, lai atbildētu uz šādu pieprasījumu, tiks pakļauti piemērojamiem tiesību aktiem, un par tiem attiecīgi paziņos datu subjektam, kad viņš/viņa iesniedz pieprasījumu.
- 8.2. Katram datu subjektam ir tiesības pieprasīt personas datu labošanu, dzēšanu vai ierobežošanu, jo īpaši, ja dati ir nepilnīgi vai neprecīzi.
- 8.3. Ikvienam datu subjektam ir tiesības jebkurā laikā, pamatojoties uz viņa konkrēto situāciju, iebilst pret savu personas datu apstrādi uzdevuma izpildei, kas tiek veikts sabiedrības interesēs vai iesaistītā uzņēmuma vai trešās puses likumīgās interesēs (tostarp profilēšanu, balstoties uz šiem pamatojumiem). Iesaistītais uzņēmums vairs neapstrādās personas datus, ja vien netiek uzrādīti pārliecinoši likumīgi iemesli apstrādei, kas ir svarīgāki par datu subjekta interesēm, tiesībām un brīvībām, vai juridisku prasību noteikšanai, īstenošanai vai aizstāvībai.
- 8.4. Ikvienam datu subjektam ir tiesības (bez maksas) iebilst pret ar viņu saistīto personas datu apstrādi tiešā mārketinga nolūkos, kas ietver profilēšanu, ciktāl tā ir saistīta ar šādu tiešo mārketingu. Ja datu subjekts izmanto savas tiesības iebilst pret ar viņu saistīto personas datu apstrādi tiešā mārketinga nolūkos, iesaistītajam uzņēmumam ir jāpārtrauc personas datu apstrāde šim nolūkam.

- 8.5. Katram datu subjektam ir tiesības saņemt paziņojumu trešajām pusēm, kurām ir izpausti personas dati, par jebkādu labošanu, dzēšanu vai ierobežošanu saskaņā ar VDAR 19. pantu.
- 8.6. Katram datu subjektam ir tiesības zināt loģiku, kas saistīta ar jebkādu automatisku personas datu apstrādi saskaņā ar VDAR 13. panta 2. punkta f) apakšpunktu.
- 8.7. Ja apstrāde balstās uz piekrišanu, katram datu subjektam ir tiesības jebkurā laikā atsaukt savu piekrišanu. Piekrišanas atsaukšana neietekmē apstrādes, kuras pamatā ir piekrišana pirms tās atsaukšanas, likumību.
- 8.8. Katram datu subjektam ir tiesības iesniegt sūdzību iesaistītajam uzņēmumam par personas datu apstrādi, izmantojot iekšējo sūdzību iesniegšanas mehānismu, kas paredzēts saskaņā ar 17. pantu.
- 8.9. Jebkuri pieprasījumi saskaņā ar šo 8. pantu (vai tālāk 9. pantu) jānosūta iesaistītajam uzņēmumam uz: [privacy@amgen.com](mailto:privacy@amgen.com). Lai gan pieprasījumu iesniegšana pa e-pastu ir ļoti ieteicama, tas neizslēdz datu subjekta mutisku pieprasījumu. Iesaistītais uzņēmums nekavējoties informē datu subjektu par pieprasījuma iznākumu un ne vēlāk kā viena mēneša laikā pēc pieprasījuma saņemšanas (tostarp iemeslus, kāpēc nav veiktas darbības, un iespēju iesniegt sūdzību kompetentajai datu aizsardzības iestādei un/vai vērsties pēc tiesiskās aizsardzības). Šo viena mēneša termiņu vajadzības gadījumā var pagarināt vēl par diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu. Iesaistītais uzņēmums informē datu subjektu par katru šādu pagarinājumu viena mēneša laikā pēc pieprasījuma saņemšanas, norādot kavēšanās iemeslus. Jebkāda saziņa, darbība un/vai informācija, kas sniegta saistībā ar pieprasījumu saskaņā ar šo 8. pantu (vai tālāk 9. pantu), datu subjektam tiek sniegta bez maksas. Ja datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši to atkārtotības dēļ, iesaistītais uzņēmums var: (a) iekasēt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas sniegšanu vai saziņu vai pieprasītās darbības veikšanu, vai b) atsakās rīkoties saskaņā ar pieprasījumu. Iesaistītajam uzņēmumam ir pienākums pierādīt pieprasījuma acīmredzami nepamatoto vai pārmērīgo raksturu.

## 9. Automatizēti individuālie lēmumi

- 9.1. Datu subjektam ir tiesības netikt pakļautam lēmumam, kas balstīts tikai uz automatizētu apstrādi, tostarp profilēšanu un kas rada juridiskas sekas attiecībā uz viņu vai līdzīgi būtiski ietekmē viņu, ja vien šāds lēmums nav:
  - 9.1.1. ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu subjektu un iesaistīto uzņēmumu;
  - 9.1.2. to pieprasa vai atļauj piemērojamie tiesību akti, kas arī nosaka piemērotus pasākumus, lai aizsargātu datu subjekta tiesības un brīvības, un likumīgās intereses (tostarp vismaz tiesības uz iesaistītā uzņēmuma cilvēka iesaistīšanos, lai paustu savu viedokli un apstrīdēt lēmumu); vai
  - 9.1.3. ir balstīta uz datu subjekta nepārprotamu piekrišanu.

## 10. Drošība un konfidencialitāte



- 10.1. Amgen īsteno atbilstošus tehniskos un organizatoriskos drošības pasākumus, lai aizsargātu pret personas datu pārkāpumiem un atklātu tos. Lai noteiktu šos drošības pasākumus, Amgen izmanto starptautiskās sistēmas, piemēram, ISO/IEC 27002.
- 10.2. Amgen ir ieviesti procesi, lai nodrošinātu, ka personas datu aizsardzības pārkāpumi tiek ziņoti, izsekoti un pēc vajadzības tiek veikti atbilstoši korigējošie pasākumi. Jebkurš personas datu aizsardzības pārkāpums ir jādokumentē (tostarp ar personas datu aizsardzības pārkāpumu saistītie fakti, tā sekas un veiktās korektīvās darbības), un dokumentācija pēc pieprasījuma ir pieejama kompetentajai DAI. Iesaistītie uzņēmumi bez nepamatotas kavēšanās paziņo par visiem personas datu pārkāpumiem Amgen France, galvenajam privātuma inspektoram un citai attiecīgajai privātuma amatpersonai/funkcijai un (ja iesaistītais uzņēmums, kas cieš no personas datu pārkāpuma, darbojas kā datu apstrādātājs) iesaistītajam uzņēmumam, kas rīkojas kā datu pārzinis. Par personas datu aizsardzības pārkāpumiem sadarbībā ar galveno privātuma amatpersonu bez liekas kavēšanās (un, ja iespējams, ne vēlāk kā 72 stundas pēc personas datu aizsardzības pārkāpuma uzzināšanas) paziņo kompetentajai datu aizsardzības iestādei, ja vien maz ticams, ka tas varētu radīt risku datu subjektu tiesībām un brīvībai. Ja personas datu aizsardzības pārkāpums var radīt lielu risku datu subjektu tiesībām un brīvībām, par to bez liekas kavēšanās arī jāpaziņo datu subjektiem.
- 10.3. Informācijas drošības riska novērtējumi tiek izmantoti, lai identificētu iespējamus draudus jūtīgiem personas datiem un vajadzības gadījumā ieviestu papildu drošības kontroles.
- 10.4. Īstenojot pasākumus, tiks ņemts vērā jaunākie sasniegumi saskaņā ar GDPR 32. pantu.
- 10.5. Galvenais informācijas drošības speciālists strādā kopā ar galveno privātuma inspektoru, lai nodrošinātu personas datu drošību un konfidencialitāti.
- 10.6. Tehniskie un organizatoriskie drošības pasākumi ir izstrādāti, lai īstenotu datu aizsardzības principus saskaņā ar VDAR 5. pantu, integrētās datu aizsardzības un noklusējuma principus saskaņā ar VDAR 25. pantu un veicinātu šo ES BCR noteikto prasību ievērošanu praksē.

## **11. Attiecības ar datu apstrādātājiem (Amgen datu importētāju vai piegādātāju)**

- 11.1. Iesaistītais uzņēmums (kas darbojas kā datu pārzinis) rūpīgi izvēlēsies datu apstrādātāju, kas var būt vai nu cits iesaistītais uzņēmums, vai pārdevējs. Datu apstrādātājam ir jāsniedz pietiekamas garantijas par saviem tehniskajiem un organizatoriskajiem drošības pasākumiem, kas regulē veicamo apstrādi, un jānodrošina šo pasākumu ievērošana.
- 11.2. Ja ārpakalpojums tiek uzskatīts par nepieciešamu pēc šāda ārpakalpojuma biznesa vajadzību un risku izvērtēšanas, datu apstrādātāja izvēles procesā tiks izvērtēti privātuma riska faktori un līdzsvarotas biznesa vajadzības un iespējamie riski.
- 11.3. Iesaistītais uzņēmums, kas darbojas kā datu pārzinis, izmantojot rakstiskus līgumiskus līdzekļus, saskaņā ar piemērojamiem tiesību aktiem (un jo īpaši VDAR 28. panta 3. punkta prasībām) cita starpā dos norādījumus datu apstrādātājam:
  - 11.3.1. datu apstrādātājam jārīkojas vadoties tikai pēc iesaistītā uzņēmuma, kā datu pārzinā, instrukcijām un ir aizliegta personas datu apstrāde paša datu apstrādātāja vai trešās puses vajadzībām;

- 11.3.2. par noteikumiem, kas attiecas uz datu apstrādātāja drošību un konfidencialitāti, un īstenot atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu apstrādes riskam atbilstošu drošības līmeni ;
- 11.3.3. personas, kas ir pilnvarotas apstrādāt personas datus, ir apņēmušās ievērot konfidencialitāti vai uz tām attiecas atbilstošs likumā noteikts konfidencialitātes pienākums;
- 11.3.4. datu apstrādātājs nepiesaista citu datu apstrādātāju bez iepriekšējas īpašas vai vispārīgas rakstiskas atļaujas no iesaistītā uzņēmuma, kas darbojas kā datu pārzinis, un, ja šāda atļauja ir dota, tādas pašas datu aizsardzības saistības, kas noteiktas līgumā vai citā tiesību aktā starp iesaistīto uzņēmumu, kas darbojas kā datu pārzinis, un datu apstrādātāju tiek uzliktas šim citam datu apstrādātājam;
- 11.3.5. ņemot vērā apstrādes raksturu, tai ar atbilstošiem tehniskiem un organizatoriskiem pasākumiem, ciktāl tas ir iespējams, jāpalīdz iesaistītajam uzņēmumam, kas darbojas kā datu pārzinis, izpildīt iesaistītā uzņēmuma pienākumu atbildēt uz datu subjekta tiesību īstenošanas pieprasījumiem ;
- 11.3.6. tai jāpalīdz iesaistītajam uzņēmumam, kas darbojas kā datu pārzinis, nodrošināt atbilstību saistībām, kas saistītas ar apstrādes drošību, paziņošanu par personas datu pārkāpumu kompetentajai datu aizsardzības iestādei, personas datu aizsardzības pārkāpuma paziņošanu datu subjektam, datu aizsardzības ietekmes novērtējumus un iepriekšēju konsultāciju ar kompetento DAJ, ņemot vērā apstrādes būtību un datu apstrādātājam pieejamo informāciju;
- 11.3.7. pēc iesaistītā uzņēmuma, kas darbojas kā datu pārzinis, izvēles tai ir jādzēš vai jāatdod visi personas dati iesaistītajam uzņēmumam, kas darbojas kā datu pārzinis pēc pakalpojumu sniegšanas, kas saistīti ar apstrādi, un jādzēš esošās kopijas, ja vien ES datu aizsardzības likums nenosaka personas datu glabāšanu;
- 11.3.8. tai ir jādara pieejama iesaistītajam uzņēmumam, kas darbojas kā datu pārzinis, visa informācija, kas nepieciešama, lai pierādītu atbilstību šajā 11. pantā noteiktajiem pienākumiem, un jāļauj veikt revīzijas, tostarp pārbaudes, ko veic iesaistītais uzņēmums, kas darbojas kā datu pārzinis, vai cits tā pilnvarots auditors.
- 11.4. Iesaistītais uzņēmums, kas darbojas kā datu pārzinis, nodrošina, lai datu apstrādātājs pilnībā ievērotu saskaņotos tehniskos un organizatoriskos drošības pasākumus.
- 11.5. Iesaistītais uzņēmums, kas darbojas kā datu pārzinis, saglabā atbildību par apstrādes likumību un joprojām ir atbildīga par datu subjekta tiesībām. Ciktāl datu apstrādātājs ir pakļauts ES datu aizsardzības likumiem, tas ir atbildīgs arī par saviem pienākumiem un atbildību kā datu apstrādātājs saskaņā ar šādiem tiesību aktiem.
- 11.6. Lai nodrošinātu šajā pantā par datu apstrādātājiem noteiktās līgumsaistības, iesaistītajiem uzņēmumiem, kas darbojas kā datu pārzinis, tiek nodrošināta līguma veidne ar nosaukumu datu privātuma grafiks . Iesaistītais uzņēmums, kas darbojas kā datu pārzinis, atkarībā no katras līgumiskās vienošanās konkrētajiem apstākļiem var vienoties par noteikumiem, kas atšķiras no tiem, kas noteikti datu konfidencialitātes grafikā, taču līguma noteikumiem joprojām ir jāietver vismaz saistības, kas noteiktas iepriekš šo 11. pantu.

- 11.7. Katram iesaistītajam uzņēmumam, kas darbojas kā datu apstrādātājs un uz kuru attiecas ES datu aizsardzības tiesību akti, ir jāuztur visu kategoriju apstrādes darbību uzskaitē, kuras veiktas iesaistītā uzņēmuma vārdā, kas darbojas kā datu pārzinis. Šis ieraksts ir jā saglabā rakstiski, tostarp elektroniskā veidā, pēc pieprasījuma ir jādara pieejams galvenajam privātuma inspektoram un kompetentajai datu aizsardzības iestādei, un tajā jāiekļauj šāda informācija: (a) iesaistītā uzņēmuma nosaukums un kontaktinformācija, kas rīkojas kā datu apstrādātājs un katra iesaistītā uzņēmuma, kas darbojas kā datu pārzinis un kura vārdā tas rīkojas, un attiecīgā gadījumā tā pārstāvis un DAI; (b) apstrādes kategorijas, kas veiktas katras iesaistītās sabiedrības vārdā, kas darbojas kā datu pārzinis; un c) attiecīgā gadījumā personas datu nosūtīšana uz trešo valsti vai starptautisku organizāciju, tostarp šīs trešās valsts vai starptautiskās organizācijas identifikācija, un, ja pārsūtīšana ir balstīta uz 49. pantā paredzēto atkāpi, ja VDAR, dokumenti, par piemērotiem drošības pasākumiem; un d) ja iespējams, vispārīgu tehnisko un organizatorisko drošības pasākumu aprakstu.

## **12. Ierobežojumi pārsūtīšanai un tālākai pārsūtīšanai**

- 12.1. Visai personas datu pārsūtīšanai, uz kurām attiecas šie ES BCR, trešām personām, kas atrodas ārpus EEZ, jāievēro ES datu aizsardzības tiesību akti par personas datu pārsūtīšanu un tālāku pārsūtīšanu, vai nu izmantojot standarta līguma klauzulas, kas atļautas saskaņā ar komisijas īstenošanas lēmumu (ES) (2021. gada 4. jūnijs) par līguma standartklauzulām personas datu pārsūtīšanai uz trešām valstīm saskaņā ar VDAR vai ar citiem atbilstošiem līdzekļiem saskaņā ar VDAR V nodaļu (tostarp izņēmuma kārtā, ja izņēmums attiecas uz konkrētu situāciju saskaņā ar VDAR 49).
- 12.2. Visiem personas datu, uz kuriem attiecas šie ES BCR, pārsūtīšanas datu apstrādātājiem, kas atrodas ārpus EEZ, jāievēro ES datu aizsardzības likumi, kas attiecas uz datu apstrādātājiem (un 11. pantā noteiktās prasības) papildus noteikumiem par pārsūtīšanu un tālāku personas datu pārsūtīšanu, kā noteikts 12. pantā un ES datu aizsardzības likumos.
- 12.3. Pirms personas datu nosūtīšanas datu importētājam vai (attiecībā uz notiekošo pārsūtīšanu) pirms jebkādu atjauninātu vietējo valsts tiesību aktu stāšanās spēkā datu eksportētājs sadarbībā ar galveno privātuma amatpersonu un Amgen France ar datu importētāja palīdzību un ņemot vērā pārsūtīšanas apstākļus, izvērtē, vai vietējie valsts tiesību akti neļaus datu importētājam izpildīt savus pienākumus saskaņā ar ES BCR, un nosaka, vai ir jāīsteno kādi nepieciešamie papildu pasākumi. Šādā novērtējumā ņems vērā:
- 12.3.1. ģpašie nosūtīšanas apstākļi (tostarp nolūki, kādos personas dati tiek pārsūtīti un apstrādāti, apstrādē iesaistīto vienību veidi, ekonomikas nozare, kurā notiek pārsūtīšana, pārsūtīto personas datu kategorijas un formāts, atrašanās vieta par apstrādi (ieskaitot uzglabāšanu) un izmantotajiem pārraides kanāliem);
- 12.3.2. galamērķa trešās valsts tiesību akti un prakse, kas ir būtiski, ņemot vērā konkrētos nosūtīšanas apstākļus (tostarp tos, kas paredz datu izpaušanu valsts iestādēm vai atļauju šādām iestādēm piekļūt) un piemērojamos ierobežojumus un aizsardzības pasākumus; un
- 12.3.3. jebkādus attiecīgus lģgumiskus, tehniskus vai organizatoriskus aizsardzības pasākumus, kas ieviesti attiecībā uz pārsūtīšanu, tostarp pasākumus, kas piemēroti personas datu nosūtīšanas laikā un personas datu apstrādei galamērķa valstī.

Turklāt šāda novērtējuma pamatā ir izpratne, ka galamērķa trešās valsts tiesību akti un prakse respektē datu subjekta pamattiesības un brīvības un nepārsniedz to, kas ir

nepieciešams un samērīgs demokrātiskā sabiedrībā, lai nodrošinātu kādu no šiem mērķiem. :

- a) valsts drošību; b) aizsardzību; c) sabiedrisko drošību; d) noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu; e) citus svarīgus vispārējo sabiedrības interešu mērķus, jo īpaši svarīgas ekonomiskās vai finanšu intereses, tostarp monetāros, budžeta un nodokļu jautājumus, sabiedrības veselību un sociālo drošību; f) tiesu neatkarības un tiesvedības aizsardzību; g) reglamentēto profesiju ētikas pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem; h) uzraudzības, pārbaudes vai regulēšanas funkcijas, kas saistītas ar valsts varas īstenošanu iepriekšējos mērķos minētajos gadījumos; ( i ) datu subjekta vai citu personu tiesību un brīvību aizsardzība; un/vai j) civiltiesisku prasību izpildi.

Privātuma galvenais speciālists pārskata un apstiprina dokumentēto novērtējumu un visus ierosinātos papildu pasākumus. Ja novērtējuma rezultāti liecina par nepieciešamību īstenot papildu pasākumus, datu eksportētājs īsteno šos pasākumus. Ja nekādus papildu pasākumus nevar ieviest (vai ja to ir norādījis galvenais privātuma speciālists vai kompetentā datu aizsardzības iestāde), datu eksportētājs aptur pārsūtīšanu. Novērtējuma rezultātus un ierosinātos papildu pasākumus reģistrē un vajadzības gadījumā iesniedz kompetentajai datu aizsardzības iestādei.

Privātuma galvenais speciālists un Amgen France informēs visus iesaistītos uzņēmumus par veikto novērtējumu un tā rezultātiem, lai varētu piemērot identificētos papildu pasākumus, ja tāda paša veida pārsūtīšanu veic citi iesaistītie uzņēmumi vai ja nevar veikt efektīvus papildu pasākumus. Šāda pārsūtīšana tiek apturēta vai izbeigta.

- 12.4. Datu importētājs nekavējoties informē datu eksportētāju, Amgen France un galveno privātuma amatpersonu, ja tam ir iemesls uzskatīt, ka uz to attiecas vai ir kļuvuši tiesību akti vai prakse, kas liegtu tam izpildīt savus pienākumus saskaņā ar šiem ES BCR, tostarp pēc izmaiņas vietējās valsts tiesību aktos trešā valstī, kā aprakstīts 12. panta 3. punktā, vai pasākums, piemēram, informācijas izpaušanas pieprasījums, kā aprakstīts 16. panta 3. punktā. Turklāt datu eksportētāji (saskaņā ar galveno privātuma amatpersonu) pastāvīgi un attiecīgā gadījumā ar datu importētāju palīdzību uzrauga notikumus trešajās valstīs, kurām datu eksportētāji ir nosūtījuši personas datus, kas varētu negatīvi ietekmēt personas datu aizsardzības līmeņa sākotnējo novērtējumu un lēmumus, kas pieņemti attiecībā uz šādu pārsūtīšanu.
- 12.5. Pēc pārsūtīšanas apturēšanas datu eksportētājam ir jāpārtrauc pārsūtīšana vai pārsūtīšanas kopums, ja datu importētājs nespēj ievērot ES BCR un/vai atbilstība netiek atjaunota viena mēneša laikā pēc apturēšanas. Šādā gadījumā datu importētājam pēc datu eksportētāja izvēles ir jāatdod vai jāiznīcina visi personas dati, kas ir pārsūtīti pirms apturēšanas, un to kopijas.
- 12.6. Jebkuras personas datu plūsmas, uz kurām neattiecas šie ES BCR un/vai kuras nav no iesaistītā uzņēmuma, kas reģistrēts EEZ dalībvalstī, netiek uzskatītas par personas datu pārsūtīšanu saskaņā ar šiem ES BCR, un attiecīgi uz tām neattiecas šo ES BCR prasības.

### **13. Apmācību programma**

- 13.1. Kā aprakstīts 2. pielikumā, Amgen nodrošina atbilstošas un atjauninātas apmācības par privātuma principiem un konkrētāk par ES BCR visam personālam. Šajā apmācībā ir iekļauta arī informācija par sekām saskaņā ar krimināltiesībām un darba tiesībām un/vai viņu pakalpojumu līgumiem darbiniekiem, kuri pārkāpj ES BCR.

- 13.2. Apmācība ir obligāta un tiek atkārtota katru gadu. Veiksmīga dalība apmācībās tiks dokumentēta.
- 13.3. Personālam, kuram ir pastāvīga vai regulāra piekļuve personas datiem vai kuri ir iesaistīti personas datu vākšanā vai personas datu apstrādei izmantojamo rīku izstrādē, katrā atsevišķā gadījumā tiks nodrošinātas īpašas apmācības .
- 13.4. Turklāt Amgen globālās privātuma atbilstības komanda nodrošina atbilstošu informāciju un resursus saistībā ar privātumu, tostarp Amgen iekštīkla portālā.

#### **14. Audita un uzraudzības programma**

- 14.1. Privātuma galvenais speciālists nodrošina, ka visi iesaistītie uzņēmumi (un to atbilstība šiem ES BCR) tiek iekļauti audita un uzraudzības programmā no privātuma un datu aizsardzības viedokļa. Visaptverošas revīzijas tiek veiktas regulāri, ne retāk kā reizi 2 līdz 3 gados (iesaistītajiem uzņēmumiem ar vidēju vai augstu riska profilu, pamatojoties uz audita departamenta riska novērtēšanas metodoloģiju) un ik pēc 4 līdz 5 gadiem (iesaistītajiem uzņēmumiem ar zema riska profilu, pamatojoties uz revīzijas departamenta riska novērtēšanas metodoloģiju) , iekšējā audita grupa vai neatkarīgi, ārēji sertificēti auditori. Visaptverošas revīzijas ietver datu aizsardzības un privātuma jautājumus to darbības jomā (tostarp atbilstību šiem ES BCR, ja tas attiecas uz iesaistīto uzņēmumu un tos izmanto). Papildus visaptverošām revīzijām un neskarot iepriekš noteiktos termiņus, tiek veiktas arī citas revīzijas jomas, tostarp starpfunkcionālas vai specifiskas problēmas (piemēram, atbilstība ES BCR), ierobežota viena vai vairāku personu revīzija. Datu apstrādes sistēmas un/vai viena vai vairāku funkcionālu nodaļu (piemēram, globālās privātuma atbilstības komandas) ierobežots audits. Revīzijas programma tiek izstrādāta un saskaņota sadarbībā ar revīzijas vadītāju un galvenā atbilstības amatpersona, kas ir vecākais viceprezidents. Galvenais privātuma speciālists, galvenais atbilstības speciālists un galvenais informācijas speciālists jebkurā laikā var uzsākt ar ES BCR saistītas ad hoc revīzijas. Piemēram, reaģējot uz jebkuru identificētu atbilstības problēmu vai ziņojumu par būtisku neatbilstību , personas datu pārkāpumu un/vai būtiskām izmaiņām ES datu aizsardzības likumos. Revīzijas programma aptver visus ES BCR aspektus, tostarp metodes, kas nodrošina korektīvo darbību veikšanu .
- 14.2. Visi ES BCR revīzijas ziņojumi tiek savlaicīgi paziņoti galvenajam atbilstības speciālistam un galvenajam privātuma inspektoram. ES BCR revīzijas kopsavilkumi un konstatējumi, kā arī cita būtiska informācija tiek regulāri ziņota Amgen Inc. direktoru padomei, izmantojot atbilstošas komitejas (piemēram, korporatīvās atbildības un atbilstības komiteju un/vai valdes revīzijas komiteju), lai Amgen France direktoru padomei un (attiecīgā gadījumā, piemēram, saistībā ar konstatējumu, kas prasa aizsardzību) attiecīgajai iesaistītajai sabiedrībai. Amgen, Inc. direktoru padomes Korporatīvās atbildības un atbilstības komiteja tiekas piecas reizes gadā . Privātums un datu aizsardzība tiek apskatīta katru gadu, parasti oktobra sanāksmē.
- 14.3. Kompetentā DAI pēc pieprasījuma var saņemt ar ES BCR saistīto revīzijas ziņojumu kopijas.
- 14.4. Katra iesaistītā sabiedrība sadarbojas ar kompetento DAI un bez ierobežojumiem piekrīt tam, ka tā tiek pārbaudīta. Katrai revidējamai struktūrai nekavējoties jāinformē galvenais privātuma speciālists, ja tā saņem paziņojumu par šādu revīziju vai šāda revīzija tiek veikta.

#### **15. Atbilstība un atbilstības uzraudzība**

- 15.1. Amgen ieceļ atbilstošu personālu, tostarp attiecīgā gadījumā datu aizsardzības inspektoru tīklu ar augstākās vadības atbalstu, lai pārraudzītu un nodrošinātu datu aizsardzības noteikumu ievērošanu. Privātuma galvenais speciālists ir atbildīgs par globālo privātuma atbilstības komandu, kas ir globāla komanda, kas sniedz ekspertu atbalstu visā pasaulē Amgen uzņēmumiem (tostarp iesaistītajiem uzņēmumiem).
- 15.2. Amgen galvenā privātuma amatpersonas pienākumos cita starpā ietilpst:
  - 15.2.1. valdes konsultēšana ;
  - 15.2.2. nodrošināt atbilstību datu aizsardzībai globālā līmenī (tostarp uzņemoties vispārēju atbildību par ES BCR );
  - 15.2.3. regulāri ziņot par atbilstību datu aizsardzībai (tostarp galvenajam atbilstības speciālistam); un
  - 15.2.4. strādājot ar kompetentās DAI izmeklēšanām.
- 15.3. Globālajā privātuma atbilstības komandā ir galvenais privātuma inspektors (kurš papildus iepriekš minētajiem pienākumiem pārrauga globālo datu aizsardzības inspektoru tīklu), Eiropas datu aizsardzības inspektors un citi vietējie datu aizsardzības inspektori. Globālā privātuma atbilstības komanda ir vispārēja atbildība par datu aizsardzību un privātuma ievērošanu visā pasaulē Amgen.
- 15.4. Amgen ir iecēlusi Eiropas datu aizsardzības inspektoru par datu aizsardzības inspektoru EEZ, Apvienotajā Karalistē un Šveicē. Eiropas datu aizsardzības inspektoram ir GDPR 39. pantā noteiktie uzdevumi. Amgen nodrošinās, lai Eiropas datu aizsardzības inspektora uzdevumi un pienākumi neradītu interešu konfliktu ar šiem uzdevumiem. Eiropas datu aizsardzības inspektoram ir tieša atskaitīšanās līnija galvenajam privātuma inspektoram (kas ir daļa no Amgen augstākā vadības līmeņa), un viņu atbalsta vietējā atbilstības vadošā iestāde Francijā. Eiropas datu aizsardzības inspektors var sazināties ar galveno privātuma inspektoru, ja viņa pienākumu izpildes laikā rodas jautājumi vai problēmas. Ar Eiropas datu aizsardzības inspektoru var sazināties: [privacy@amgen.com](mailto:privacy@amgen.com)
- 15.5. Vietējā līmenī datu aizsardzības inspektori ir atbildīgi par datu subjektu vietējo privātuma pieprasījumu apstrādi, par atbilstības nodrošināšanu vietējā līmenī ar Globālās privātuma atbilstības komandas atbalstu un par svarīgāko privātuma problēmu ziņošanu galvenajam privātuma speciālistam. Amgen uztur datu aizsardzības inspektoru tīklu un nodrošina, ka DAI tiek iecelts vai nozīmēts katrā valstī, kurā Amgen ir korporatīvā vienība (iesaistītā sabiedrība), un šādas iesaistītās sabiedrības jurisdikcijas piemērojamie tiesību akti pieprasa šādu iecelšanu.
- 15.6. Parasti datu aizsardzības inspektori ir vai arī viņus atbalsta vietējie atbilstības vadītāji, kas ziņo vispasaules atbilstības un biznesa ētikas departamentam. Globālā privātuma atbilstības komanda ir daļa no vispasaules atbilstības un biznesa ētikas departamenta, ko vada atbilstības vadītājs, un ziņo tai. Galvenais atbilstības speciālists ir vispāratzīts par Amgen grupas juridisko un normatīvo aktu atbilstību visā pasaulē. Retos gadījumos iesaistītā uzņēmuma īpašo apstākļu vai citu īpašu apstākļu dēļ datu aizsardzības inspektors var būt no citas funkcijas, piemēram, reglamentējošās. Jebkurā gadījumā globālā privātuma atbilstības komanda nodrošina, ka datu aizsardzības darbinieki un atbilstības vadītāji ir atbilstoši apmācīti un viņiem ir pietiekams vadības un zināšanu līmenis, lai veiktu savu pienākumu. Turklāt datu aizsardzības inspektoriem ir tieša ziņošanas līnija galvenajam privātuma

inspektoram, un viņus atbalsta globālās privātuma atbilstības komandas darbinieki, ja viņiem ir nepieciešami papildu norādījumi.

15.7. Katrs iesaistītais uzņēmums, kas darbojas kā datu pārzinis, ir atbildīgs par atbilstību ES BCR un spēj pierādīt to atbilstību. Šīs prasības ietvaros visiem iesaistītiem uzņēmumiem:

15.7.1. jāsaglabā visu kategoriju apstrādes darbību uzskaitē, kas veikta saskaņā ar VDAR 30. panta 1. punktā noteiktajām prasībām. Šis ieraksts ir jāsaglabā rakstiski, tostarp elektroniskā veidā, pēc pieprasījuma ir jādara pieejams galvenajam privātuma inspektoram un kompetentajai datu aizsardzības iestādei, un tajā jāiekļauj šāda informācija: (a) iesaistītā uzņēmuma nosaukums un kontaktinformācija, kas rīkojas kā datu pārzinis, tā pārstāvis un DAI; (b) apstrādes mērķi; (c) datu subjektu kategoriju un personas datu kategoriju apraksts; (d) to saņēmēju kategorijas, kuriem personas dati ir izpausti vai tiks izpausti, tostarp saņēmēji trešās valstīs vai starptautiskās organizācijās; (e) attiecīgā gadījumā personas datu nosūtīšana uz trešo valsti vai starptautisku organizāciju, tostarp šīs trešās valsts vai starptautiskās organizācijas identifikācija un, ja pārsūtīšana ir balstīta uz atkāpi, dokumentācija par piemērotiem aizsardzības pasākumiem; (f) ja iespējams, dažādu kategoriju personas datu dzēšanas paredzētie termiņi; un (g) ja iespējams, vispārīgu tehnisko un organizatorisko drošības pasākumu apraksts.

15.7.2. saskaņā ar VDAR 35. pantu veikt datu aizsardzības ietekmes novērtējumus attiecībā uz apstrādes darbībām, kuras var radīt augstu risku fizisko personu tiesībām un brīvībām. Ja ietekmes uz datu aizsardzību novērtējums saskaņā ar 35. pantu norāda, ka apstrāde radītu augstu risku, ja iesaistītā sabiedrība neveiks pasākumus riska mazināšanai, pirms apstrādes ir jākonsultējas ar galveno privātuma amatpersonu, kas pēc tam apspriežas ar kompetento datu aizsardzības iestādi saskaņā ar VDAR 36. pantu.

## **16. Darbības, ja valsts tiesību akti novērš ES BCR ievērošanu**

16.1. Ja iesaistītajai sabiedrībai ir iemesls uzskatīt, ka tai piemērojamie tiesību akti neļauj iesaistītajai sabiedrībai pildīt savas saistības saskaņā ar ES BCR vai būtiski ietekmē noteikumus paredzētās garantijas, tā nekavējoties informēs privātuma aizsardzības vadītāju (izņemot gadījumus, kad aizliedz tiesībaizsardzības iestāde, piemēram, krimināllikumā noteikts aizliegums saglabāt tiesībaizsardzības izmeklēšanas konfidencialitāti) un Amgen France.

16.2. Ja pastāv pretrunas starp vietējiem valsts tiesību aktiem un ES BCR saistībām, galvenais privātuma speciālists sadarbībā ar vietējo juridisko konsultantu un vietējo datu aizsardzības inspektoru noteiks, kāda juridiski piemērota darbība ir nepieciešama. Ja nepieciešams, galvenais privātuma speciālists konsultēsies arī ar kompetento DAI.

16.3. Ja kāda juridiska prasība, kas ir pakļauta iesaistītajam uzņēmumam trešā valstī, var būtiski negatīvi ietekmēt ES BCR sniegtās garantijas, datu importētājs nekavējoties informē Amgen France galveno privātuma amatpersonu un datu eksportētāju. Importētājs un galvenais privātuma speciālists informē kompetento DAI un (ja iespējams) datu subjektus. Tas ietver (a) jebkuru juridiski saistošu pieprasījumu par personas datu izpaušanu, ko veic tiesībaizsardzības iestāde vai valsts drošības iestāde, un šādā gadījumā kompetentajai datu aizsardzības iestādei jābūt skaidri informētai par pieprasījumu, tostarp informāciju par pieprasītajiem datiem, pieprasījuma iesniedzēja iestāde, juridiskais pamats izpaušanai un sniegtajai atbildei (ja vien nav aizliegts citādi, piemēram, krimināllikumā noteikts aizliegums saglabāt tiesībaizsardzības izmeklēšanas konfidencialitāti), un (b) jebkāda valsts iestāžu tieša

piekļuve personas datiem, pārsūtītāmiem saskaņā ar šiem ES BCR un saskaņā ar galamērķa valsts tiesību aktiem, un šādā gadījumā šādā paziņojumā iekļauj visu informāciju, kas ir pieejama šādai iesaistītajai sabiedrībai (ja vien nav aizliegts citādi, piemēram, krimināllikumā noteikts aizliegums saglabāt informācijas konfidencialitāti). tiesībaizsardzības izmeklēšana).

- 16.4. Ja konkrētos gadījumos apturēšana un/vai paziņošana ir aizliegta, iesaistītā sabiedrība, kas saņem pieprasījumu, pieliks visas pūles, lai iegūtu tiesības atteikties no šī aizlieguma, lai sniegtu pēc iespējas vairāk informācijas, cik ātri vien iespējams, lai pierādītu (pēc datu eksportētāja pieprasījuma), ka tā ir rīkojusies.
- 16.5. Datu importētājs regulāri sniegs datu eksportētājam pēc iespējas vairāk būtisku informāciju par saņemtajiem pieprasījumiem (jo īpaši pieprasījumu skaitu, pieprasīto personas datu veidu, pieprasījuma iesniedzēju iestāžu identitāti, vai pieprasījumi ir apstrīdēti un šo apstrīdējumu iznākumus). Datu importētājs saglabās šo informāciju tik ilgi, kamēr uz personas datiem attiecas ES BCR paredzētie drošības pasākumi, un pēc pieprasījuma darīs to pieejamu kompetentajai DAI. Ja datu importētājam ir vai tiek daļēji vai pilnībā aizliegts sniegt datu eksportētājam iepriekš minēto informāciju, datu importētājs bez liekas kavēšanās attiecīgi informēs datu eksportētāju.
- 16.6. Datu importētājs sadarbībā ar galveno privātuma amatpersonu pārbaudīs valsts iestādes informācijas izpaušanas pieprasījuma likumību, lai noteiktu, vai tas ietilpst pieprasījuma iesniedzējai valsts iestādei piešķirtajās pilnvarās. Datu importētājs apstrīdēs pieprasījumu, ja pēc šāda novērtējuma tas secinās (saskaņā ar galveno privātuma amatpersonu), ka ir pamatots iemesls uzskatīt, ka pieprasījums ir nelikumīgs saskaņā ar galamērķa valsts tiesību aktiem, piemērojamiem pienākumiem saskaņā ar starptautiskajām tiesībām, un /vai starptautiskās pieklājības principiem. Ja datu importētājs uzskata, ka ir pamatots iemesls uzskatīt pieprasījumu par nelikumīgu, tas izmantos pārsūdzības iespējas. Apstrīdot pieprasījumu, datu importētājs izmantos pagaidu pasākumus, lai apturētu pieprasījuma ietekmi, līdz kompetentā tiesu iestāde būs pieņēmusi lēmumu par tā būtību. Datu importētājs neizpauž pieprasītos personas datus, kamēr tas nav jādara saskaņā ar galamērķa valsts piemērojamiem tiesību aktiem un procesuālajiem noteikumiem. Datu importētājs dokumentēs savu juridisko novērtējumu un jebkādas apstrīdēšanas prasības attiecībā uz izpaušanas pieprasījumu un, ciktāl to pieļauj galamērķa valsts tiesību akti, darīs dokumentāciju pieejamu datu eksportētājam un pēc pieprasījuma kompetentajai datu aizsardzības iestādei.
- 16.7. Datu importētājs, atbildot uz informācijas izpaušanas pieprasījumu, sniegs minimālo pieļaujamo informācijas apjomu, pamatojoties uz pieprasījuma saprātīgu interpretāciju.
- 16.8. Jebkurā gadījumā personas datu nosūtīšana, ko veic iesaistītā sabiedrība nevienai valsts iestādei, nedrīkst būt masveida, nesamērīga un nediskriminējoša veidā, kas pārsniegtu to, kas ir nepieciešams demokrātiskā sabiedrībā.
- 16.9. Iesaistītajiem uzņēmumiem, kas atrodas EEZ, jebkurš tiesas vai tribunāla spriedums un jebkurš trešās valsts administratīvās iestādes lēmums, ar kuru datu pārzinim vai datu apstrādātājam ir jāpārsūta vai jāizpauž personas dati, var tikt atzīti vai jebkādā veidā izpildāmi tikai tad, ja tie ir pamatoti uz starptautisku nolīgumu, piemēram, savstarpējās tiesiskās palīdzības līgumu, kas ir spēkā starp pieprasījuma iesniedzēju trešo valsti un ES vai EEZ dalībvalsti, neskarot citus pārsūtīšanas pamatojumus saskaņā ar GDPR V nodaļu.

## 17. Iekšējie sūdzību mehānismi



- 17.1. Amgen izmantos esošo sūdzību izskatīšanas procesu, lai iekļautu jebkuru ar ES BCR saistītu sūdzību vai bažu izskatīšanu.
- 17.2. Jebkurš datu subjekts jebkurā laikā var sūdzēties par to, ka kāds iesaistītais uzņēmums neievēro ES BCR. Šādas sūdzības izskatīs globālā privātuma atbilstības komanda galvenā privātuma amatpersonas vadībā un sadarbībā ar attiecīgo vietējo datu aizsardzības inspektoru.
- 17.3. Amgen iesaka šādas sūdzības iesniegt rakstiski vai nu pa pastu, vai e-pastu tieši globālās privātuma atbilstības komandai vai iesaistītajam uzņēmumam. Ar globālās privātuma atbilstības komandu var sazināties, izmantojot tālāk norādīto kontaktinformāciju.  
  
Adrese : 25 quai du Président Paul Doumer, 92400 Courbevoie .  
  
E-pasts : [privacy@amgen.com](mailto:privacy@amgen.com)
- 17.4. Amgen personāls var izmantot Business Conduct Hotline, lai ziņotu par ES BCR sūdzību, ja tas ir pieņemams saskaņā ar likumiem, kas piemērojami iesaistītajam uzņēmumam.
- 17.5. Ja iesaistītais uzņēmums sūdzību saņem vietējā līmenī, DAI vajadzības gadījumā iztulkos un bez liekas kavēšanās pārsūtīs to globālajai privātuma atbilstības komandai.
- 17.6. Sākotnējā atbilde datu subjektam tiks sniegta desmit (10) darba dienu laikā, informējot viņu par to, ka viņa sūdzība tiek izskatīta un ka viņš vai viņa saņems atbildi pēc būtības bez nepamatotas kavēšanās un jebkurā gadījumā viena mēneša laikā pēc pieprasījuma saņemšanas. Ņemot vērā pieprasījumu sarežģītību un skaitu, viena mēneša termiņu var pagarināt ne vairāk kā par diviem mēnešiem, tādā gadījumā par to attiecīgi informējot datu subjektu. Būtiskā atbilde ietvers detalizētu informāciju par mūsu konstatējumiem un jebkuru darbību, ko Amgen ir paredzējusi vai ierosina veikt. Ja Amgen konstatē, ka nekādas darbības nav jāveic, tas ir jāpaskaidro datu subjektam kopā ar šāda lēmuma iemesliem.
- 17.7. Ja Amgen apmierinās sūdzību, Amgen veiks atbilstošus korektīvos pasākumus. Par šiem pasākumiem katrā atsevišķā gadījumā lems galvenais privātuma speciālists un globālā privātuma atbilstības komanda, vietējais DAI un attiecīgā gadījumā jebkura cita attiecīgā nodaļa. Turklāt, ja globālā privātuma atbilstības komanda atklās individuālu pārkāpumu, tiks veikti atbilstoši disciplinārie pasākumi, līdz pat darba attiecību pārtraukšanai vai darba attiecību pārtraukšanai, ciktāl to pieļauj piemērojamie tiesību akti.
- 17.8. Datu subjekts saņems atbildi, informējot viņu par sūdzības iznākumu. To veic bez liekas kavēšanās un jebkurā gadījumā viena mēneša laikā pēc sūdzības saņemšanas (ar pietiekamu informāciju, lai Amgen varētu identificēt sūdzības būtību, un tikai tad, ja tas ir pamatoti nepieciešams, ar jebkādu informāciju, kas pieprasīta, lai apstiprinātu sūdzības iesniedzēja identitāti). Ņemot vērā pieprasījumu sarežģītību un skaitu, viena mēneša termiņu var pagarināt ne vairāk kā par diviem mēnešiem, tādā gadījumā par to attiecīgi informējot datu subjektu.
- 17.9. Datu subjekts tiks informēts, ka, ja Amgen atbilde viņu neapmierina, viņš/viņa var iesniegt prasību EEZ dalībvalsts tiesā vai kompetentajā datu aizsardzības iestādē. Tomēr datu subjektam nav obligāti jāiziet Amgen sūdzību izskatīšanas process, pirms viņš vai viņa var sūdzēties kompetentajā datu aizsardzības iestādei vai celt prasību EEZ dalībvalsts tiesā.
- 17.10. Šis sūdzību izskatīšanas process tiks publiskots, publicējot ES BCR, kā minēts iepriekš 7. pantā.

## 18. Trešo personu labuma guvēju tiesības un atbildība

- 18.1. Datu subjektam, kura personas datu izcelsme ir EEZ vai kuru personas dati ir aizsargāti ar ES datu aizsardzības likumiem un tiek nodoti iesaistītajiem uzņēmumiem ārpus EEZ, ir tiesības īstenot ES BCR kā trešās puses labuma saņēmējam, un viņam ir tiesības meklēt kompensāciju tiesā, saņemt tiesiskās aizsardzības līdzekļus un attiecīgā gadījumā kompensāciju par faktiskajiem zaudējumiem, kas nodarīti šo ES BCR pārkāpuma rezultātā. Jebkuru šādu prasību datu subjekts var iesniegt kompetentajā datu aizsardzības iestādē (kas var būt datu subjekts EEZ dalībvalstī, kurā datu subjekts pastāvīgi uzturas, vai viņa/viņas darba vietas datu aizsardzības iestāde, vai datu subjekta datu subjekts iespējamais pārkāpums). Datu subjekti var arī iesniegt prasību kompetentā tiesā EEZ dalībvalstī (kas var būt tās EEZ dalībvalsts tiesas, kurā atrodas attiecīgā iesaistītā uzņēmuma iestāde, vai tās EEZ dalībvalsts tiesas, kurā datu subjektam atrodas viņa pastāvīgā dzīvesvieta). Datu subjektu, īstenojot savas tiesības uz efektīvu tiesiskās aizsardzības līdzekli pret iesaistīto uzņēmumu, var pārstāvēt bezpeļņas organizācija, organizācija vai apvienība, ja šāda struktūra, organizācija vai apvienība ir pareizi izveidota saskaņā ar piemērojamiem tiesību aktiem, ir likumā noteikti mērķi, kas ir sabiedrības interesēs, un tā darbojas datu subjektu tiesību un brīvību aizsardzības jomā saistībā ar viņu personas datu aizsardzību. Datu subjekts kā trešās personas labuma saņēmējs var īstenot šādus pantus :
- 18.1.1. pants (Darbības joma), 2. pants (Definīcijas), 3. pants (Mērķa ierobežojums), 4. pants (Datu kvalitāte un samērīgums), 5. pants (Personas datu apstrādes juridiskais pamats) un 6. pants (Jūtīgu personas datu apstrāde );
  - 18.1.2. 7. pants (Pārredzamība un tiesības uz informāciju );
  - 18.1.3. 8. pants (Piekluves tiesības, datu labošana, dzēšana un ierobežošana) un 9. pants (Automatizēti individuāli lēmumi );
  - 18.1.4. 10. pants (Drošība un konfidencialitāte), 11. pants (Attiecības ar datu apstrādātājiem (Amgen datu importētājs vai piegādātājs) un 12. pants (Pārsūtīšanas un tālākas pārsūtīšanas ierobežojumi );
  - 18.1.5. 16. pants (Rīcības valsts tiesību aktu gadījumā, kas liedz ievērot ES BCR) un 21. pants (Saistība starp valstu tiesību aktiem un ES BCR );
  - 18.1.6. 18. pants (Trešās puses labuma saņēmēja tiesības un atbildība); un
  - 18.1.7. 19. pants (Savstarpēja palīdzība un sadarbība ar datu aizsardzības iestādēm).
- 18.2. Lai izvairītos no šaubām, trešās puses labuma saņēmēja tiesības neattiecas uz tiem ES BCR pantiem un elementiem, kas attiecas uz iekšējiem mehānismiem, kas ieviesti iesaistītajos uzņēmumos vai Amgen grupā, piemēram, informāciju par apmācību (tostarp 2. pielikumu), revīzijas programmām, iekšējiem atbilstības tīkliem un struktūrai, un ES BCR atjaunināšanas mehānismam.
- 18.3. Amgen France uzņemas atbildību un piekrīt veikt tādas darbības, kas ir pamatoti nepieciešamas, lai labotu ārpus EEZ reģistrēto iesaistīto uzņēmumu darbības. Amgen France maksā kompensāciju par jebkādiem materiāliem vai nemateriāliem zaudējumiem, kas radušies šo ES BCR pārkāpumu dēļ, ja vien tā nevar pierādīt, ka ārpus EEZ reģistrētā iesaistītā

sabiedrība nav atbildīga par notikumu, kas izraisījis kaitējumu. Amgen France ir pietiekami finanšu līdzekļi un apdrošināšanas segums, lai segtu zaudējumus saskaņā ar ES BCR.

- 18.4. Jebkurš datu subjekts, kuram ir nodarīts kaitējums, ko izraisījis šo ES BCR pārkāpums, ko veicis iesaistītais uzņēmums, kas nav reģistrēts EEZ, attiecīgā gadījumā ir tiesības saņemt kompensāciju no Amgen France par nodarīto kaitējumu, un tiesām vai citām kompetentajām iestādēm EEZ, kam ir jurisdikcija. Datu subjektam ir tiesības un tiesiskās aizsardzības līdzekļi pret Amgen France tā, it kā pārkāpumu ES būtu izraisījusi Amgen France, nevis iesaistītais uzņēmums, kas nav reģistrēts EEZ. Ja iesaistītais uzņēmums, kas nav reģistrēts EEZ, ir atbildīgs vai tiek saukts pie atbildības par šādu pārkāpumu, tā, ciktāl tas ir atbildīgs, atlīdzinās Amgen France visas izmaksas, maksas, bojājumus, izdevumus vai zaudējumus, kas radušies saistībā ar Amgen France par šo pārkāpumu.
- 18.5. Gadījumā, ja datu subjekts iesniedz pretenziju, ka viņam ir nodarīts kaitējums un ir konstatēts, ka šāds kaitējums ir radies šo ES BCR pārkāpuma dēļ, Amgen France ir pienākums pierādīt, ka datu subjektam nodarītie zaudējumi šā ES BCR pārkāpuma dēļ nav attiecināmi uz attiecīgo iesaistīto uzņēmumu.. Ja Amgen France var pierādīt, ka iesaistītais uzņēmums, kas reģistrēts ārpus EEZ, nav atbildīgs par notikumu, kas izraisījis kaitējumu, tas nav atbildīgs par zaudējumiem.

## **19. Savstarpēja palīdzība un sadarbība ar datu aizsardzības iestādēm**

- 19.1. Iesaistītie uzņēmumi sadarbojas un palīdz viens otram, lai apstrādātu datu subjekta pieprasījumu vai sūdzību vai kompetentās DAI veiktu izmeklēšanu vai izmeklēšanu.
- 19.2. Iesaistītie uzņēmumi sadarbībā ar galveno privātuma amatpersonu atbildēs uz kompetentās datu aizsardzības iestādes ar ES BCR saistītiem pieprasījumiem atbilstošā termiņā, ņemot vērā pieprasījuma apstākļus (jebkurā gadījumā ne vēlāk kā jebkurā kompetentās DAI noteiktajā termiņā) un atbilstoši detalizēti, pamatojoties uz informāciju, kas ir pamatoti pieejama iesaistītajam uzņēmumam. Saistībā ar ES BCR ieviešanu un pastāvīgo piemērošanu iesaistītie uzņēmumi pienācīgi ņem vērā kompetentās DAI paziņojumus un ieteikumus un ievēro visus oficiālos lēmumus vai paziņojumus, ko izdevusi kompetentā DAI.
- 19.3. Jebkuru strīdu, kas saistīts ar kompetentās DAI uzraudzību attiecībā uz atbilstību šiem ES BCR, risina attiecīgās DAI dalībvalsts tiesas saskaņā ar šīs dalībvalsts piemērojamajiem tiesību aktiem.

## **20. ES BCR atjaunināšana un izmaiņas**

- 20.1. Amgen patur tiesības jebkurā laikā mainīt un/vai atjaunināt šos ES BCR. Šāda ES BCR atjaunināšana var būt nepieciešama īpaši jaunu juridisku prasību, būtisku izmaiņu Amgen grupas struktūrā vai kompetentās DAI noteikto oficiālo prasību dēļ.
- 20.2. Amgen nekavējoties un bez liekas kavēšanās ziņos par jebkurām būtiskām izmaiņām ES BCR vai iesaistīto uzņēmumu sarakstā visiem pārējiem iesaistītajiem uzņēmumiem un kompetentajai DAI, lai ņemtu vērā izmaiņas piemērojamos tiesību aktos, normatīvajā vidē un/vai Amgen grupas struktūrā. Jo īpaši, ja izmaiņas ietekmētu ES BCR piedāvāto aizsardzības līmeni, galvenais privātuma speciālists nekavējoties paziņos par šādām izmaiņām kompetentajai datu aizsardzības iestādei, sniedzot īsu skaidrojumu par izmaiņu iemesliem. Dažām izmaiņām var būt nepieciešams jauns apstiprinājums no kompetentās datu aizsardzības iestādes.

- 20.3. Galvenais privātuma speciālists uzturēs pilnībā atjauninātu iesaistīto uzņēmumu sarakstu ES BCR un izsekos visiem noteikumu atjauninājumiem, kā arī pēc pieprasījuma sniegs nepieciešamo informāciju datu subjektiem vai kompetentajai DAI. Par visām administratīvajām izmaiņām ES BCR tiks regulāri ziņots iesaistītajiem uzņēmumiem.
- 20.4. Nekāda personas datu pārsūtīšana jaunam iesaistītajam uzņēmumam netiks veikta saskaņā ar ES BCR garantijām, līdz jaunais iesaistītais uzņēmums nebūš faktiski saistīts ES BCR un atbilstošs ES BCR prasībām.
- 20.5. Jebkuras administratīvas izmaiņas ES BCR vai iesaistīto uzņēmumu sarakstā būs regulāri paziņotas iesaistītajiem uzņēmumiem un vismaz reizi gadā par to ziņos kompetentajai DAI ar īsu paskaidrojumu par atjaunināšanas iemesliem.
- 20.6. Būtiskas izmaiņas ES BCR arī tiks paziņotas datu subjektiem, izmantojot jebkādus līdzekļus saskaņā ar ES BCR 7. pantu.

## **21. Saistība starp valsts tiesību aktiem un ES BCR**

- 21.1. Ja Vietējie valsts tiesību akti, kas piemērojami iesaistītajam uzņēmumam, pieprasa augstāku personas datu aizsardzības līmeni, tiem būs prioritāte pār ES BCR. Ja vietējie valsts tiesību akti, kas attiecas uz iesaistīto uzņēmumu, nodrošina zemāku personas datu aizsardzības līmeni nekā ES BCR, tiks piemēroti ES BCR.
- 21.2. Gadījumā, ja pienākumi, kas izriet no vietējiem nacionālajiem tiesību aktiem, kas piemērojami iesaistītajam uzņēmumam, ir pretrunā ar ES BCR, iesaistītais uzņēmums bez nepamatotas kavēšanās informē galveno privātuma amatpersonu un ievēro papildu prasības, kas iepriekš noteiktas 16. pantā.
- 21.3. Jebkurā gadījumā personas dati tiek apstrādāti saskaņā ar GDPR 5. pantu un attiecīgajiem vietējiem tiesību aktiem.

## **22. Nobeiguma noteikumi**

- 22.1. ES BCR stājas spēkā pēc tam, kad to apstiprinājusi kompetentā DAI, un tie ir piemērojami iesaistītajiem uzņēmumiem, parakstot ES BCR pieņemšanas līgumu.
- 22.2. Iesaistītajam uzņēmumam neveic nekādus pārskaitījumus, ja vien tai nav saistoši šie ES BCR. Ja datu importētājam vairs nav saistoši ES BCR, tam nekavējoties ir jāatgriež vai jādzēš visi personas dati (tostarp to kopijas), kas ir pārsūtīti saskaņā ar šiem ES BCR, izņemot gadījumus, kad datu importētājs nodrošina juridiski saistošus pienākumus saglabāt personas datus saskaņā ar GDPR V nodaļu tā var saglabāt personas datus, kas ir pārsūtīti saskaņā ar šiem ES BCR.
- 22.3. Datu importētājam ir nekavējoties jāinformē datu eksportētājs, Amgen France un galvenais privātuma speciālists, ja tas kāda iemesla dēļ nevar ievērot šos ES BCR (tostarp 12.3. pantā aprakstītās situācijas). Ja datu importētājs pārkāpj šos ES BCR vai nespēj tos ievērot, datu eksportētājam ir jāinformē galvenais privātuma inspektors un jāaptur personas datu pārsūtīšana.

22.4. Pēc datu eksportētāja izvēles datu importētājam ir nekavējoties jāatgriež vai jādzēš visi personas dati (tostarp to kopijas), kas ir pārsūtīti saskaņā ar šiem ES BCR, un jāapliecina tie datu eksportētājam, ja:

22.4.1. datu eksportētājs ir apturējis personas datu pārsūtīšanu, un atbilstība šiem ES BCR netiek atjaunota saprātīgā termiņā un jebkurā gadījumā viena mēneša laikā pēc apturēšanas; vai

22.4.2. datu importētājs būtiski pārkāpj šos ES BCR; vai

22.4.3. datu importētājs nepilda saistošu kompetentas tiesas vai kompetentas DAI lēmumu par tā saistībām saskaņā ar šiem ES BCR.

Kamēr personas dati nav dzēsti vai atgriezti, datu importētājam ir jāturpina nodrošināt atbilstību šiem ES BCR. Ja vietējie valsts tiesību akti, kas piemērojami datu importētājam, aizliedz atgriezt vai dzēst personas datus, kas pārsūtīti saskaņā ar šiem ES BCR, datu importētājam ir jāturpina nodrošināt atbilstību šiem ES BCR un jāapstrādā personas dati tikai tādā apmērā un tik ilgi, cik to pieprasa vietējie valsts tiesību akti.

### **23. Pielikumi**

Pievienotie pielikumi ir ES BCR neatņemama sastāvdaļa.

1. pielikums: Amgen datu plūsmu pārskats

2. pielikums: Amgen apmācības programmas pārskats

**1. pielikums: Amgen datu plūsmu pārskats**

<b>Datu subjekti</b>	<b>Datu kategorijas</b>	<b>Mērķi</b>	<b>Pārsūtīšana</b>
Darbinieks	<p>Identifikācijas dati, piemēram, vārds, adrese, dzimšanas datums un vieta, darba līguma datums, sociālās apdrošināšanas numuri, kredītkaršu numuri, bankas konta un finanšu informācija, kā arī autovadītāja apliecības un valsts izdotas identifikācijas karšu numuri</p> <p>Atvaļinājumi un pabalsti, sūdzības, prēmijas, paaugstinājumi, pārskati un novērtējumi, darba ieraksti, informācija par veselības un labklājības nodrošinājumu, pensijas plāns un akciju opciju informācija</p> <p>Nodokļu un finanšu personas informācija</p> <p>Sensitīvi dati, piemēram, izcelsmes valsts, ja to atļauj vietējie tiesību akti</p>	<p>Personāla vadības, informācijas tehnoloģiju atbalsta un administrēšanas nolūkos saistībā ar darba attiecībām un pabalstiem vai pēcnodarbinātības pabalstu administrēšanai, kā arī Amgen juridisko, administratīvo un korporatīvo pienākumu izpildei</p>	<p>Amgen globālās datu bāzes atrodas ASV, kur atrodas Amgen Inc., galvenā mītne.</p> <p>Dati plūst no Amgen France (vai attiecīgā datu eksportētāja) uz Amgen Inc. Amerikas Savienotajās Valstīs vai uz iesaistītajiem uzņēmumiem Šveicē. Pēc tam dati:</p> <ul style="list-style-type: none"> <li>- tur vienkārši jāuzglabā un jāuztur</li> <li>- jāanalizē, lai nodrošinātu globālu statistiku un pārskatus</li> <li>- tiek izplatīti Amgen grupas iekšienē ar citiem iesaistītajiem uzņēmumiem, ja ir biznesa vajadzība pēc šādas piekļuves konkrētam personālam vai uzņēmējdarbības funkcijām šajos iesaistītajos uzņēmumos (piemēram, darbinieks, kurš piesakās darbam ārpus savas valsts vai viņam ir jāatskaitās vadītājam ārpus savas valsts). Vairumā gadījumu šādi iesaistītie uzņēmumi</li> </ul>
Veselības aprūpes speciālisti	<p>Vārds, uzņēmuma kontaktinformācija, tostarp tālruna numurs un e-pasta adrese, kompetences joma</p> <p>Profesionālā pieredze (CV)</p> <p>Dalība citos pētījumos</p> <p>Finanšu informācija (norēķinu un maksājumu informācija)</p>	<p>Amgen profesionālo un zinātnisko darbību administrēšana un vadība – pētniecība un attīstība (piemēram, piedalīšanās medicīniskajos pētījumos, klīniskajos pētījumos, profesionālās sanāksmēs vai kongresos)</p> <p>Amgen produktu un pakalpojumu veicināšana</p> <p>Finanšu informācijas izpaušana, ja to pieprasa piemērojami tiesību akti vai nozares kodeksa ievērošana</p> <p>Atbilstība normatīvajiem aktiem, piemēram, drošības uzraudzība un ziņošana par nevēlamām blakusparādībām</p>	

			darbosies kā datu pārziņi, taču atkarībā no biznesa vajadzībām iesaistītie uzņēmumi var darboties arī kā datu apstrādātāji (piemēram, sniedzot IT palīdzības dienesta atbalstu vai sniedzot atbalstu saistībā ar HR Connect pakalpojumu centru).
Pārdevēji / piegādātāji	Personas nosaukums, organizācijas nosaukums, uzņēmuma kontaktinformācija  Norēķinu un maksājumu informācija	Maksājumu apstrāde pārdevējiem un piegādātājiem  Atbilstība normatīvajiem aktiem, piemēram, nodokļu tiesību aktiem	
Klīnisko pētījumu datu subjekti (tostarp var būt bērni, kas jaunāki par 18 gadiem, ja Amgen sponsorētā klīniskā pētījumā ir iesaistīts bērns).	Kodēti dati – pacienta vārds un kontaktinformācija tiek aizstāta ar iekšēji ģenerētu identifikācijas numuru. Tikai klīniskās izpētes vieta (slimnīca/pētniecības vieta) uztur sarakstu, lai identifikācijas numuru saistītu ar pacienta vārdu.  Netiešie identifikatori, piemēram, dzimšanas gads vai datums (pilns dzimšanas datums tiek apkopots tikai pediatrijas pētījumiem), dzimums, svars, augums.  Nepieciešamie veselības dati, kā norādīts pētījuma protokolā.  Citi dati, kas attiecas uz pacientu, kas nepieciešami pētījuma veikšanai, tostarp etniskā piederība, ģimenes stāvoklis (piemēram, bērnu skaits), narkotiku, alkohola, narkotiku lietošana, vispārējie ieradumi vai uzvedība, profesionālā situācija, piemēram, darbs, bezdarbs, dalība citos pētījumos.	Biomedicīnas pētījumu administrēšana un vadība (klīniskie pētījumi, novērošanas pētījumi)	
Pacienti (ieskaitot bērnus, kas jaunāki par 18 gadiem, ja ir novērotas	Pacienta netiešie identifikatori, piemēram, vecums, dzimšanas gads vai datums, pacienta iniciāļi (atbilstoši vietējiem tiesību aktiem),	Atbilstība normatīvajiem aktiem un farmakovigilance, piemēram, drošības	

<p>nevēlamas blakusparādības, kas saistītas ar Amgen produkta lietošanu pediatriskās indikācijās).</p>	<p>dzimums, svars/augums vai pacienta identifikācijas numurs (izņemot valsts veselības identifikatorus).</p> <p>Dati, kas attiecas uz Amgen produkta identifikāciju, piemēram, izmantotais produkts vai ierīce, ierīču sērijas numuri, piegādes veids vai produkta deva, produkta partijas/sērijas numuri.</p> <p>Veselības dati, tostarp veiktās ārstēšanas metodes, izmeklējumu rezultāti, jebkādas nevēlamas(-u) ietekmes raksturs, personīgā vai ģimenes slimības vēsture, saistītās slimības vai notikumi, riska faktori, informācija par zāļu izrakstīšanu un lietošanu, kā arī veselības terapeitisko darbību profesionāļi, kas iesaistīti pacienta slimības ārstēšanā.</p> <p>Citi dati, kas attiecas uz pacientu, kas nepieciešami nevēlama veselības notikuma novērtēšanai saskaņā ar normatīvajiem atbilstības pienākumiem, piemēram, etniskā piederība, profesionālā dzīve, narkotiku, alkohola, narkotiku lietošana un/vai vispārējie ieradumi vai uzvedība.</p>	<p>uzraudzība un ziņošana par blakusparādībām (ja to atļauj vietējie tiesību akti)</p>	
--	---	--	--



## **2. pielikums: Amgen apmācības programmas pārskats**

### ***Privātuma un datu aizsardzības apmācība/izpratnes programma***

Privātuma un datu aizsardzības apmācības programmas mērķis ir nodrošināt, lai visi Amgen darbinieki būtu atbilstoši apmācīti par Amgen EU BCR, kā arī par jebkādam juridiskajām saistībām, kas ietekmē personas datu apstrādi. Šī programma satur dažādus elementus.

#### **Vispārīga apmācība visam Amgen personālam**

Visam Amgen personālam ir jāveic ikgadēja tiešsaistes apmācība par datu aizsardzību, kas ir daļa no Rīcības kodeksa apmācības. Šī apmācība ir obligāta un uzraudzīta, un tās pabeigšana parasti aizņem apmēram 75 minūtes. Šajā apmācībā ir iekļauti ES BCR un informācija par sekām saskaņā ar krimināltiesībām un darba tiesībām un/vai viņu pakalpojumu līgumiem darbiniekiem, kuri pārkāpj ES BCR.

#### **Īpaša apmācība DAI**

Visi Amgen DPO tiek regulāri apmācīti par jauniem procesiem, izmantojot regulārus DPO zvanus, ko veic globālā privātuma atbilstības komanda, un privātuma seminārus uz vietas un/vai tiešsaistē, pamatojoties uz nepieciešamību zināt. Visiem DPO ir piekļuve wiki lapai, kurā ir sniegtas atbildes uz visbiežāk uzdotajiem jautājumiem un sniegti norādījumi, kā arī saites uz ārējiem resursiem.

#### **Īpaša apmācība personālam**

Īpašas apmācības var nodrošināt, pamatojoties uz nepieciešamību zināt, vai nu tiešsaistē, vai uz vietas, vai arī ievieojot informāciju Amgen iekštīklā. Šīs apmācības var būt vērstas uz konkrētām grupām, kas var vai nu apstrādāt personas datus katru dienu, vai atbalstīt citas grupas, kas apstrādā personas datus. Piemēram, revīzijas grupa, pētniecības un attīstības funkcijas un juridiskā nodaļa tiek regulāri apmācītas. Tas ietver informāciju par procedūram, lai pārvaldītu valsts iestāžu pieprasījumus piekļūt personas datiem, ja tas attiecas uz konkrētiem darbiniekiem. Šīs apmācības var notikt vai nu reģionālā līmenī, vai valsts līmenī. Papildu īpašas ES BCR apmācības var tikt izstrādātas, pamatojoties uz nepieciešamību zināt.

#### **Apzināšanās**

Amgen iekštīklā ir īpaša lapa par privātumu un datu aizsardzību, kas nodrošina saites uz citiem iekšējiem vai ārējiem resursiem.

Amgen globālās privātuma atbilstības komanda sadarbojas ar informācijas drošības nodaļu Sentinel programmā, kas ir globāla programma, lai palielinātu Amgen personāla informētību par informācijas drošību.

#### **Apmācības atbalsts**

Visas ar privātumu saistītās apmācības ir izstrādājuši globālā privātuma atbilstības komanda un apstiprinājuši galvenā privātuma amatpersona. Apmācību var tieši veikt globālās privātuma atbilstības komandas loceklis vai vietējais DPO pēc modeļa "apmācīt pasniedzēju".